Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 2, February : 2024

MULTIPLE FORMAT VIDEO STEGANOGRAPHY USING AES 256 AND RSA ENCRYPTION

Prof. Premanand Ghadekar, Prajwal Atram, Hitashri Patil, Nupur Shinde, Vishal Singh, Sameer Meshram, Vishwakarma Institute of Technology, Pune, India

Abstract: The word steganography relates to hiding confidential information or messages within non secret data, for example hiding image into image for the purpose of transaction security. The same approach is used for video steganography. Least significant bits approach is considered a popular technique for implementing steganography. Improving the accuracy of this technique is somewhat difficult as proper awareness towards the series of frames of video is not provided and affects the accuracy of the method. The proposed model discusses the application encryption methodologies like AES 256 and RSA for securing the data which is stored in the video without more loss of data. The video frames for storing data are randomly chosen and the sequence of frames is again stored in another image to recollect the chosen order. The proposed model hides data formats like text, audio, image and video in the video at a time.
Keywords: Steganography, Encryption, LSB, Decryption, Multiple data formats, simultaneously.

I. INTRODUCTION

In recent times, Snapchat, Instagram, and other social media applications are being considered widely used applications. The center of attraction of these applications is to focus on videos and images as a key technique for digital communication. Enormous quantities of data can be transmitted using videos and images across the world. Several applications and research have been established to isolate and inspect the embedded data within the video or image. In addition to that, there are numerous methods that make use of videos and images to conceal secret data. Videos and images have an understandable benefit in hiding information because of the failure of the human eye to distinguish between the minuscule variations in pixels of videos and images. Videos and images are presenting a significant part in hiding information and data security.

The word ‘Steganography’ is a Greek word. It is a mixture of two words "stegno” which implies "to cover up” and “graphein” which implies “text". Nowadays, steganography is being utilized as a secret communication and interaction technique in the digital domain to hide the original data in another medium such as videos, images, documents etc.In steganography fields, the established technique is image steganography and there are many scientists that have previously done research on image steganography and its decryption. Usually, the video contains various images or frames with sound or without sound. Hence, video steganography can be considered as an expansion of image steganography.

In this research paper, a system is proposed that uses video steganography to hide information in different formats into the initial video. The use of AES 256 and RSA encryption in video steganography stems from a dual commitment to strong security measures and established cryptographic standards AES 256, as an advanced encryption standard, ensures data privacy video content through its symmetric encryption capability. Its 256-bit key provides an exceptionally high level of security, making malicious attacks impossible on a computer. Accordingly, RSA encryption introduces an asymmetric layer to the security framework, managing encryption keys and ensuring secure communication between entities The Public-private key pair mechanism of the RSA algorithm adds an extra layer of security, somewhere a private key is only held by the authorized user.

II. RELATED WORK

Several In the proposed system, the authors have developed a project, which has an objective i.e., requirements of this steganography are that the hider message carried by Stego-media should not to citizenry. The project allows users to settle on the bits for replacement rather than LSB replacement from the image. But it has limitations like images can have attacks like diluting, noising, contrast

changes [1].

The authors of this paper have suggested a system which offers two levels of safety to the information i.e., cryptography and Steganography. Initially the information is encoded by using a cryptography process, then the encoded information is inserted into video frames. It has the drawback that just a single text message can be concealed in the video [2].

In the suggested system, the authors have proposed the Integer Wavelet Transform method with Joint Photographic Expert Group compression so that the problems with steganography techniques can be overcome. Cover files of videos that are original video and Joint Photographic Expert Group compression enhance hiding capacity because of their fundamental features. It has limitations i.e. video quality gets affected by adding a message into it [3].

In the proposed model, the authors have proposed a unique technique regarding video steganography which uses a suggested key task technique that can encrypt confidential data so that it can improve protection. Moreover, it employs a key task to encode data, it can understand subjective values that are different in every method to improve the effectiveness and toughness for the suggested technique. [4].

