Video Steganography Using RC6 And HLSB

Malathi N[1], Nasuha Nazia N[2], Subalakshmi S[3], Mrs. Hemamalini R[4]
[1, 2, 3] Dept of ECE
[4]Assistant Professor, Dept of ECE
[1, 2, 3, 4] Meenakshi Sundararajan Engineering College

Abstract- *For secure data transmission over the internet, it's important to transfer data with high security and high confidentiality. Information security is the most important issue of data communication in networks and the internet. To secure transferred information from interferers, it's important to convert the information into cryptic format. Different styles like Steganography and cryptography are used to insure data security and confidentiality during transmission. Based on Steganography, we have convert plain textbook to cipher textbook using RC6(Rivest Cipher interpretation 6)Algorithm.The proposed algorithm ensures the encryption and decryption process using RC6 sluice cipher.The RGB pixel mapping is done using Hash- least significant Bit(HLSB) that makes use of hash function to develop a significant way securely store the data. For Security evaluations KSA, PRGA are used crucial generation and Modified LSB Algorithm for overwriting the LSB bits of the RGB pixel values in the named frame(given by the stoner) from the videotape.*

I. INTRODUCTION

Now a days internet has become major source to transfer information, online shopping, online rail reservation, online money transfer, online payment. But there is a major need to secure information in order to avoid the interception from an unauthorized interceptor/intruder. Steganography is the technique which is used to minimize this problem.

Steganography is a technique that has been used for centuries to conceal messages within other data. In recent years, with the growth of digital media, steganography has become increasingly important in the field of digital security. The goal of steganography is to hide information in a way that is not detectable by an observer who is not aware of the existence of the hidden data. This is typically accomplished by making small changes to the data that are not noticeable to the human eye or ear.

The major reason for using steganography is to maintain privacy and to prevent an unauthorized person from extracting information.. That means if we have to increase the capacity of secret data it will decrease the quality of stegovideo.The advantage of video steganography over other forms of steganography is that it allows for the transmission of large amounts of data in a single file. Video files can contain a vast amount of data, which can be utilized to conceal secret information. Moreover, video files can be easily transmitted over the internet or any other communication channel, making it an ideal choice for secure communication.

However, video steganography is not foolproof and can be detected by advanced algorithms and techniques. Therefore, it is essential to use robust and secure encryption algorithms such as RC6, AES, and Blowfish to protect the secret information from unauthorized access.

Overall, video steganography is an effective technique for secure communication and can be utilized in various fields such as military communication, digital watermarking, and medical imaging. The field of steganography involves the process of hiding messages or information within other data, such as images, videos, or audio files.

Video steganography has become increasingly important in recent years due to the growth of digital communication and the need for secure transmission of data. The technology is widely used in fields such as military communication, law enforcement, and digital watermarking.

In military communication, video steganography is used to transmit secret information over a secure channel without detection. The information can be hidden in the video file, and only authorized parties can extract it using the appropriate decryption key. This makes it difficult for attackers to intercept or tamper with the data during transmission.

In addition to these applications, video steganography can also be used in medical imaging to hide sensitive patient information in medical images, ensuring patient privacy and confidentiality.

One of the main challenges in video steganography is to ensure that the hidden information remains undetectable and does not affect the quality of the video. This requires a delicate balance between the amount of information that can be hidden and the degree of modification required to embed it.
Overall, video steganography is a powerful tool for secure communication and has a wide range of applications in

various fields. As technology advances, video steganography is likely to become even more important in ensuring the secure transmission of information over digital channels.

In this project, we explore the use of RC6 encryption algorithm for video steganography. The goal of this project is to implement a video steganography system that can securely hide information within a video file using RC6 encryption.

II. LITERATURE REVIEW

1.Hiding Data in Video Sequences using RC6 Algorithm - .YaminiPriya; K.Priyadharshini; K.Sowndharya; S.Swathi; K.Swetha, IJCSMC,2020.

In this paper , it focuses on the analysis of RC 6 Encryption and Decryption using LSB Technique.The binary representation of the each hidden data is used to overwrite the LSB of each byte within the encrypted image randomly.The simulation result is to indicate that the framework can be successfully used in Image data hiding applications.It is efficient and provides good accuracy.

2.A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector Ramadhan J. Mstafa; Younis Mohammed Younis; Haval Ismael Hussein; MuhsinAtto ,IEEE,2020.

