HYBRID SCHEME OF INFORMATION HIDING USING CRYPTOGRAPHY AND VIDEO STEGANOGRAPHY (IHCVS)

[1]Dr. Sumathy Kingslin, [2]R.Saranya,
[1]Associate Professor, [2] M.Phil Research Scholar,
[1,2]PG & Research Dept. of Computer Science,
[1,2]Quaid-E-Millath Government College for Women (A), Anna Salai, Chennai 600002, Tamil Nadu, India

Abstract : In recent years, security is a complicated task in the transmission medium due to the rapid development of multimedia contents such as image, video, audio over the network. Nowadays many security aspects are available to protect the information from the people who have malicious intentions. Cryptography, Steganography and Digital watermarking are most commonly used techniques for protecting the secret and sensitive information. This paper presents a new hybrid scheme for protecting the text message during transmission over the network. In this hybrid scheme, a combination of three symmetric key encryption algorithms are used for the encryption process and video steganography is used for hiding process. The proposed hybrid scheme is evaluated based on the payload capacity and CER value for the quality of stego-video that provides authentication and validation.

Index Terms **- Hill Cipher, AES, Thrice Columnar Transposition Cipher, Video Steganography**

I.INTRODUCTION

Internet has become the most effective and fast media for digital communication due to a rapid development of technology. At the same time the growth and easy access to the internet makes the digital information reach unauthorized hands [1]. Information Security (IS) is designed to protect the confidentiality, integrity and availability of digital information from those with malicious intentions. Therefore, securing the information is one of the most challenging aspects in digital communication. Confidentiality, integrity and availability are sometimes referred as the CIA triad to information security. Confidentiality is achieved by protecting information from being disclosed to unauthorized parties. Integrity is to protect information from being modified through unauthorized parties. Availability is the access to information to the right when requested [12]. There are many different information security techniques put to practice are some of them Cryptography, Digital Watermarking, Steganography, Digital signatures.

The various sensitive information like banking transactions, credit card information, user profile are being transferred over internet. To protect this kind of data from being hacked and eavesdropped, there is a dire need for security, secrecy and privacy. Cryptography is one such method widely practiced to protect confidential information being sent via insecure network Cryptography is an art and science of converting original message into non-readable form. There are various cryptographic algorithms that are being practiced from simple to complex in nature with each day a new method being evolved. Cryptographic algorithms are classified into three type secret key cryptography, public key cryptography and hash function based on how key is used for the process. Steganography is the art and science of hiding information by embedding data into media [2]. Steganography means “covered writing”. Generally steganography is known as “invisible” communication [3]. Steganographic techniques have been used for centuries even before the cryptographic systems were developed. Steganography is classified into five different categories based on the cover medium used to conceal the secret information. They are Text, Image, Audio, Video and Network Steganography.

II.LITERATURE REVIEW

Many researchers have implemented various approaches for information security to achieve secret and secure communication. Studying the results and the performances of various encryption and steganographic algorithms can give an idea to implement the new methodology for protecting the information from the intruders as well as attackers.

Amandeep Kaur et al. proposed a hybrid technique of cryptography and watermarking for data encryption and decryption. This scheme also analyzed the performance of one bit LSB, two bit LSB and three bit LSB. This hybrid scheme is based on five encryption algorithms and one of the spatial domain techniques of steganography. In this literature the message was divided into five segments. The segmentation key is avoided in this scheme. First segment of the message was encrypted using Fibonacci series. Second segment was encrypted using XOR cipher. The third segment was encrypted PN sequence. Fourth and fifth segment was encrypted using RSA and Hill cipher. Public and private key is used for the encryption and decryption process. The encrypted message was hided inside an image using one bit LSB, two bit LSB and three bit LSB. Quality of the watermarked image was evaluated using PSNR, RMSE and MSE. The PSNR value for the LSB is high when compared to the existing methods. When compared to the existing hybrid technique this scheme was increased the security. But time density and

complexity one of the drawbacks of this scheme. LSB is simplest technique among all but cannot be considered as a good technique in terms of security because the data from the stego-image can be easily retrieved [4].