In the proposed system, the authors have proposed a system which uses video steganography algorithm PyraGAN, which maintains various sized cover video frames. Performance is enhanced by the CU mask created by VVC. The drawback of this paper is appropriate error correction encoding technique is necessary for complete removal of concealed messages [5].

In the proposed model, the authors have suggested an algorithm for concealing data within a picture. The suggested system concentrates on analysis of 3 methods centered on LSB methods which want to leave bits of idea in the LSB from every image pixel. Furthermore, other proposed models have suggested an enhanced methodology for LSB-established image steganography. In this method, the authors have decreased the size of concealed message by using Deflate algorithm [6].

In the proposed system, the authors have examined applications like QR codes to interchange data using steganography and AES methodology. The last conclusions' presentation would be evaluated from evaluating file of an image feature earlier and after information had been concealed from point of view in the documents [7].

In the proposed model, the authors aim to build an information safety simulation established on steganography and cryptography for information in cloud computation that pursues to decrease current safety and confidentiality worries, such as information failure, information management, and information stealing. To recognize the problem and establish its primary reason, from several literature on present cloud computing safety prototypes. [8].

In the proposed work, a study on video steganography multi-layer algorithms is suggested. This paper widely reviews frequency and three-dimensional domain methods mixture with cryptography, steganography and error modification methods [9].

The proposed method built a perfect user-friendly approach that encoded text messages utilizing the AES algorithm. The encoded letter is then encoded into image by making use of steganography methods like Discrete Cosine Transform, Least Significant Bit and Discrete Wavelet Transform [10].

In the proposed method, batch steganography is applied to protect information communication from one user to another. Frequently a password can be employed for encrypting the data into the original image. Here the information is encoded employing AES, encryption techniques, hashing and SHA-256. [11].

The paper suggested a cross breed algorithm 128-digit key i.e., CBA-128 established on DES and AES for improving the safety and utilizes steganography-centered encoding to improve the safety of the information throughout information communication over the association. [12].

In the proposed work, multilayer techniques for video steganography are reviewed. This study broadly analyzes the steganography, three-dimensional, frequency field methods fusion with error correction techniques and cryptography [13].

III. METHODOLOGY

The proposed work focuses on secure transmission of multiple data formats by hiding them inside the cover video simultaneously as well as individually. These paper focuses on the enhancement of robustness, security, and capacity of the transfer information.

Following are the data formats that can encode individually as well as simultaneously into cover video.

1)Image 2) Audio 3) Video 4) Text/Text Document

A. Video Steganography-AES Encryption:

By implying paper [1] based on LSB an approach to overcome these drawbacks is the AES-256 Algorithm used in the proposed model. Here the state is 256 bits, which allows encrypting and decrypting with three different key lengths. AES-256-bit key length is used in the proposed model. To encrypt text into videos without affecting the quality of the video.

Encryption: This figure shows that the algorithm takes 128 bits of block for a particular format and converts it into 128-bit encrypted format.

Decryption: This figure shows that algorithm takes 128 bits encrypted block for a respective format and converts it into 128-bit decryption format.

B: Video Steganography- RSA Algorithm:

RSA is a cryptographic algorithm of asymmetric type. It works on two different keys i.e., Public Key and Private Key.

Encryption using RSA:

For Encrypting a plaintext M using an RSA public key it generally represents the plaintext as number 0 and N-1 and then convert the ciphertext C as:

i) C = Me mod N. … (1) [14]