Recent developments in the speed of the Internet and information technology have made the rapid exchange of multimedia information possible. These developments in technology lead to violations of information security and private information. Digital steganography provides the ability to protect private information that has become essential in the current Internet age. Among all digital media, digital video has become of interest to many researchers due to its high capacity for hiding sensitive data. Numerous video steganography methods have recently been proposed to prevent secret data from being stolen. Nevertheless, these methods have multiple issues related to visual imperceptibly, robustness, and embedding capacity. To tackle these issues, this paper proposes a new approach to video steganography based on the corner point principle and LSBs algorithm. The proposed method first uses Shi-Tomasi algorithm to detect regions of corner points within the cover video frames. Then, it uses 4-LSBs algorithm to hide confidential data inside the identified corner points.

3. A Survey on Different Video Steganography Techniques - J. Mary Jenifer; S. Raja Ratna; J.B. ShajilinLoret; D. Merlin Gethsy,ICOEI,2020.

Steganography is the method of hiding the secret message inside the data source. It not only keeps the information as secret but also the existence of the information is kept as secret. It is used in various fields such as defense, medical and online transactions. It is mainly used in secure communication. In steganography, the message can be hidden in carriers such as text files, images, audios, and videos. The aim of this paper is to provide a general overview of various video steganography techniques. It covers related works, the strength of steganography, types of steganography and different video steganography techniques. The comparative analysis of various video steganography techniques is also highlighted.

4. A secure video steganography with encryption based on LSB technique -
Pooja Yadav; Nishchol Mishra; Sanjeev Sharma ,IEEE ,2019.

Need of hiding information from intruders has been around since ancient times. Nowadays Digital media is getting advanced like text, image, audio, video etc. To maintain the secrecy of information, different methods of hiding have been evolved. One of them is Steganography, which means hiding information under some other information without noticeable change in cover information. Recently Video Steganography has become a boon for providing large amount of data to be transferred secretly. Video is simply a sequence of images, hence much space is available in between for hiding information. In proposed scheme video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. To enhance more security each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR.

III. EXISTING SYSTEM

The existing ways are substantially grounded onLSB(Least Significant Bit) where least significant bits of the cover train are directly changed with communication bits.

A significant number of styles have been proposed fo r LSB steganography. Masud et al has proposed a LSB fashion for RGB true colour image by enhancing the existing LSB negotiation ways to enhance the security position of retired information. Security is a veritably important part of IT diligence in day to day life and it's a fleetly growing area in the IT sector. Data hiding is one of the arising ways that give for security byhiding secret informat

ion into the multimedia contents by altering some factors in the host or cover train. Data hiding, Steganography and Watermarking are three nearly affiliated fields that have a great deal of imbrications and share numerous specialized approaches as private, nonpublic and secret data in ultramodern society.

IV. PROPOSED SYSTEM

The security of information communication and particularly pictures got to be a critical objective as the network is developing. The security of pictures is an vital inquire about field in diverse patterns like information security, secure information transmission and copyright security.

So, Picture encryption calculations and stowingaway calculations oughtto be planned to improve the viability of transmission and keep it more secure from assaults by the gatecrashers.

So, the proposed strategy can accomplish the most elevated level of information astuteness, secrecy and security.
In this extend we are attempting to confirm the privacy of grayscale picture that makes employments of pixel rearranging and RC6 stream cipher for cryptography and Hash-LSB for steganography.

RC 6 ALGORITHM:

RC6 is a symmetric key square cipher calculation that was outlined by Ron Rivest. It is an moved forward form of the RC5 calculation, which was discharged in 1994. RC6 is a symmetric key calculation that employments the same key for both encryption and decryption.

The RC6 calculation is a square cipher, which implies that it works on fixed-size squares of information. The estimate of the piece in the RC6 calculation is 128 bits. RC6 employments a variable-length key, which can be up to 2040 bits in length. The RC6 calculation is based on the Feistel organize structure, which is a sort of square cipher that employments a arrangement of rounds to change the data.

The RC6 calculation employments four parameters: w, r, b, and the mystery key. The w parameter indicates the estimate of the word in bits, which is 32 bits in the RC6 calculation. The r parameter indicates the number of rounds in the calculation, which is ordinarily between 16 and 32. The b parameter indicates the estimate of the key in bytes, which can be up to 255 bytes. At last, the mystery key is the key utilized for encryption and decryption.