Muhammad Khaerul Anam et al. proposed a Random Pixel Embedding for Hiding Secret Text over Video File. In this methodology the information is hidden in the video using Random pixel embedding method. Random pixel embedding method is the Least Significant Bit modified by utilizing the Random Number Generator function. Quality of the stego video is evaluated using Signal to Noise Ratio (SNR) and the process experiment is evaluated using Character Error Rate (CER) parameter. In the first, fourth, fifth, sixth, ninth, twelfth and thirteenth experiments CER is not equal to zero because one character was damaged [5].

Himanshu Wadekar et al. proposed a new approach to video steganography using pixel pattern matching and key segmentation. In this methodology modified AES is employed for encrypting the secret message. The encrypted message is converted in the form of Quotient, Remainder and Divisor using the Division method. Finally the pixel pattern matching method is used for embedding the quotient, remainder and divisor into the random frame of a video file. Address of the embedded pixel stored in different frames using key segmentation method. Initial size of video file 5.210 KB is taken in the proposed methodology. Up to embedding 2,00,000 characters there is no difference between the original and stego video. When embedding 3,50,000 characters 0.001 KB is increased. Finally this methodology gives a remarkable approach of covering data in a video with negligible bit distortion [6].

Aarti Mehndiratta et al. proposed A New Hybrid Scheme to Improve Security for Digital Message. The Secret message is encrypted using 128 bit AES algorithm. The cover medium is divided into several frames. Encrypted message is embedded inside the frame using transform domain DCT technique. In this methodology image is taken as the secret message. Finally PSNR value is calculated for evaluation process. PSNR value 40.412 db is obtained. This methodology gives better PSNR value when compared to the existing methodology [7].

III.PROPOSED WORK - IHCVS

The proposed methodology IHCVS enhances the security by combining the techniques of cryptography and steganography. Each encryption technique in cryptography has its own strong and susceptible points. When compared to asymmetric key encryption techniques, the symmetric key encryption techniques have the advantage of not consuming too much of computing power and it works with high speed in encrypt them [11]. In the video steganography random block method will provide best embedding capacity [5]. Thus based on the merits of symmetric key encryption techniques and random block method a new methodology has been proposed which will provide better security enhancement in encrypting the secret message. At the sender's side, the secret text is encrypted using the three versatile and powerful symmetric key algorithms and the cipher text is hidden under video steganography. The reverse process of extraction of cipher from the cover video and decryption of cipher to plain text happens at the receiver's end. The process is clearly explained in the diagram given below. The IHCVS methodology at sender's side is as shown in figure 3.1.

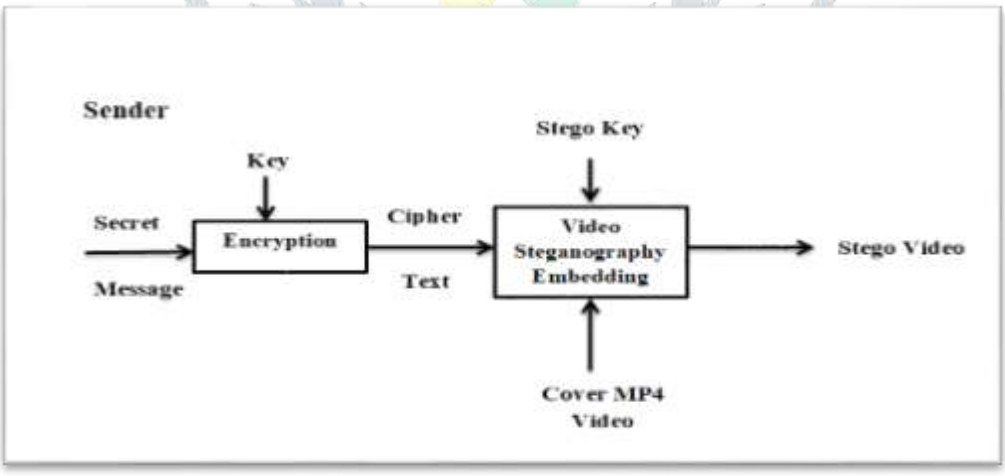

Fig. 3.1 IHCVS - Sender Side

The extraction of plain text at the receiver's end is explained in figure 3.2

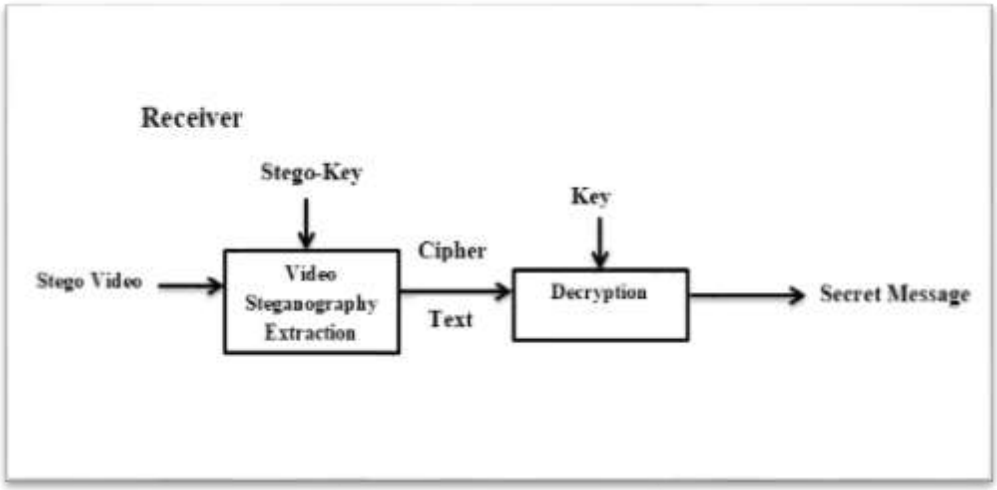

Fig.3.2 IHCVS - Receiver Side

The receiver can extract the cipher text from the stego video and decrypt the cipher text to know the secret message using the same keys used for encryption and embedding during transforming the plaintext at sender's side.

3.1. Encryption - Embedding of IHCVS Methodology

The steps to encrypt the secret message using symmetric key encryption algorithm to receive the input for embedding process is given below

IHCVS Encryption Process

Input : Secret Message (S), Secret Key (K1, K2, K3) **Output : Cipher Text (C)**	
I.	Divide the secret message S into three segments S1, S2 and S3.
II.	S4 ← E (S1, K1) using the Hill Cipher
III.	S5 ← E (S2, K2) using the AES.
IV.	For i=1 to 3 do S6 ← E (S3, K3) using the Thrice columnar transposition cipher.
V.	C ← Integrate (S4+S5+S6)
VI.	Return C.

3.1.1. Encryption using Hill Cipher

The Hill cipher is a polygraphic substitution cipher using linear algebra. In the Hill cipher one unique number, from 0 to 25 is alerted to each letter of the secret message. The first part of the message was encrypted using Hill Cipher. Messages are divided into n-letter blocks. Encryption process is performed by multiplication of all the blocks of encrypted message by one n x n secret matrix. All the results should be modulo 26. In the Decryption procedure one has to divide the cipher text into blocks and multiply them via the inverse of the key matrix modulo 26 [8]. The inverse of the key matrix is calculated as follow

$$\mathbf{Key^{-1} = d^{-1} * adj(Key)} \quad \ldots. \ (3.1)$$

3.1.2. Encryption using AES

The AES (Advanced Encryption Standard) algorithm is very powerful and faster when compared to the DES and triple DES. It encrypts data blocks of 128 bits in 14, 12 and 10 round depending on key size. In the proposed method middle segment of the message was encrypted using AES. Each encryption process needs four type of operation to alter the state of array.

- Shift Rows - Each row is rotated to the right by a certain number of bytes.
- Mix Columns- To produce a new column, each column of the state array is processed separately. The old one is replaced by new column.
- Sub Bytes - This operation converts every bit into a different value so this is the simple substitution.
- XOR Round Key- This operation takes the existing state array

To encrypt a 128-bit block the following steps as used.

1. First the set of round keys are derived from the cipher key.
2. Initialize the state array with the blocks of plaintext.
3. To starting state array add the initial round key
4. Perform nine rounds of state manipulation.
5. Perform the tenth and last round of state manipulation.
6. At the end the final state array is copied as the cipher text [13].

3.1.3. Encryption using Thrice Columnar Transposition Cipher

The Columnar transposition cipher is a rearrangement of the characters of the plaintext into columns. The order of the columns then will become the important thing to the algorithm. The order of the columns is considered as a key. In the proposed methodology the last part of the secret message was encrypted using columnar transposition cipher. For the security concern the message was encrypted for three times [9]**.**

3.1.4. Embedding Process

One of the common and the simplest approach to embed information in a video file is the random block technique. In this technique the video is divided into the number frames. Encrypted message is hided in a random block of the frame so the human eye would be unable to notice the hidden message in the covered video. Steps for embedding a secret message in a video is given below

IHCVS Embedding Process

Input : Cipher Text (C), Stego Key, Cover video file (CV), Position (P), Embedded Block(EB) **Output : Stego video file (SV)**	
I.	Split the CV into frames.
II.	Divide the frames into blocks of the cover frame
III.	For I= 1 to N Do P← Get the position from the random block EB ← Hide(C, P) using Stego Key
IV.	SV ← Regenerate (EB ,video frames)
V.	Return SV

3.2. Extraction - Decryption of IHCVS Methodology

The extraction and decryption process is performed at the receiver side. The encrypted message is obtained in the extraction process and original secret message is obtained in the decryption process.

3.2.1. Extraction Process

The stego-video is sent to the receiver through communication media like gmail etc. The receiver can download the stego video. When the receiver enters the appropriate stego key the encrypted message is displayed. The steps to extract the encrypted message from the stego video to receive encrypted message as an output is given below

IHCVS Extraction Process

Input: Stego- Video File (SV), Stego Key, Position (P), Embedded Block (EB), Blocks (B) **Output: Cipher Text (C)**	
I.	Split the SV into frames.
II.	Divide the frames into the block.
III.	For B = 0 to N Do Check EB P← Get the position from the EB
IV.	C← Extract (P) using Stego Key
V.	Return C

3.2.2. Decryption Process

Decryption is the process of converting cipher text data into original plain text something that appears to be meaningful. When the key is longer, it is more difficult to decrypt every piece of cipher text without possessing the key. The power of the

decryption algorithm is based on the key. The steps to decrypt the encrypted message using symmetric key encryption algorithm to receive the secret message as an output is given below.

IHCVS Decryption Process

Input : Cipher Text (C), Secret Key (K1, K2, K3) **Output: Secret Message (S)**	
I.	Divide the Cipher Text C into three segments S6, S7, S8
II.	S1 ← D (S6, K1) using the Hill Cipher.
III.	S2 ←D (S7, K2) using the AES.
IV.	For i=1 to 3 do S3← D (S8, K3) using the Thrice Columnar Transposition Cipher.
V.	S← Integrate(S1+S2+S3)
VI.	Return S

IV. RESULT AND ANALYSIS

NetBeans is the best platform for developing java desktop applications and also it is open source integrated development software so the proposed IHCVS methodology used the NetBeans IDE 7.3.1 for implementing methodology. The Microsoft SQL server is the database used for storing the stego video. The Experimental result of the proposed IHCVS methodology is based on the difference between the original and extracted message and the stego video.

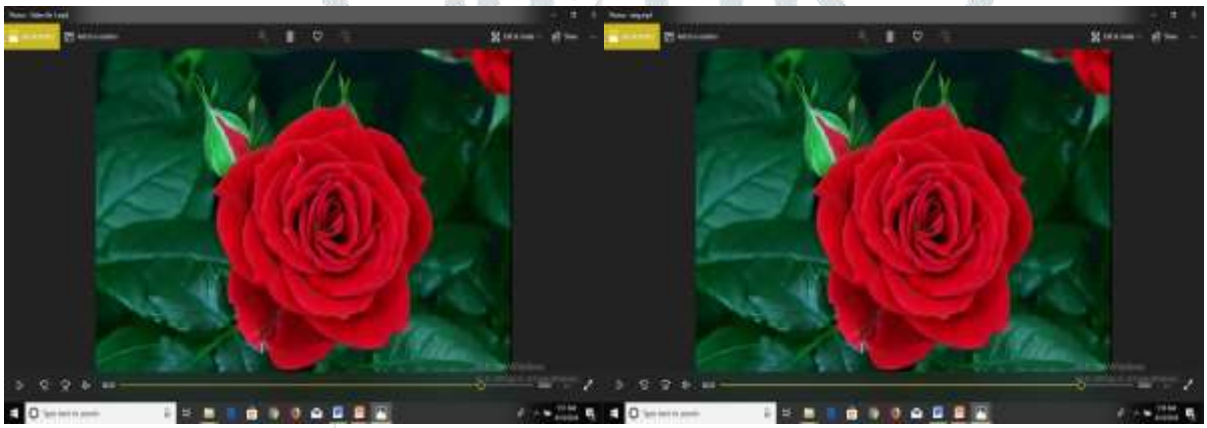

Fig.4.1 Difference between original and stego video at 20 sec

4.1. Pay load Capacity

One of the important performance parameter for the direct impact on the robustness of the video is the payload capacity. Payload Capacity is also referred as the embedding capacity. Payload Capacity is quantity metric of the steganography. The payload capacity corresponds to the secret message and pixels of the cover frame. It can be calculated as follows

$$Payload\ \ Capacity = \frac{Bits\ of\ the\ secret\ message\ embedded}{No\ of\ \ pixels\ of\ cover\ frame} \quad \ldots (4.1)$$

Table: 4.1 Comparison of payload capacity of the exiting methodology with proposed IHCVS

Total number of characters in Secret Message	Existing Methodology (in MB) [6]		Proposed IHCVS Methodology (in MB)			
	Original Video Size	Stego Video Size	Original Video Size	Stego Video Size	Original Video Size	Stego Video Size
1,00,000	5.210	5.210	5.210	5.210	4.382	4.382
2,00,000	5.210	5.210	5.210	5.210	4.382	4.382
3,50,000	5.210	5.211	5.210	5.210	4.382	4.382

4,00,000	-	-	5.210	5.210	4.382	4.383
5,00,000	-	-	5.210	5.211	4.382	4.384

In the table 4.1 the payload capacity of the video is not changed up to embedding 2,00,000 characters of secret message in the existing methodology. When embedding 3,50,000 characters, the size of the video was increased from 5.210 MB to 5.211 MB in the existing methodology. In the proposed IHCVS there is no change up to embedding 3,50,000 characters. When embedding 4,00,000 and 5,00,000 characters there is slight size change between the original and stego video.

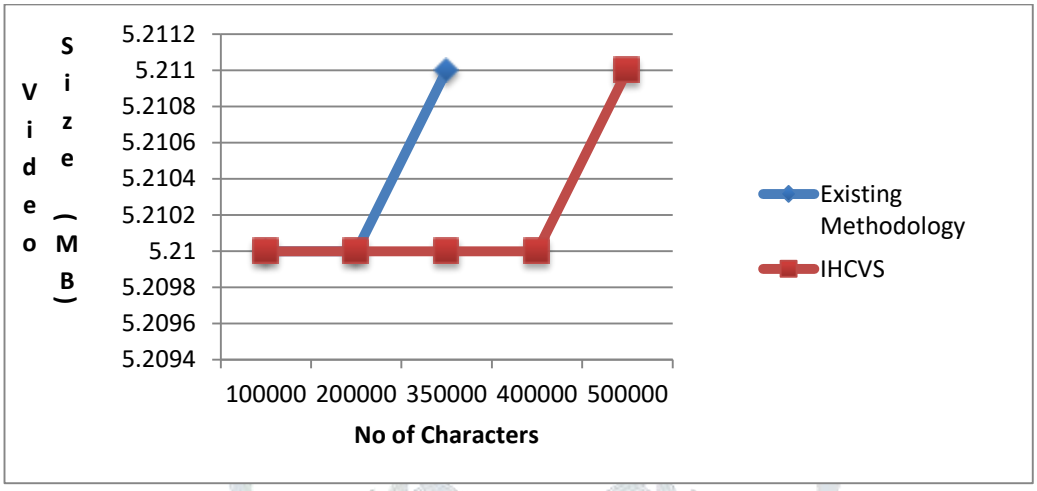

Fig.4.2 Comparison of payload capacity of the proposed IHCVS with existing methodology

4.2. CER

CER is the text similarity measure. This parameter can evaluate the text similarity between the original and extracted message. CER is calculated to know how many characters are corrupted during the application processing.

The CER can be calculated as follows

$$CER = \frac{Sum\ of\ character\ errors}{Sum\ of\ total\ characters} \quad \ldots \quad (4.2)$$

When the CER=0 means there is no characters are corrupted during the application processing [5]. Similarity is measured using CER. In the table 6.6 shows the character error rate comparison between the existing and proposed IHCVS methodology.

Table 4.2 Comparison of the CER between the existing and IHCVS methodology

Experiment Number	Existing Methodology[5]	Proposed IHCVS Methodology
1	0.0588	0
4	0.0556	0
5	0.0102	0
6	0.0417	0
9	0.0651	0
12	0.0486	0
13	0.0509	0
16	-	0
17	-	0
18	-	0.016
19	-	0.023
20	-	0.025

In the table 4.2 CER for the first fourth fifth sixth ninth thirteenth are not equal to zero because some characters can be corrupted during the existing methodology.

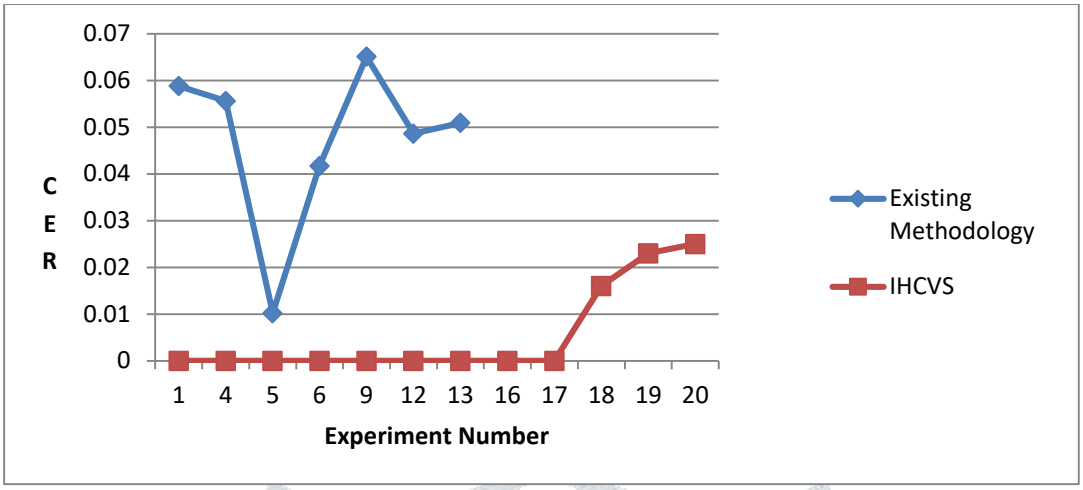

Fig.4.3 Comparison of CER of the proposed IHCVS methodology with existing methodology

In the Figure 4.3 shows the comparison of CER between the proposed IHCVS methodology and the existing methodology. In the IHCVS methodology from 1 to 17 experiment CER=0 therefore no character were not corrupted. In the eighteenth, nineteenth and twentieth experiments only some characters were corrupted.

V. CONCLUSION

Due to the rapid development and speed of internet and more advances in technology, people are turning out to be stressed more because their valuable data being hacked by malicious intruders. No single algorithm is sufficient for providing the security so the proposed methodology used the three different kind of symmetric encryption algorithms namely Hill Cipher, AES and Columnar transposition cipher for encrypting the message. Random Block method of video steganography is taken to hide the encrypted secret message. The proposed IHCVS methodology is the best methodology for hiding large amount of data when compared to the Pixel pattern matching method. The size of the video in the IHCVS methodology is not changed up to 3,50,000 characters but in the pixel pattern matching method the size of the video is changed when embedding 3,50,000 characters. The embedding capacity is also increased from 3,50,000 characters to 5,00,000 characters and the size of the video is also decreased. The proposed IHCVS is the best methodology for the text similarity measure because the number of characters corrupted between the original and extracted message is zero up to 17 experiments. In the random pixel embedding methods the characters are corrupted that is the CER value is not equal to zero for some of the experiments. The proposed IHCVS methodology is the best methodology for text similarity measure and hiding large amount of data. So the proposed IHCVS is efficient and effective way for secure communication over network channel.

REFERENCES

1. Han-ling∗ZHANG et al. “Image Steganography using Pixel-Value Differencing”, Second International Symposium on Electronic Commerce and Security, Pp.109-112, 2009.
2. Jayaram et al. “Information Hiding Using Audio Steganography – A Survey”, The International Journal of Multimedia & Its Applications (IJMA), Vol.3, No.3, August 2011.
3. Vipula Madhukar Wajgade et al. “Enhancing Data Security Using Video Steganography” International Journal of Emerging Technology and Advanced Engineering Website, Volume 3, Issue 4, April 2013.
4. Amandeep kaur et al. “A Hybrid Technique of Cryptography and Watermarking for Data Encryption and Decryption”, 2016 Fourth International Conference on parallel, Distributed and Grid Computing(PDGC) , 978-1-5090-3669-1/16, 2016.
5. Muhammad Khaerul Anam et al. “Random Pixel Embedding for Hiding Secret Text over Video File”, 1st International Conference on Informatics and Computational Sciences (ICICoS), 978-1-5386-0903-3/17, 2017 IEEE.
6. Himanshu Wadekar et al. “ A new approach to video steganography using pixel pattern matching and key segmentation”, International Conference on Innovations in information Embedded and Communication Systems (ICIIECS), 978- 1-5090-3294-5/17, 2017
7. Aarti Mehndiratta et al. “ A New Hybrid Scheme to Improve Security for Digital Message”, Proceedings of the International Conference on Inventive Computing and Informatics (ICICI 2017) IEEE Xplore Compliant - Part Number: CFP17L34-ART, ISBN: 978-1-5386-4031-9, 2017
8. William Stallings “Cryptography and network security principles and practice”, fifth edition , 2006 Pearson Education, Inc., publishing as Prentice Hall.

9. Malay B. Pramanik "Implementation of Cryptography Technique using Columnar Transposition", International Journal of Computer Applications (0975 – 8887) Second National Conference on Recent Trends in Information Security, GHRCE, Nagpur, India, Jan-2014.
10. Sumathy Kingslin, Saranya," Evaluative study on Substitution and Transposition Cipher " published in the International Journal of Creative Research Thoughts (IJCRT), Volume 6, Issue 1, January 2018.
11. Priyadarshini Patila et al. "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.
12. https://www.infosec.gov.hk/english/information/what_icana.html#c
13. http://etutorials.org/Networking/802.11+security.+wi+protected+access+and+802.11i/Appendixes/Appendix+A.+Overview+of+the+AES+Block+Cipher/Steps+in+the+AES+Encryption+Process/