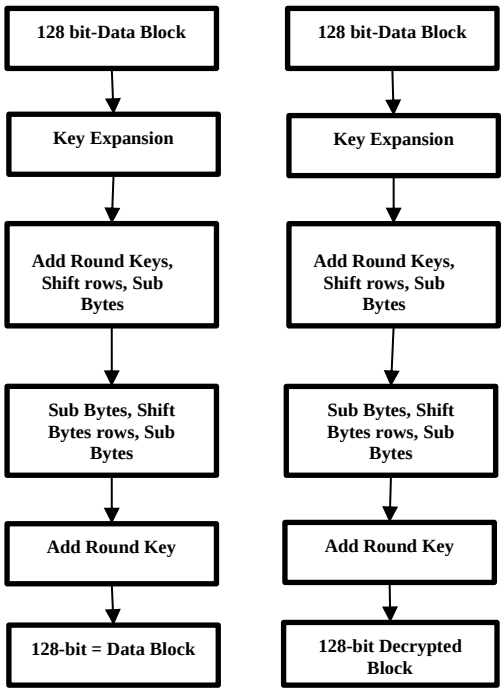

Figure 1: Encryption and Decryption

Decryption using RSA:

For the decryption of ciphertext C using the RSA public key it normally converts the plaintext M as:

ii) M = Cd mod N. … (2) [14]

The suggested work is the combination of all the above- mentioned approaches, one is used for the purpose of encryption and another for decryption to achieve and provide high protection.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 2, February : 2024

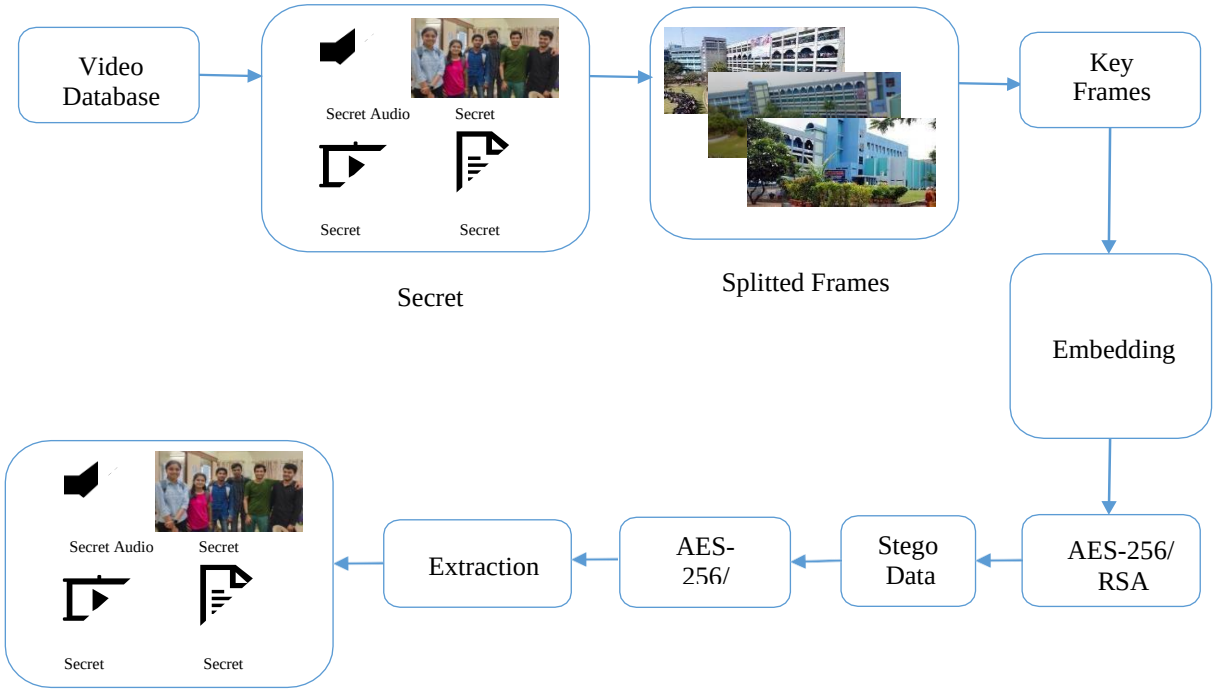

Figure 2: Flow diagram of multiple format video steganography using AES and RSA algorithm.