The RC6 calculation has a few points of interest over other symmetric key calculations. One of the primary points of interest is its speed, which is comparable to other quick symmetric key calculations. Moreover, the RC6 calculation has a solid security profile, which makes it a prevalent choice for applications where security is a concern.RC6 calculation is a symmetric key square cipher that employments four registers, to be specific A, B, C, and D, to perform encryption and unscrambling operations. These registers hold a parcel of the cipher key, and they are utilized in combination with the plain content or cipher content piece to create a one of a kind output.

In rundown, the RC6 calculation is a symmetric key piece cipher calculation that employments a variable-length key and a Feistel arrange structure. It is a quick and secure calculation thatis broadly utilized in different applicatis, counting obsequious communication, e-commerce, and secure information capacity

HLSB TECHNIQUE :

HLSB INSERTION

The Hash Based Least Significant Bit Technique For Video Steganography deals with hiding secret message or information within a video.Steganography is nothing but the covered writing it includes process that conceals information within other data and also conceals the fact that a secret message is being sent.Steganography is the art of secret communication or the science of invisible communication. Hash based least significant bit technique for video steganography has been proposed whose main goal is to embed a secret information in a particular video file and then extract it using a stego key or password.
A hash function is used to select the particular position for insertion of bits of secret message in LSB bits.

LSB INSERTION

LSB (Least Significant Bit) Insertion is a steganography technique that involves hiding secret information in the least significant bits of an image or a video. The LSBs are the binary digits that carry the least weight in a binary number, and they are usually not visible to the human eye. This technique works by modifying the LSBs of the pixels in the cover image to embed the secret information. Since the modification is minimal, it is difficult to detect the presence of the hidden data by visual inspection.

COMPARING HLSB AND LSB

The hash based LSB technique is different from LSB technique on basis of hash function as the hash function hide eight bits of secret data on a time and hide them in LSB positions of RGB pixels of carrier frame the distribution of bits is of order 3,3,2 respectively and distributed in such a way that first 3 bits of the 8 bits secret message are inserted into R pixel and other 3 bits of secret message into G pixel and remaining 2 bits are inserted into B pixel. This bits are inserted into LSB position on basis of the returned value using hash function.As human eye has chromatic influence of the blue colour is more than the red and green colour hence this order of distribution takes place. In the LSB insertion technique, one can take the binary representation of the hidden data and overwrite the LSB of each byte in the cover file.The amount of change occurred in cover file will be minimal and not noticeable to the human eye.

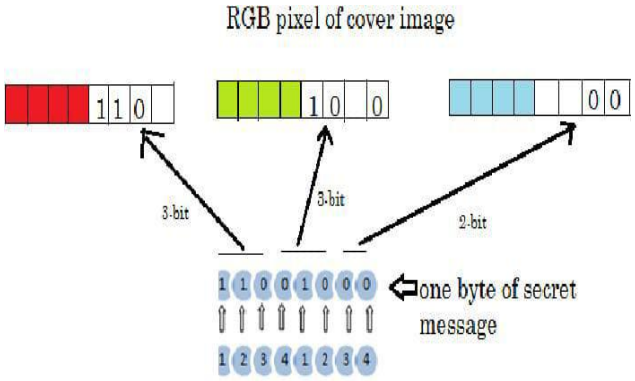

FIG 1 PROPOSED HASH BASED LSB EMBEDDING TECHNIQUE. SHOWS SECRET DATA EMBEDDED IN 4 BITS OF LSB IN 3,3,2 ORDER IN CORRESPONDING RGB PIXELS OF CARRIER FRAME

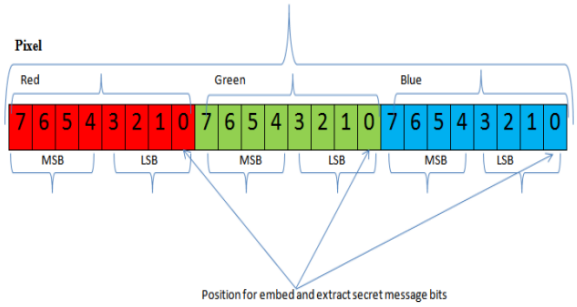

FIG 2 EXPLAINS THE SPATIAL OPERATION FOR HLSB

EXPLAINS THE SPATIAL OPERATION FOR HLSB

IMPLEMENTATION OF RC 6 :

In the context of video encryption, RC6 can be used to encrypt video content to prevent unauthorized access and protect the content from being stolen or tampered with. The encryption process involves breaking the video content into blocks of 128 bits and encrypting each block using the RC6 algorithm. The key used for encryption can be generated using a key scheduling algorithm, which initializes the key that will be used in each round of encryption and decryption.