Encrypting

Step 1: Select a video as a cover where the data can be encoded.
Step 2: Ask for file formats to be hidden.
Step 3: Isolate the frames of the cover video in a tmp named folder.
Step 4: Ask for an algorithm which the user wants to use.
Step 5: Ask for the ASCII value and path of the public key for convert text to cipher text.
Step 6: Select the frame number.
Step 7: Give path gives a path of image of a cover file and data is encoded successfully.

Decrypting

Step 1: Ask for the frame numbers where you stored the data.
Step 2: Ask for algorithm which he want to use for decryption.
Step 3: Need to enter key to generate key that is use for decryption.
Step 4: The generated decrypted key is to be enter here. This gives the frame numbers where the data is stored.
Step 5: Ask to enter the frame numbers where the data is stored.
Step 6: Multiple formats data like image, audio, video and text is decrypted at the same time.

IV. COMPARISON OF EXISTING MODEL WITH THIS ARCHITECTURE

The proposed model works with all the expected file formats of the video. The data can be hidden in the form of Text, Text document, Audio, Video, Image both symmetrically and asymmetrically in the video which this can't be performed by using least significant bits and other algorithms. Users can select the frames of their choice from the video for hiding the data. The hiding frame's information can be hidden inside the image of any file format. The file formats which use lossy compression especially JPEG which means the pixels of the file formats are modified to reduce the quality of the image during the hiding of the information and therefore data loss happens [15] and this proposed model works well fine, and each frame can be extracted information successfully without any single loss of the frames information in which the system hides the frames information.
Exchanging the keys made this model more secure and efficient to avoid extracting the data. The

steganographic video after successful encoding is in .mov structure, which supports images that are 16 bit in nature for the embedding the data during the selection of the frames of the video for hiding the data both symmetric and asymmetrically by using AES-256 and RSA algorithms.[16] The multiple formats data like audio into video, video into video, and images into video etc. The system can hide in this proposed model.

V. RESULTS

In this proposed model first, the system has to generate keys i.e., public and private keys.
As shown in Figure 3 to make a secure transmission of the message between sender and receiver which is stored inside the keys folder of the root directory by running the keys generation script which is shown in Figure 3.

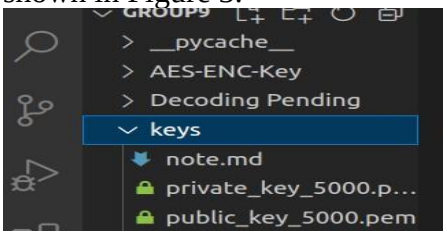

Figure 3: Public and Private Keys.

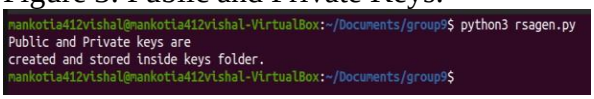

Figure 4. Keys are Stored inside any keys folder.

Now, users have to run an encoding file present in the root directory to encode data using AES-256 & RSA algorithm. Then user can select the file format from text, audio, video, or image which user wants to hide in the video and follow procedure as shown in image below.

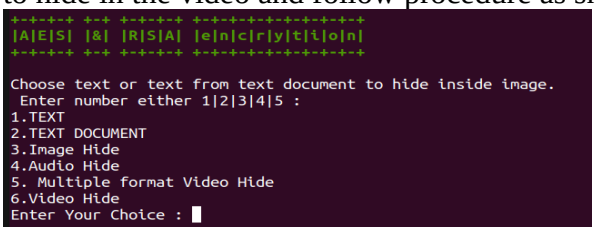

Figure 5. Choose any Option to Hide Data

The video consists of the frames and all the frames of the video are stored in the root tmp directory. Users can choose any algorithm to send data to the receiver i.e., AES or RSA algorithm. Users have to give the path of our public key to move further. Now users can choose frames of our desired choice to encode data and then save the information of the frames of the video in which users are the hiding the information and successfully users can encrypt the data inside a video and steganographic video output is in the video.mov format as shown in figure 6 and a key receiver.txt is generated in the AES & RSA root directory as shown in figure 6.

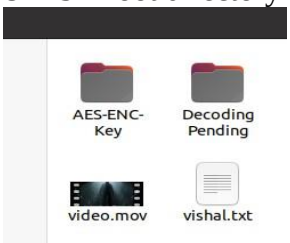

Figure 6. Output video

The system can use this steganographic video to decrypt the data that the sender is sending and use the image to extract information of the frames in which the information can be hidden.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 2, February : 2024

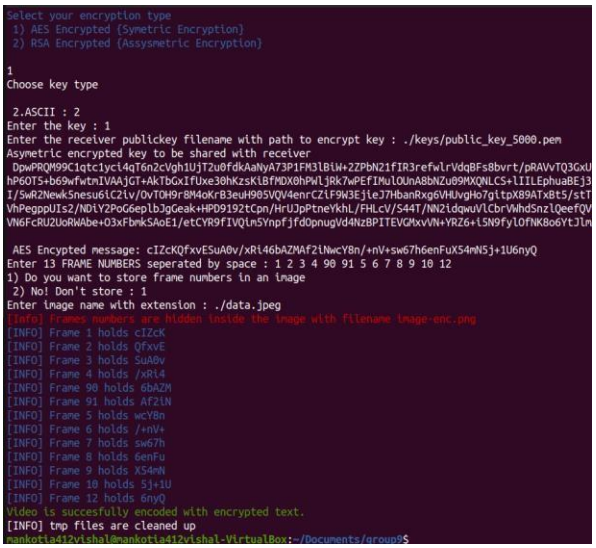

Figure 7. Select frames to encrypt data.

The data and the use that receiver key to extract the information that is generated during the successful encryption. Thus, by following the steps the system can successfully decrypt the data that users have hidden inside the video as shown in Figure 8 & Figure 9.

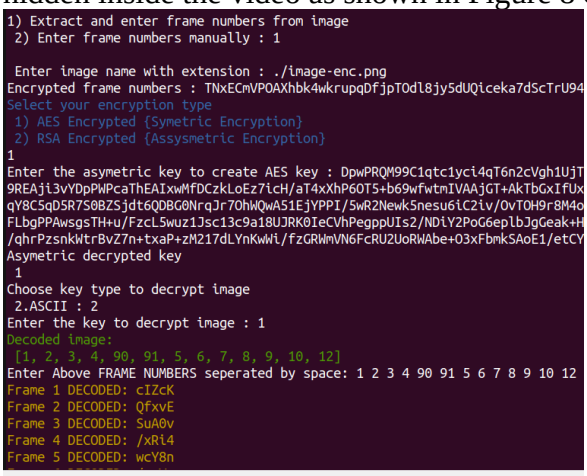

Figure 8. Frames decoded in which data is hidden.

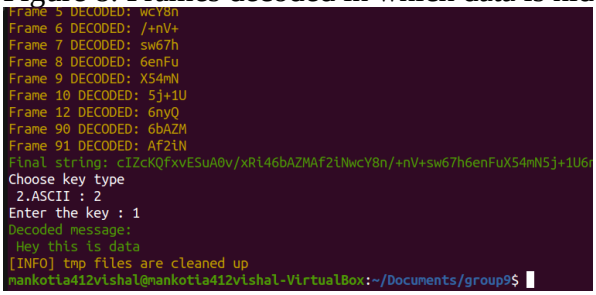

Figure 9. Decryption of the text data from the video.