The RC6 algorithm involves three stages: key scheduling, encryption, and decryption. In the key scheduling stage, the key is expanded and initialized to generate a set of subkeys that will be used in subsequent rounds of encryption and decryption.

In the encryption stage, each block of data is encrypted using the subkeys generated in the key scheduling stage. In the decryption stage, the encrypted data is decrypted by reversing the encryption process using the same subkeys generated in the key scheduling stage.

One advantage of using RC6 for video encryption is that it allows for a variable-length key, which means that longer keys can be used to enhance the security of the encrypted data. Additionally, RC6 is relatively fast and efficient, making it a good choice for encrypting large amounts of video data**.**

6.3 IMPLEMENTATION OF HLSB:

Hash Least Significant Bit (LSB) is a data hiding technique that involves the modification of the least significant bits of the cover image's pixel values to hide a secret message. The process involves two stages: embedding and extraction.

6.3.1 EMBEDDING:

- Convert the secret message to binary.
- Divide the binary message into equal-sized segments.
- Calculate the hash value of each segment using a hash function (e.g., MD5, SHA-1, SHA-256).
- For each pixel in the cover image, retrieve its least significant bit value and save it.
- If the hash value of the current segment is odd, set the pixel's least significant bit to 1. Otherwise, set it to 0.
- Repeat steps 4-5 for all segments of the message.

6.3.2 EXTRACTION:

- Retrieve the least significant bits of all pixels in the stego-image.

- Divide the bits into equal-sized segments.
- Calculate the hash value of each segment using the same hash function used in the embedding process.
- Compare each hash value with the original hash values stored during embedding to determine the binary value of each segment.
- Concatenate the binary values to obtain the secret message.
- It is worth noting that the hash LSB technique is susceptible to attacks such as statistical analysis and brute force attacks. Therefore, it is not recommended to use it for highly sensitive information. Additionally, the technique may introduce visible distortions in the cover image, making it less suitable for some applications.

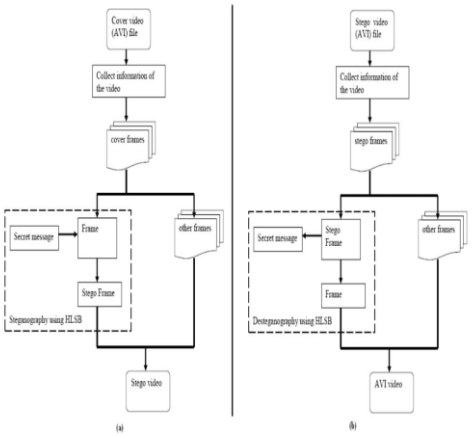

FIG 3 FLOW DIAGRAM

6.4 INTEGRATION OF RC6 AND HLSB FOR VIDEO STEGANOGRAPHY :

The integration of RC6 and HLSB (Hash Least Significant Bit) algorithm for video steganography encryption and decryption involves the following steps:

6.4.1 ENCRYPTION:

- Break the video file into frames and convert each frame into binary data.
- Generate a strong secret key using a secure random number generator.
- Use RC6 algorithm to encrypt the binary data frames using the secret key. This involves dividing the binary data frame into blocks, performing encryption rounds on each block, and reassembling the encrypted binary data frame.
- Generate a hash of the encrypted binary data frames using a hash algorithm such as SHA-256.
- Use HLSB algorithm to embed the hash into the video frames. This involves replacing the least significant bits of each pixel in the video frame with a bit of the hash value.
- Combine the video frames with the encrypted binary data frames into a single video file.

6.4.2 DECRYPTION:

Break the video file into frames and extract the hash value from the video frames using HLSB algorithm.

Generate a strong secret key using the same method used during encryption.

Decrypt the binary data frames using RC6 algorithm and the secret key. This involves dividing the encrypted binary data frame into blocks, performing decryption rounds on each block, and reassembling the encrypted binary data frame.

Generate a hash of the decrypted binary data frames using the same hash algorithm used during encryption.

Compare the hash values obtained from step 1 and step 4. If they match, the video has not been tampered with and the decrypted binary data frames can be used to reconstruct the original video frames.

Note that the specific implementation details of RC6 encryption and decryption and HLSB hiding can vary depending on the specific requirements and use case of the video steganography application. It is important to follow best practices for key management, data security, and integrity checking when implementing any encryption and hiding algorithm.

VI. RESULTS

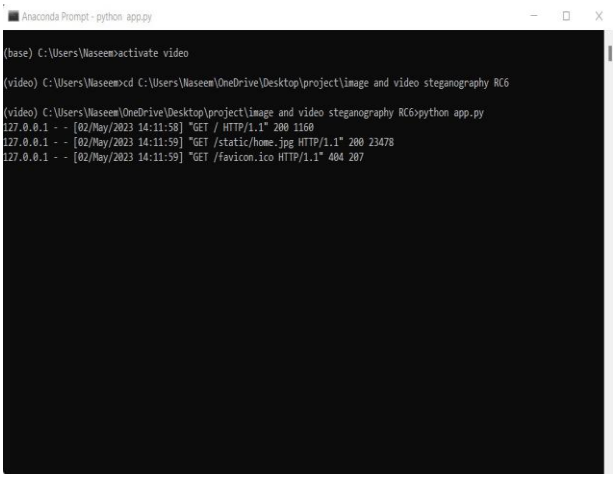

FIG 4 COMMANDS DISPLAYED IN ANACONDA PROMPT

FIG 5 HOME PAGE

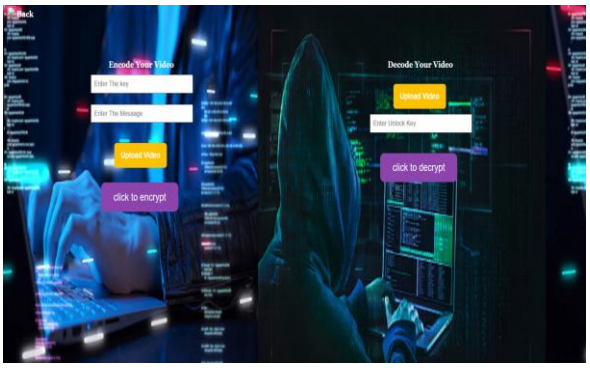

FIG 6 .USER INTERFACE

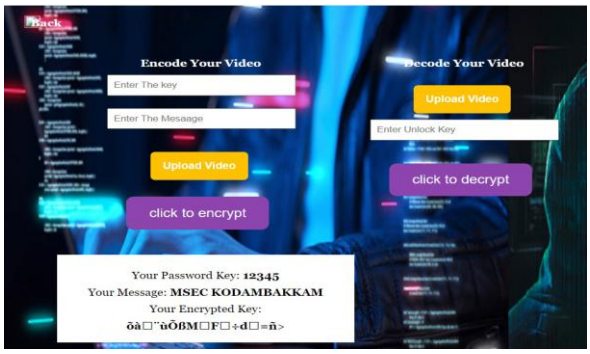

FIG 7 ENCRYPTION PROCESS

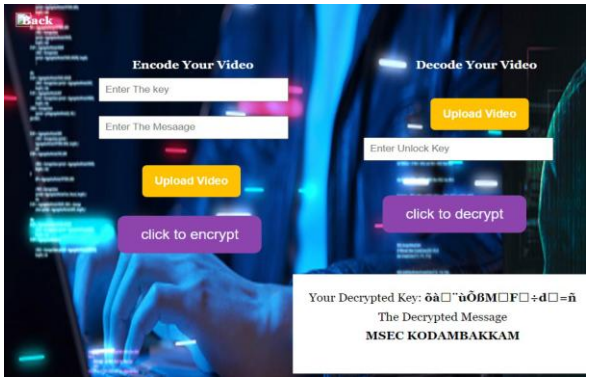

FIG 8 DECRYPTION PROCESS

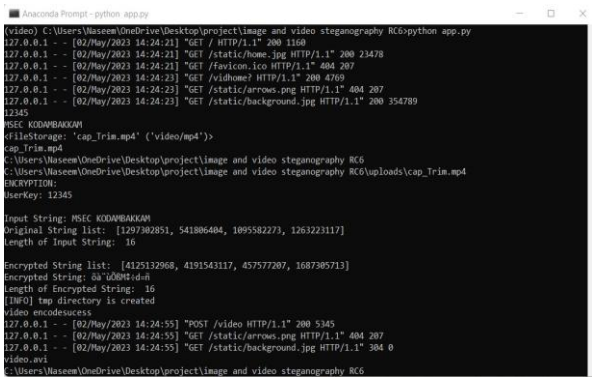

FIG 9 RESULTS DISPLAYED IN ANACONDA PROMPT

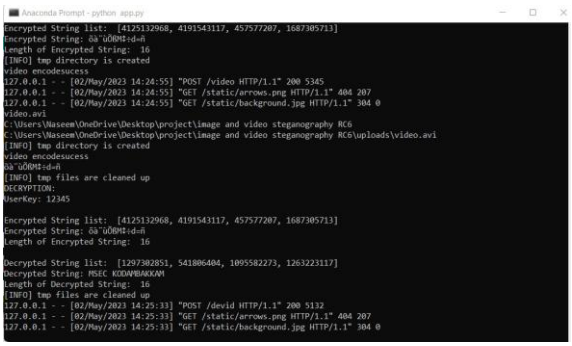

FIG 10 RESULTS DISPLAYED IN ANACONDA PROMPT

VII. CONCLUSION

Video steganography using RC6 encryption and hash LSB provides an effective way to hide secret messages within a video file while maintaining the video's original quality. RC6 encryption ensures the security of the hidden message by using a strong encryption algorithm that is difficult to break, while hash LSB provides a robust way to embed the message by utilizing the least significant bit of the pixel values.

However, it is important to note that while steganography can be used for legitimate purposes such as secure communication and copyright protection, it can also be used for malicious activities such as data theft and espionage. Therefore, it is crucial to use steganography responsibly and ethically.

Additionally, the effectiveness of steganography depends on various factors such as the size of the message, the complexity of the encryption algorithm, and the method of embedding the message. Thus, further research and experimentation are necessary to improve the performance of steganography techniques and make them more secure and reliable.

VIII. FUTURE SCOPE

Improving the efficiency and security of the algorithm: Researchers can focus on developing more efficient and secure techniques for RC6 encryption and embedding the secret messages. This would make the algorithm more robust and less susceptible to attacks.

Developing real-time steganography systems: Real-time video steganography systems can be developed for live video streaming applications. This would enable secure communication of confidential information over video conferencing platforms.

Enhancing the capacity of the algorithm: The capacity of the algorithm can be enhanced by developing more sophisticated techniques for embedding the secret messages. This would enable hiding larger amounts of data in a video file.

Integration with artificial intelligence: Researchers can explore integrating video steganography techniques with artificial intelligence to develop more advanced and intelligent steganography systems that can automatically adapt to different types of videos and encryption requirements.

Application in digital watermarking: Video steganography techniques can be applied to digital watermarking to protect digital content such as images, audio, and video files from piracy and unauthorized distribution.

Overall, video steganography using RC6 encryption has a significant potential for future advancements, which can lead to more secure and efficient methods of hiding secret messages within videos.

REFERENCES

[1] Jorg J. Buchholz, “Advanced Encryption Standard” http://buchholz.hs-bremen.de , December 19, 2019.
[2] PriyaPareshBandekar and Suguna G C, “LSB Based Text and Image Steganography using AES Algorithm” the International Conference on Communication and Electronics systems (ICCES 2018) IEEE Xplore Part Number: ISBN:978-1-5386-4765-3.
[3] Ramadhan J. Mstafa, Khaled M. Elleithy,andAbdelfattah, “A Robust and Secure Video Steganography Method in DWT- DCT Domains Based on Multiple Object Tracking and ECC”.
[4] ShumeetBaluja “Hiding Images in Plain Sight : Deep Steganography” 31st Conference on Neural Information Processing Systems NIPS 2017.
[5] SofyaneLadghamChikouche and NoureddineChikouche, “An Improved Approach for LSB-Based Image Steganography using AES Algorithm” The 5th International Conference on Electrical Engineering – ICEE-B October 29- 31, 2017.