Users can see the data that is sent by the sender successfully. The other operations It can perform data hiding of multiple formats like video into video, audio into video, image into video & text documents are similar but just data that the system is going to hide inside the video changes else everything remains the same and follows the same procedure for that also. The videos and audio images data that the system is using is as shown in Figure 10.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 2, No. 2, February : 2024

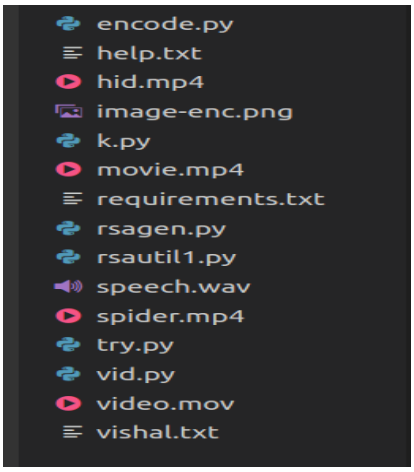

Figure 10. Files and the directories present in the root directory.

For the multiple formats sending at same time the user has to give input to the model.

In the sequence as shown in Figure 11.

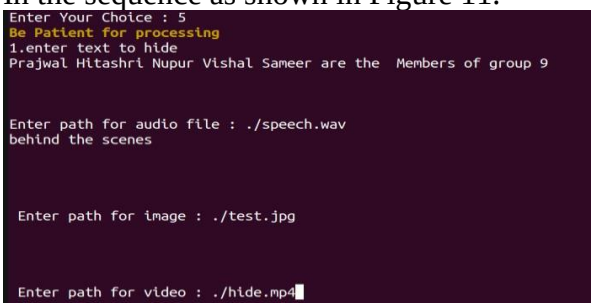

Figure 11. Enter the multiple formats of data for hiding inside a video at once.

The user has to be patient while sending the multiple format data as an input. It will take some computations and follow the same procedure as shown in Figure 12.

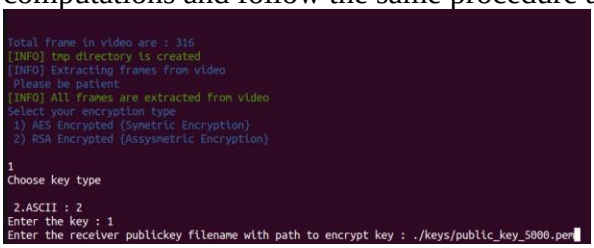

Figure 12. Enter the public key path.

The user will get this message as shown in Figure 13. As video is successfully encoded with multiple format data that is text audio video and image.

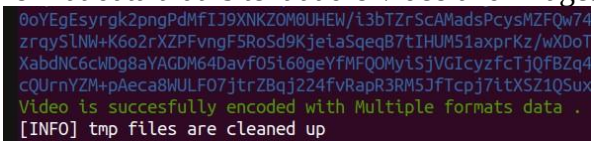

Figure 13. Message of Successful Encryption into video.

And while decoding the user has to write the choice and give the frame number information in which data is hidden and choose the algorithm by which the user has hidden the data as shown in Figure 14.

Figure 14. Enter the frames in which data is hidden.

The final results will be that the user will get information back whatever the user has hidden inside the video and the results are shown in Figure 15 and Figure 16.

Figure 15. Extraction of messages decrypted from the video at once.

There is no loss of data while decoding the message and thus successful decoding is done by using AES 256 and RSA algorithm.

Figure 16. Output image from the stenographic video.

Table 1. PSNR and MSE Value of the Proposed System

PSNR	98.15383916647286
MSE	0.002452907301524711

The Proposed system has Mean square error (MSE) value as 0.002452907301524711 and Peak Signal Noise Ratio (PSNR) value as 98.15383916647286.

VI. CONCLUSION AND FUTURE WORK

The primary objective of our paper is to encode multiple formats like Video, Audio, Image, Text message together at the same time in the video. It is successfully retrieved by using the AES and RSA Encryption Algorithms. The data stored in the video depends upon the length of the cipher text. If cipher text goes more than 4 lacs, then data cannot be encrypted. The users can store only a limited amount of data using AES 256 & RSA algorithm.

The proposed method provides two levels of encryption to hide the hidden information of the cover video. It is very difficult for an attacker to crack the ciphertext. Encryption techniques used to secure the data which prevents the breaching of data. Approximately 400 KB of data is stored in the video of size 4.3 MB using this algorithm.

The idea proposed in the paper is efficient. Advance improvements that can be done in sending more information messages in the video using some additional techniques like along with AES 256, RSA also use wavelets to send more information and get high Video Compression without affecting the quality of the video. An innovative advancement can be to solve the problems of container misusing such as adding noise, constricting, or cutting video temporally and spatially, etc. by continuously storing secret data within cover, which can be considered as future work.

VII. REFERENCES

[1] Jagruti Mishra, Madhavi Chavan, Riddhi Ambekar, "Video Steganography," International Research Journal of Engineering and Technology, Volume: 07, Issue: 06, June 2020.

[2] Gat Pooja Rajkumar, Dr. V. S. Malemath, "Video Steganography: Secure Data Hiding Technique," I. J. Computer Network and Information Security, 38-45, 2017.

[3] Urmila Pilania, Rohit Tanwar, Mazdak Zamani, Azizah Abdul Manaf, "Framework for Video Steganography Using Integer Wavelet Transform and JPEG Compression," Future Internet 2022, 14,

254.
[4] Zeyad Safaa Younus, Ghada Thanoon Younus, "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data," J. Intell. Syst., 2020; 29(1): 1216–1225.
[5] Huanhuan Chai, Zhaohong Li, Fan Li, Zhenzhen Zhang, "An End-to-End Video Steganography Network Based on a Coding Unit Mask," Electronics 2022, 11(7), 1142.
[6] S. L. Chikouche, N. Chikouche, "An improved approach for LSB-based image steganography using AES algorithm," 2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B), 2017, pp.1-6.
[7] Abhinav Agarwal, Sandeep Malik, "An AES-Based Efficient and Valid QR Code for Message Sharing Framework for Steganography," Expert Clouds and Applications, Lecture Notes in Networks and Systems, Springer, Singapore, vol 444, 2022.
[8] Rose Adee, Haralambos Mouratidis, "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography," Sensors 2022, 22(3), 1109.
[9] Siti Norul Huda Sheikh Abdullah, "Challenges in Multi-Layer Data Security for Video Steganography Revisited," Asia-Pacific Journal of Information Technology and Multimedia (APJITM), 2022.
[10] Alicia Biju, Lavina Kunder, J. Angel Arul Jothi, "Analysis on Advanced Encryption Standard with Different Image Steganography Algorithms: An Experimental Study," Data Engineering and Communications Technologies, vol 111. Springer, Singapore, 2022.
[11] R. Joshi, A. K. Bairwa, V. Soni, S. Joshi, "Data Security Using Multiple Image Steganography and Hybrid Data Encryption Techniques," 2022 International Conference for Advancement in Technology (ICONAT), 2022, pp. 1-7.
[12] A. Gupta, S. Ganapathy, "A New Security Mechanism for Secured Communications Using Steganography and CBA," ECTI-CIT Transactions, vol. 16, no. 4, pp. 460–468, Oct. 2022.
[13] Samar Kamil, Masri Ayob, Siti Norul Huda Sheikh Abdullah, Zulkifli Ahmad, "CHALLENGES IN MULTI- LAYER DATA SECURITY FOR VIDEO STEGANOGRAPHY," Asia-Pacific Journal of Information Technology and Multimedia Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik Vol. 7 No. 2-2, December 2018: 53 – 62.
[14] A. Nitaj, M. R. B. Kamel Ariffin, N. N. H. Adenan, T. S. C. Lau, J. Chen, "Security Issues of Novel RSA Variant," IEEE Access, vol. 10, pp. 53788-53796, 2022.
[15] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography."