Video Steganography using Concept of DNA Sequence and Index Compression Technique

Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, Vineet Kumar Singh

Abstract*: Cryptography is the process to secure sensitive information through the means of implementing security algorithms. Cipher text that is generated as output after algorithm implementation can be read only by authorized and authenticated persons after converting it into plain text. It is believed by security practitioner that cipher text is difficult to decrypt if reverse procedure plus key is unknown. Steganography on the other hand is the method of hiding sensitive information into carrier medium in such a fashion that its presence cannot be detected by unauthorized persons. . Metamorphic cryptography is the fusion of these techniques, cryptography and steganography. In paper presented, metamorphic cryptography concept is implemented. DNA (Deoxyribonucleic Acid) based cryptography is implemented to achieve cryptographic strength. Plaintext message which contain sensitive information is converted into its corresponding ASCII values. Obtained ASCII values is then changed into corresponding binary values. Apply binary index compression technique. Applying compression technique reduces data up to 50% which improves payload capacity. Output of the above steps is converted into sequences of DNA nucleotides. Concept of steganography is implemented with the help of LSB algorithm. Proposed metamorphic algorithm is secure as it utilizes the concept of DNA, have higher payload capacity as it uses binary index compression technique and simple to implement as LSB algorithm is used for hiding purposes.

Index Terms*: Metamorphic cryptography, DNA Sequence, DNA nucleotides, binary index Compression LSB and Steganography, Technical steganography.

I. INTRODUCTION

A. *Cryptography*

Cryptography is the process to convert secret message into secret codes i.e. cipher codes. Cipher text is believed unbreakable by unauthorized user if reverse procedure and decrypting key is unknown. In cryptography, encrypting/decrypting algorithm and key value play very important role. Some security experts focused on nano-cryptography system to make their secret message more secure. Some scientist think Bio-cryptography is the best option to ensure security into the system. Bio-cryptography (bimolecular computers, DNA computers) now a day's considered as one of the growing multidiscipline concept which harvest both, concepts of biometrics with cryptography. In addition to its advantages of biometrics with cryptography, it plays very important role to protect against attacks (biometric system). Biometric concept can be considered as technology or sciences which investigate and evaluate the biological data. This biological data is used for acceptance and labeling some features, but now it is used for authentication purposes. The individual features or characteristics is stored in the database using appropriate input devices, which is used in further comparison with the features extracted from the traits of the individual need to be identified. This kind of technique plays very crucial role in term of security requirement. The biometric system have a lots of benefit over traditional considered systems such as: they cannot be theft or lost or guessed. It is very convenient to send and receive data through digital, no need to remember or carry, and are more affectionate, where its adaptability creates easy to handle approach. It can be used with its own or can mixture with other security and authentication methods. DNA cryptography is a recent technology, which contains essential feature deoxyribonucleic acid (DNA). Security experts have done some extra work on DNA cryptography to resolve some issue to make a system which is resistant to popular attacks like brute-force attacks, dictionary attacks, etc.

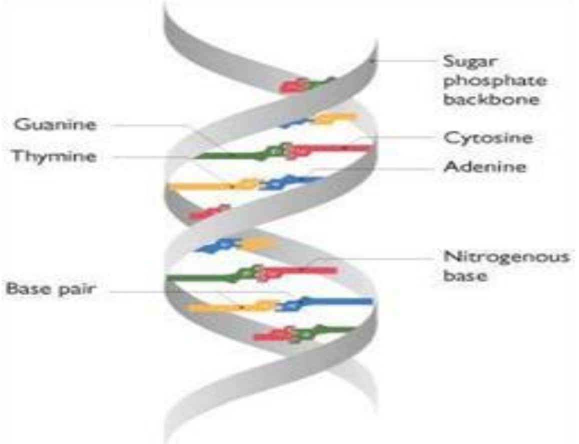


Figure 1. DNA system

Manuscript published on 30 June 2019.
***** Correspondence Author (s)

Pooja Dixit*, Computer Science and Engineering Department, ABES Engineering College, Ghaziabad, India.
Munesh Chandra Trivedi, Computer Science and Engineering, NIT, Agartala, India.
Avadhesh Kumar Gupta, Information Technology, IMS, Ghaziabad
Virendra Kumar Yadav, Computer Science and Engineering, ABES Engineering College, Ghaziabad, India.
Vineet Kumar Singh, Informaion Technology, Dr. RML Avadh University, Ayodhya, India

The method of using DNA computing in terms of metamorphic cryptography has been recognized as a possible automation that may lead ahead a new rise to create un-hack able secure algorithms. Strands of DNA are long polymers of numbers which may be in millions of linked nucleotides.

These nucleotides consist of one out of the four bases of nitrogen, a phosphate group & five carbon sugar. The nucleotides that make up these polymers are named after the nitrogen base. It contains Adenine (A), Cytosine (C), Guanine (G) and Thymine (T).

Following few points of advantages are: -

- Speed: Traditional computers can execute approximately 100 MIPS (millions of instruction per second).
- Storage Requirements (minimal): Density of DNA, consider memory stores of about per cubic nanometer for one bit where regular storage media need 1012 cubic nanometers to store one bit. Medium of Ultra-compact Information storage: huge amounts of data that can be stored in compact volume. A gram of DNA contains 1021 DNA bases = 108 Terabytes of data. Some quantity in terms of grams of DNA may hold all data stored in the world.
- Minimal Power Requirements: Power is minimally required for DNA computing at the computation time. Some slots of DNA which are built from chemical bonds held without require any outside power source. There is no need to compare power of DNA computing with regular computers.

B. *Steganography*

After encrypting our plain text with DNA cryptographic procedure, steganography have been performed. Steganography word is the combination of two Greek word’s "stego" and "graphia". Stego means "cover" and grafia means "writing". Staganalysis is a technique to examine the existence of steganography generally practiced by staganalyst. Steganography is an approach for hiding the information or plain text into carrier medium or hiding one form of information into another form of information. Steganography is the method of secret communication generally known for creating less suspect as its beautiful feature. It provides mechanism which encode information in particular manner that ensures presence of information invisible. In this process original file is called cover file and after hiding information on that cover file is called stego file. To hide the secret information there is need of stego-key for encoding and decoding the information (secret message). In this system scenario, first select appropriate hiding medium (i.e. Text, Image, Audio/Video or Protocol). Some steganography algorithm are also available but approach is always need to select more efficient algorithm that is able to encode information in secure manner.

Medium of Steganography

There are many types of steganographic method which are now a day’s practiced to cover the sensitive information.

- Technical Steganography: This is used technically as its name pronounced. It uses some special tools, devices or technical method for hiding the information. It can be use of microdots, secret ink, computer based techniques or many hiding medium to keep information secret.
- Cover: The cover defines the medium, where information can be hidden commonly known as information carrier. Carrier could be image, text, audio, video etc. The cover is divided into blocks, in each block, hide some bit of message. Here information is hidden by changing the various properties. If message block size is zero then there is no need to change cover block.
- Text Steganography: In this method the cover text is explain by changing words within a text, arranging the formatting of an existing text to hide the message, generating character sequences which are random in nature, or by utilizing the concept of context free grammar.
- Image Steganography: This technique is most popular than other steganographic technique. Bulk of e-image information is present on internet, that are generated from digital devices such as from digital cameras s. Mostly image contain some type of noise within itself . Noise refers to the defect inherent in the procedure of rendering an analog picture as digital image. In this type of steganography message is hidden in pixels of an image. In this secret communication scheme, hide secret message in a digital image using some hiding procedure. Another end or receiver can regenerate the original plain text from the stego image by decoding procedure. Original image is called carrier image and image obtained after hiding message into carrier image is called stego- image. There are some methods available to hide the secret information such as Data hiding, Data embedding and Data extracting method.
- Audio Steganography: In this type of stego procedure message is covered using audio as cover medium.
- Video Steganography: Is the method for hiding secret information inside a video. Addition of the secret sensitive plain text (secret information containing message) inside a video is done in such a fashion that it is unrecognizable by the human's eye. This can be achievable because some negligible changes of the color of the pixel. In video steganography first extract the frame. This frame is chosen randomly to ensure the security characteristics i.e. confusion. Hide the secret message into this randomly selected frame. This stego frame is again placed in its correct location and video is reconstructed. Check the integrity of the video before sending to other side i.e. receiver. It is now ready to send to receiver side. Original video is recognized as cover video and message containing video is called stego video.

The Objective of the paper presented is to study and analyze various problems solving model of DNA computing Idea is to develop the efficient metamorphic cryptographic algorithm.

Lots of DNA Computing model and video steganography approaches have been developed but separately. Some of the problems are problem specific like: [Aldeman, 1994], that compared with electronic computers, these model show potential advantage to solve difficult problem. The technology for DNA computer is work in progress. It is clear that molecular computers have

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)
© Copyright: All rights reserved.

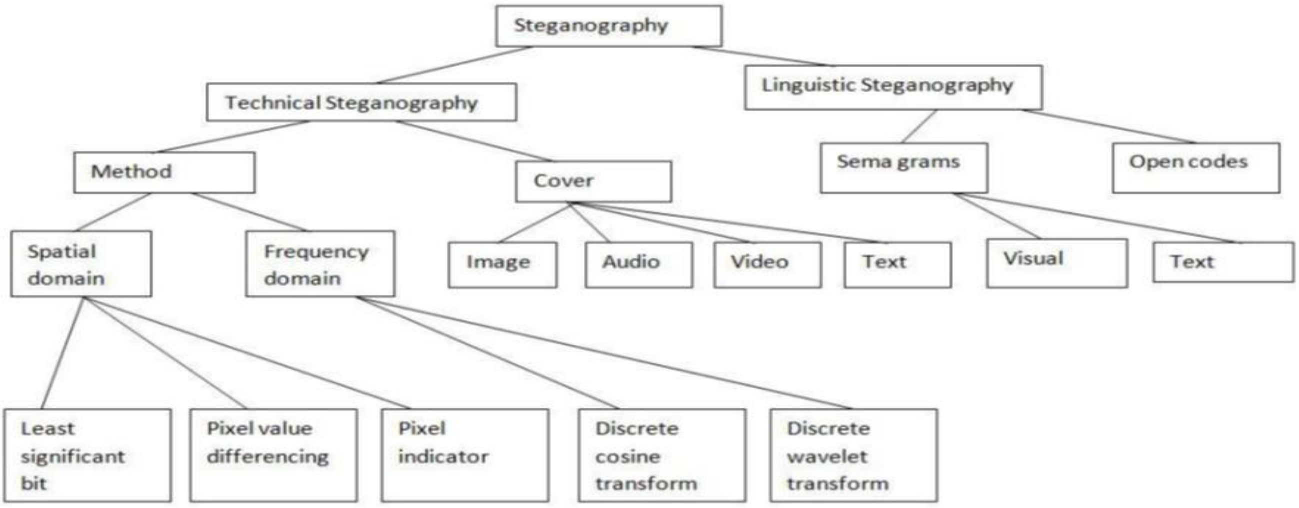


Figure 2. Types of Steganography

more specific properties. Paper presented proposes the combination of DNA sequence for encrypting purposes along with LSB approach to provide steganographic security strength to provide more efficient and secure communication. DNA sequence with binary indexed compression technique increases the payload capacity of proposed algorithm.

II. SYSTEMATIC LITERATURE SURVEY

Sherif T. Amin proposed YAEA (Yet Another Encryption Algorithm) encryption algorithm which is based on DNA. . In his research author describes about this technique which uses search technique to establish and coming with location of quadruple DNA nucleotides sequence that represent binary octet of plaintext (characters).

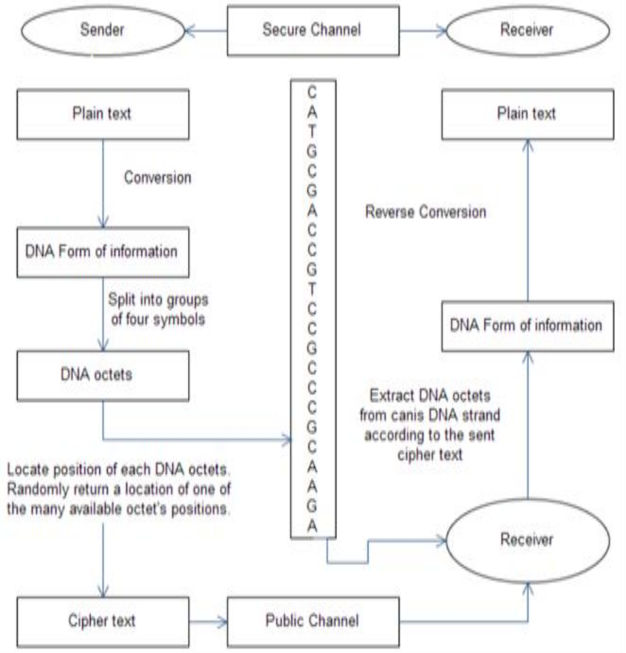

Sender
Secure Channel
Receiver
Plain text
Conversion
DNA Form of information
Split into groups of four symbols
DNA octets
Locate position of each DNA octets. Randomly return a location of one of the many available octet's positions.
Cipher text
Public Channel
C A T G C G A C C G T C C G C C C G C A A G A
Plain text
Reverse Conversion
DNA Form of information
Extract DNA octets from canis DNA strand according to the sent cipher text
Receiver

Figure 3. The Computational graph of single YAEADNA

In this paper data preprocessing means plaintext which is actually secret text is first converted into binary form. The binary form resulted as output from first step is converted into DNA encoding. In second step, generate secret key NCBI (National Center for Biotechnology Information) that is the master bank of human genome which has length equal to 256. After performing above steps successfully, follow encryption process through secret key based on vigenere table which results in polyalphabetic cipher. On receiver side decrypt cipher through vigenere table. Do data post-processing which converts DNA sequence into binary form. Authors tried to improve regular vigenere cipher through some security evaluation. Authors claim proposed DNA cryptography algorithm provides better security.Noorul Hussain Ubaidur Rahman and Chithralekha Balamurugan in 2015 proposed two algorithms, one is the DNA computing based encoding algorithm and another is the DNA Computing based encryption and decryption algorithm. Encoding table (DNA) is created after session which is predefined intervals and hence DNA sequences and the alphabets assignments would be random across different sessions [3]. After that, use DNA encryption algorithm. First divide plain text into two equal halves. If plaintext is not even in length then add random alphabets into that sequence to make length even. Use DNA encoding table and transform the code with help of multiple round function as transformation.DNA, mRNA, tRNA and shift sequence etc. In next step, use Amino acid table which generated by two mRNA sequences. To perform decryption, reverse procedure is performed.Authors also have performed experimental analysis i.e. time taken for encoding & decoding and encryption & decryption algorithm. Author also have performed frequency analysis. Bhaskar Mondal and

Tarni Mandal describes in detail with experimental analysis in their research title “A light weight secure image encryption scheme based on chaos & DNA computing”. In their paper, authors used both concept: chaotic and DNA sequence. A chaotic map is a discrete-time dynamical system, defined as per equation

$$X_{k+1} = ã(x_k),\ xϵ(0,1),\ k = 0,1,2,3$$

In DNA sequence nucleic acid bases are used: A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, G and C are complementary. This paper generate proposed scheme. L.Jani et al. discussed about Multi-Secret image which is based on DNA sharing in detail. First step is DNA encoding.

Second step is to hide the secret message through text steganography technique. The proposed approach was based on the Lagrange interpolation polynomial. First all secret images are coded with the help of DNA sequence, and again shuffled using the addition rules of DNA, and then follow encryption process by using Shamir's secret scheme of sharing. Since the meaningless shadows were generated, with the each shadow is covered into a host image. Then distribution is performed. At least 'k' participants pool their shares during reconstruction to recover the multiple secrets. Finally, DNA subtraction rules results secret images. Since prior to the secret sharing scrambling of pixel is performed, this reduces the correlation among the pixels. As a result high efficiency (correlation) is achieved. According to authors, their paper provides a highly secure, perfect multi secret sharing scheme.Monika et al in their research describe about DNA encryption technique via SSL protocol. Basically, in their paper authors define basic DNA (nucleotides bases) that exchange public key between sender and receiver via SSL layer.

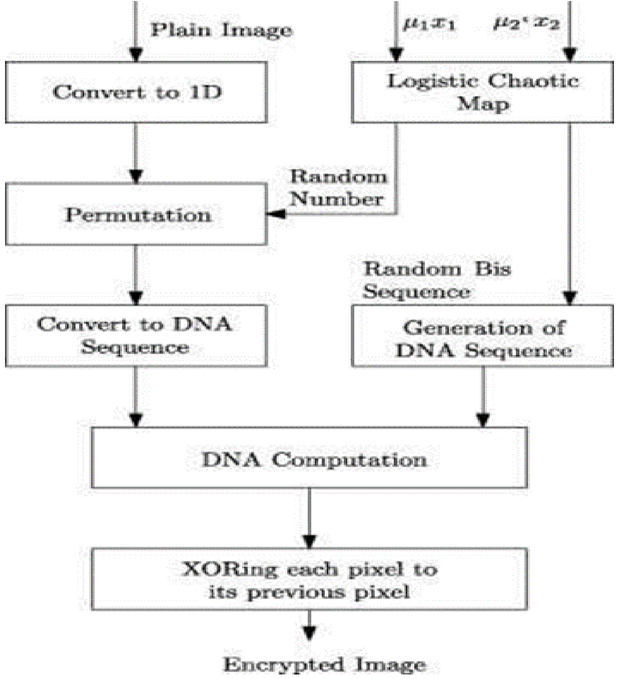


Figure 4. Scheme of chaotic and DNA sequence

Abhinav Thakur [6], discuss about different techniques of image and video steganography. In his review paper, author describe major techniques that are mostly used in recent year. Souma Pal [7], describe various method of video steganography. Some methods are steganography, digital watermarking, Least Significant Bit, Discrete Wavelet Transform, and Discrete Cosine Transform. Pal also discusses about performance evaluation criteria. Performance is evaluated based on secret images numbers, expansion of pixel, image format and share generated type.Syeda Musfia Nasreen [8], explain video steganography and their technique with comparative analysis. It describe in brief about Non-uniform rectangular partition, compressed video steganography, Anti-forensics technique, Masking and filtering.

III. THE PROPOSED METHOD

This section presents proposed work. DNA along with LSB approach has been used. DNA in one side improves security in terms of encryption (cryptographic approach of proposed algorithm), L the i.e. proposed metamorphic cryptography approach with the help of DNA and LSB to ensure more security simultaneously creating less suspect. Binary index compression technique is used to increase the payload capacity of proposed algorithm.In this approach, first step is to convert secret plain text into its corresponding ASCII values. Convert these ASCII values generated in first step into binary form. Index compression technique is then applied three times to compress the data. When all the above steps applied successfully, convert into nucleotides that make up polymers, named after the nitrogen base that it consists of; Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Select a carrier video. From that selected video, select one random frame. Here random frame is selected with the help of chaotic sequence formula. Hide encrypted message i.e. nucleotides into the LSB of selected frame. Concept of XOR is used to create less distortion in carrier frame. In decryption process it will be vice versa.

A. *Detailed Description of Methodology Used:*

DNA sequence with index compression has been used. First one is cryptography that has some relationship with the corresponding computing model more or less. Second is some biological technologies computations used in DNA approach.

This paper using DNA sequence with compression technique, that compression technique is lossless compression technique that reduce 50% of data. It is provide best compressed data to give space complexity and manage payload capacity. In video steganography, secret data encode inside a cover video. In this section describes some information regarding techniques in brief that used in video steganography. i.e. Spatial Domain Steganography Techniques, and Frequency Domain Steganography Techniques.

B. *Types of Video Steganography:*

Spatial Domain Steganography Techniques: This technique is based on Least Significant Bit (LSB). Message data is encoded into the LSB of the carrier video frame. To check the quality with the help of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). With the help of indexing hide the data into frame of video and instead to check whole information, through index retrieve the information from stego video. It will reduce the computational time rather than existing method. And another method is back propagation neural network, where XOR operation perform to hide the information into cover video.

Frequency Domain Steganography Techniques: This technique use Lazy lifting wavelet transform technique to hide the information and gives high payload capacity video

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

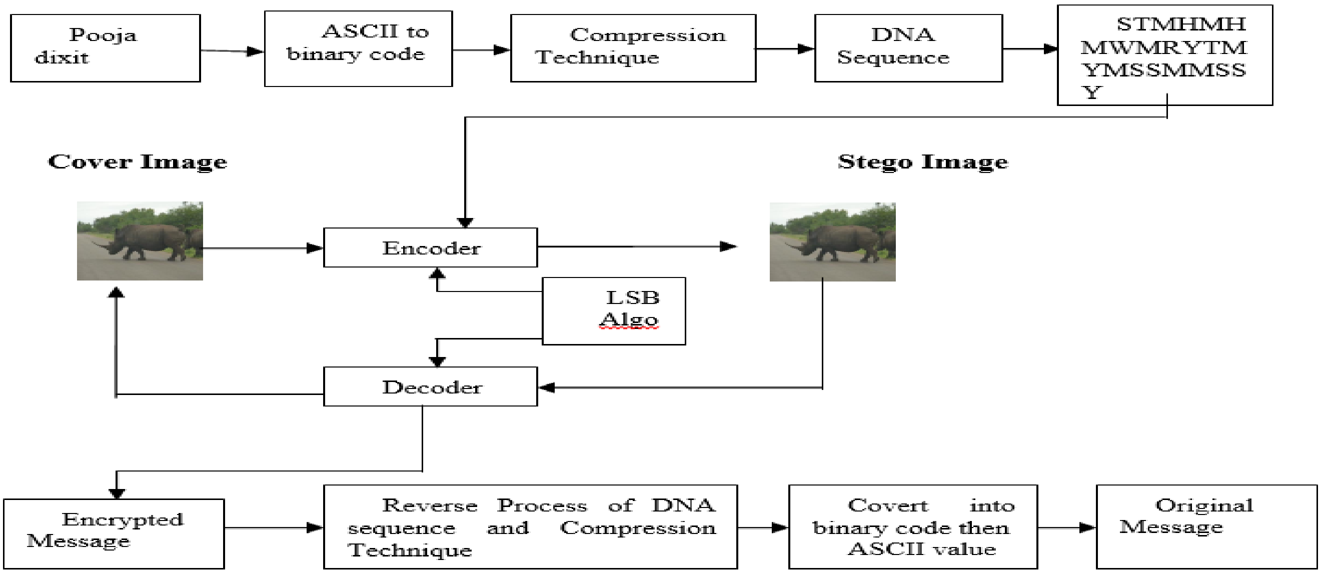


Figure 6. Encrypt message through DNA and Hide into video.

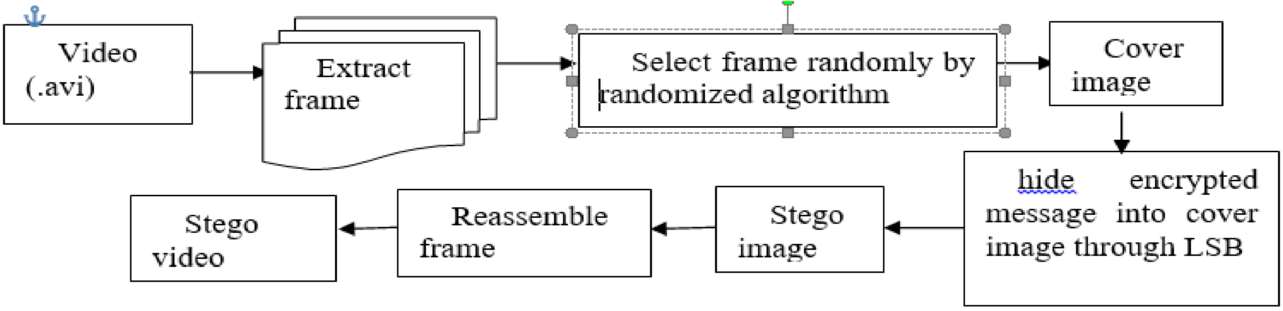
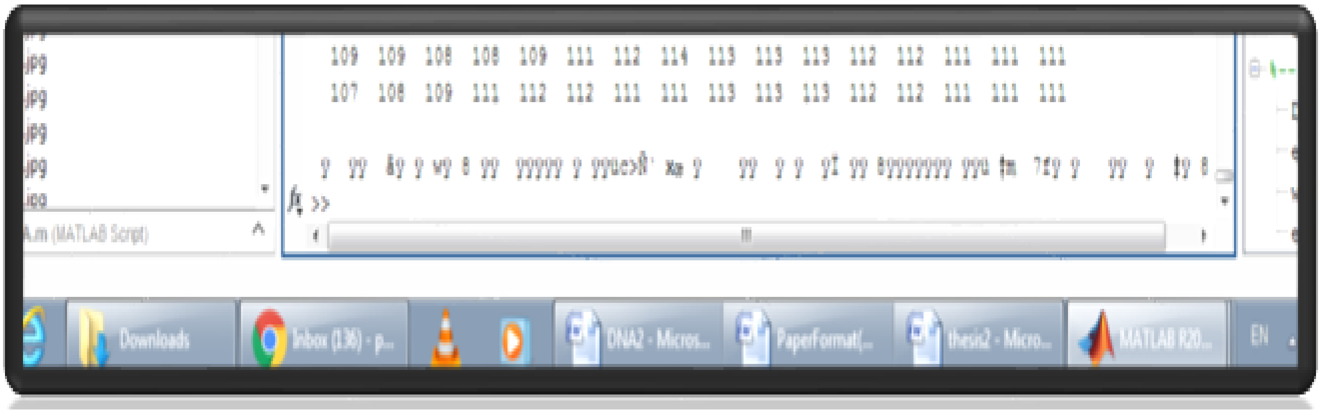

Video (.avi)
Extract frame
Select frame randomly by randomized algorithm
Cover image
hide encrypted message into cover image through LSB
Stego image
Reassemble frame
Stego video

Figure 7. Extraction and selection of frame from video



```
   109   109   108   108   109   111   112   114   113   113   113   112   112   111   111   111
   107   108   109   111   112   112   111   111   113   113   113   112   112   111   111   111


 ÿ  ÿÿ  âÿ ÿ wÿ ð ÿÿ  ÿÿÿÿÿ ÿ ÿÿÿu©>Å'  Xæ ÿ   ÿÿ  ÿ ÿ  ÿÏ  ÿÿ ðÿÿÿÿÿÿÿ ÿÿÜ fæ  7£ÿ ÿ   ÿÿ  ÿ  ‡ÿ ð
fx >>
```

Figure 8. Encoded message into video frame

Figure 9. Original image

Figure 10. Stego image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

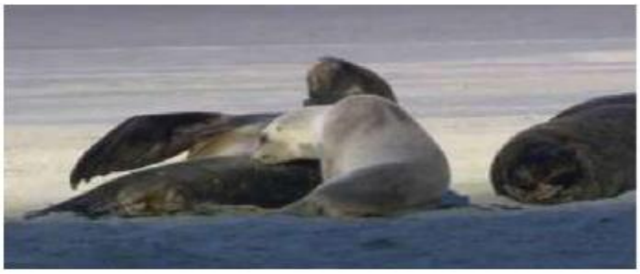


Figure 11. Original image

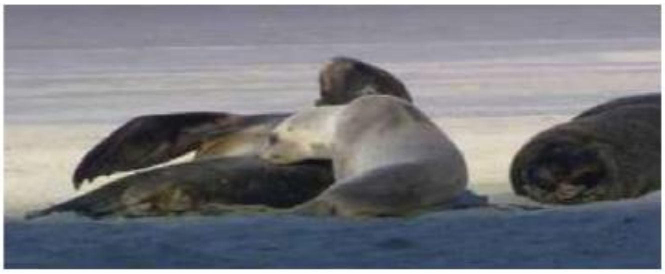


Figure 12. Stego image

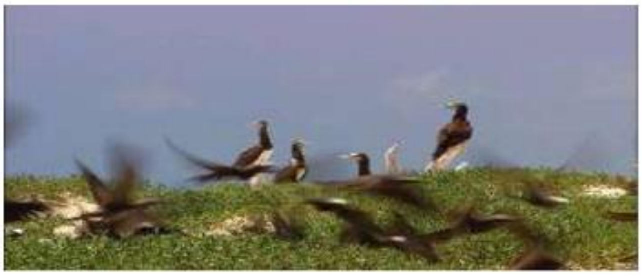


Figure 15. Original image

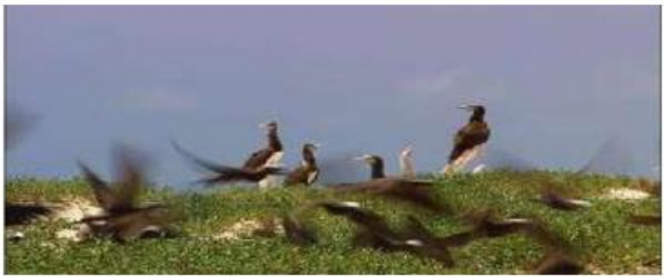


Figure 16. Stego image

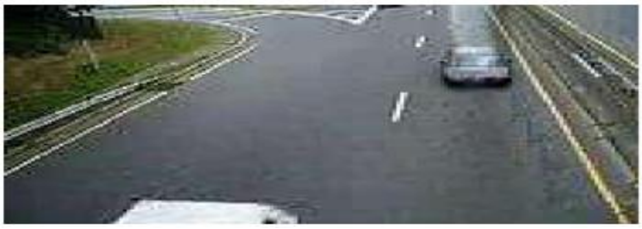


Figure 17. Original image

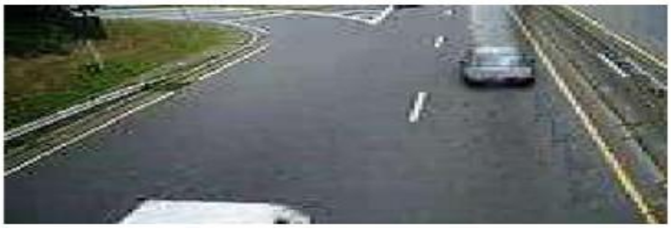


Figure 18. Stego image

Steganography. First of all wavelet is apply into the video frame and then apply LSB approach that hide data in the coefficients of video frames. Hiding techniques based on the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT).This research is utilizes the concept of Spatial Domain Steganography Techniques, so it uses PSNR and MSE, i.e.

$$\text{MSE} = \sum_{x=1}^{M}\sum_{y=1}^{N}(S(xy) - C(xy))\hat{}2$$

$$\text{PSNR} = 10\log\left(C_{max}{}^{2} / MSE\right)$$

Where x and y represents coordinates of images, image dimensions are M and N, Sxy is the image obtained after encoding i.e. stego image and cover image Cxy . Maximum value in the image is 2.Tools and Software Used: MATLAB R2017/ 64-bit Operating System/ Bioinformatics Tool/ Image Processing Tool

IV. PROPOSED ALGORITHM

Algorithm to encrypt message:

- Input the message to be encrypted
- Convert it into ASCII code
- Change ASCII code into binary form
- Use index compression technique till length of cipher text equal to plaintext
- Encode into nucleotides symbol
- Hide message via video medium
- First of all extract frame of video
- Hide message through XOR and LSB technique.
- Combine all frame into video and send that video to receiver side.

Algorithm to decrypt message:

- Accept video by receiver that send by sender.
- Divide video into frame. Select the required frame.
- Extract information via reverse process of XOR and LSB technique.
- Decode nucleotides symbol into integer. # Snippet of implemented MatLab code.

M=
['ST';'MH';'MH';'MW';'MR';'YT';'MY';'MS';'SM';'MS';'SY'];

- Use reverse process of index compression technique.
- Change binary form into decimal code.
- Resultant has been converted into text. # Text is original message.

This method has been reduce the problem of storage and improve secrecy. This compress technique compress message into 50 percent binary form of data at each level.

V. IMPLEMENTATION & RESULTS

The proposed technique has implemented on different video (i.e. video frames) formats i.e. .avi, .wmv etc. to check it's efficiency. From figure 9 to figure 18, it is clear that there is no difference between original video frame and frame obtained after the implementation of proposed algorithm. Figure 21 contains comparison i.e. Proposed method Vs XOR technique. Proposed method provides low MSE value in comparison to XOR approach. From figure 20 it can be concluded that proposed method provides high PSNR values. High PSNR and low MSE values itself ensures quality of video remains good after proposed method has implemented.

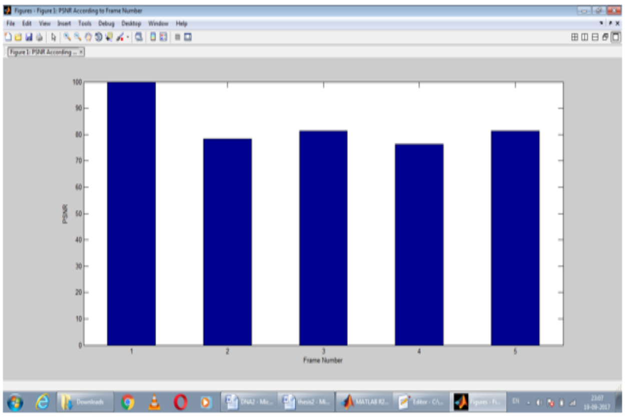
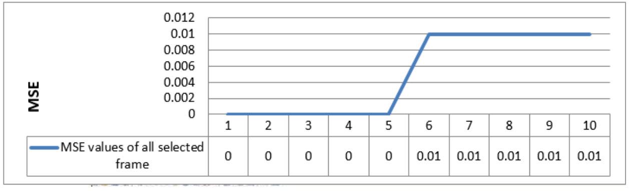
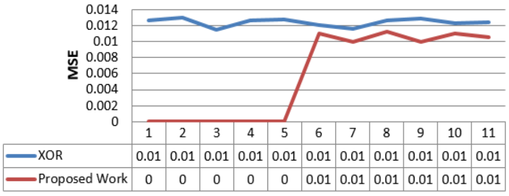


Figure 11. PSNR Values of all selected frame



	1	2	3	4	5	6	7	8	9	10
MSE values of all selected frame	0	0	0	0	0	0.01	0.01	0.01	0.01	0.01

Figure 20. MSE Values of all selected frame (Proposed Technique)



	1	2	3	4	5	6	7	8	9	10	11
XOR	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
Proposed Work	0	0	0	0	0	0.01	0.01	0.01	0.01	0.01	0.01

Figure 21. Comparison of MSE Values of all selected frame (Proposed Vs XOR)

VI. CONCLUSION

Data confidentiality is very important during communication between two parties. The objective of presented paper is to develop an efficient steganographic algorithm which not only utilizes the concept of binary indexed based compression technique but also uses the fundamental idea behind encryption technique. Binary indexed based compression technique has been used to reduce the size of secret message which on the other hand increases payload capacity of the carrier video. Proposed approach is robust against cipher attacks. Applying compression technique reduces data up to 50% which improves payload capacity. Output of the above steps is converted into sequences of DNA nucleotides. Concept of steganography is implemented with the help of LSB algorithm. LSB is very easy and simple method that reduce the computation time. Proposed algorithm has implemented on several videos and some of the results have been shown in figures contained in this presented paper. Proposed method also provide high PSNR with low MSE, it means video quality is good. So, there is difficult to detect secret message from message-embedded video which states good steganographic strength.

REFERENCES

1. Sherif T. Amin, Magdy Saeb Salah El-Gindi.:, "A DNA-based Implementation of YAEAEncryptionAlgorithm," www.magdysaeb.net/images/DNAYAEAaminsaeb.pdf.
2. Noorul Hussain Ubaidur Rahman., "A Novel DNA Computing Based Encryption and Decryption Algorithm," Procedia Computer Science, Vol. 46, (2015).
3. Bhaskar Mondal , Tarni Mandal., "A light weight secure image encryption scheme based on chaos & DNA computing," Journal of King Saud University - Computer and Information Sciences, March (2016).
4. L.Jani Anbarasi , G.S.Anandha Mala., "DNA based Multi-Secret Image Sharing," International Conference on Information and Communication Technologies, ICICT 2014.
5. Monika , Shuchita Upadhyaya., "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks," 4thInternational Conference on Eco-friendly Computing and Communication Systems, 2015.
6. Souma Pal., "Various methods of video steganography," International Journal of Information Research and Review, Vol. 03, pp. 2569-2573, Issue, 06 (2016).
7. Abhinav Thakur., "Different Techniques of Image and Video Steganography," A ReviewIn: e-ISSN: 1694-2310, Vol. 2, Issue, 2 (2015).
8. Syeda Musfia Nasreen.: A Study on Video Steganographic TechniquesIn: International Journal of Computational Engineering Research (IJCER), Vol. 05, Issue, 10 October (2015).
9. Navneet Kaur., "A Survey on various types of Steganography and Analysis of Hiding Techniques," International Journal of Engineering Trends and Technology (IJETT), Vol. 11, May (2014).
10. Kalpana Singh., "Selective encryption technique in RSA based singular cubic curve with AVK for text based documents," Enhancement of Koyama approach., Deakin University, Dept. of Comput. Sci. & Eng., Motilal Nehru Nat. Inst. of Technol., Allahabad, India., DOI: 10.1109/ICNIT.2010.5508497 Conference: Networking and Information Technology (ICNIT)., International Conference on Source: IEEE Xplore, 2010.
11. R. Ganga Sagar., 2 N. Ashok Kumar., "Encryption Based Framework for Cloud Databases Using AES algorithm," International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), Vol. 2, pp. 27-32, Issue 6, June (2015).
12. Aishwarya Asesh., "Encryption Technique for a Trusted Cloud Computing Environment," IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, pp. 53-60, Vol. 17, Issue 1, Ver. V, www.iosrjournals.org, (2015).
13. Mehrdad.S.Sharbaf., "QuantumCryptography: A New Generation of Information Technology SecuritySystem," http://ieeexplore.ieee.org/xpl/freeabs all?arnumber=5070885, 2009.
14. E. Thambiraja., Dr. R. Umarani., "A Survey on Various Most Common Encryption Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 7, (2012).
15. Sourabh Chandraa.,Bidisha Mandalb., Sk. safikul Alamc., Siddhartha Bhattacharyya., "Content based double encryption algorithm using symmetric key cryptography," International Conference on Recent Trends in Computing (2015),2015.
16. Sridhar C. Iyera.,, R.R. Sedamkarb., Shiwani Gupta., "A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach," 7th International Conference on Communication, Computing and Virtualization (2016),2016.
17. Md.Atiullah Khan.,Kailash Kr.Mishra., N. Santhi., J.Jayakumari., "A New Hybrid Technique for Data Encryption," Proceedings of 2015 Global Conference on Communication Technologies (2015), 2015.
18. WU Xing-hui., "Research of the Database Encryption Technique Based on Hybrid Cryptography," International Symposium on Computational Intelligence and Design. (2010), 2010.
19. Pradeep H Kharat., "A secured Transmission of data using 3D chaotic map encryption and data hiding technique," International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune, India, May (2015).
20. Nur Nabila Mohamed., Habibah Hashim., Yusnani Mohd Yussoff., "Compression and Encryption Technique on Securing TFTP Packet," IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, April (2014).
21. Hadia M.S. El Hennawy., Alaa E.A. Omar b., Salah M.A. Kholaif., "LEA: Link Encryption Algorithm ProposedStream Cipher Algorithm," 2014 Production and hosting by Elsevier B.V. on behalf of Ain Shams University (2014), 2014.

22. S. Shivani, Yadav V. K., B., "Zero Distortion Technique: An Approach to Image Steganography on color images," International Conference on Information and Communication Technology for Competitive Strategies, ICTCS '14, November 14 – 16 pages 79-83 (Published by ICPS-ACM, Proceedings Volume ISBN No: 978-1-4503-3216-3).
23. R Paul, AK Acharya, VK Yadav, S Batham., "A Novel Approach of Bulk Data Hiding using Text Steganography," Third International Conference on Recent Trends in Computing (ICRTC 2015) will be held in SRM University, NCR Campus, Modinagar, Ghaziabad, India, during March 12th – 13th, 2015". Publisher: Elsevier Procedia Computer Science Journal.
24. S Batham, VK Yadav, AK Mallik., "ICSECV: An Efficient Approach of Video Encryption," Contemporary Computing (IC3), 2014 Seventh International Conference, 7-9 Aug. 2014, Pages: 425 – 430 (Available at IEEE Xplorer and DBLP, indexed by SCOPUS).
25. Shivani Sharma, Virendra Kumar Yadav, Saumya Batham., "Zero Distortion Technique: An Approach to Image Steganography using Strength of Indexed Based Chaotic Sequence". symposium proceedings published by Springer in Communications in Computer and Information Science Series(CCIS), Volume 467, 2014, pp 407-416, ISSN: 1865:0929.
26. Saumya Batham, Anuja Kumar Acharya, Virendra Kumar Yadav, Rahul paul., "A New Video Encryption Algorithm Based on Indexed Based Chaotic Sequence," Fourth International conference Confluence 2013: The Next Generation Information Technology Summit, Sept 27-28, Page(s): 139 – 143 (available at IET and IEEE xplorer).
27. Adedeji Kazeem B., Ponnle Akinlolu., "A New Hybrid Data Encryption and Decryption Technique to Enhance Data Security in Communication Networks: Algorithm Development," International Journal of Scientific & Engineering Research, Vol. 5, Issue 10, October (2014).
28. https://en.wikipedia.org/wiki/Steganography.
29. Pooja Dixit., Virendra Kumar Yadav., Munesh Chandra Trivedi., "Traditional And Hybrid Encryption Techniques: A Survey," ICRACCCS-2016, conference proceedings, a signed Springer, Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur, India(2016), 2016.
30. Ramandeep Kaur., Pooja., "XOR Encryption Based Video Steganography," International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Vol. 4, Issue 11, November (2015).

AUTHORS PROFILE

Pooja Dixit is currently M.Tech second year student in computer science department at ABES Engineering College, Ghaziabad.

Dr. Munesh Chandra is currently working as Associate Professor, Department of Computer Science & Engineering, National Institute of Technology, Agartala (Tripura). Previously He was Dean Academics, HoD & Associate Professor (IT), Rajkiya Engineering College with additional responsibility of Associate Dean UG Programs, Dr. APJ Abdul Kalam Technical University, Lucknow (State Technical University). He was also the Director (In charge) at Rajkiya Engineering College, Devgaon. He has a very rich experience of teaching the undergraduate and postgraduate classes in Government Institutions as well as prestigious Private institutions. He has published 12 text books and 81 research papers publications in different International Journals and in Proceedings of International Conferences of repute. He has also edited 21 books of the Springer Nature and also written 23 book chapters for Springer Nature. He has received numerous awards including Young Scientist Visiting Fellowship, Dronacharya Award, Author of Year and Vigyan Ratan Award from different national as well international forum. He has organized more than 30 international conferences technically sponsored by IEEE, ACM and Springer's. He has also worked as Member of organizing committee in several IEEE international conferences in India and abroad. He has delivered numerous invited and plenary conference presentations and seminars throughout Country and chaired the technical sessions in International and national conferences in India. He has also delivered many invited talks in India. He is on the review panel of IEEE Computer Society, International Journal of Network Security, Pattern Recognition letter and Computer & Education (Elsevier's Journal), Recent Patents in Computer Science (Bentham Science) and many Journals of IGI Global. He is also member of editorial board for International Journal of Computer Application, Journal of Modeling and Simulation in Design and Manufacturing (JMSDM) and International Journal of emerging trends and technology in Computer Science& Engineering. He has been appointed member of board of studies as well as in Syllabus committee of different private Indian universities and member of organizing committee for various national and international seminars/workshops. He was Executive Committee Member of IEEE UP Section, IEEE computer Society Chapter India Council and also IEEE Asia Pacific Region-10. He is an active member of IEEE Computer Society, International Association of Computer Science and Information Technology, Computer Society of India, International Association of Engineers, and life member of ISTE.

Virendra Kumar Yadav is currently pursuing PhD in the area of Image processing using deep learning from Indian Institute of Technology, Delhi. He worked as Assistant Professor in the Department of Computer Science & Engineering at ABES Engineering College, Ghaziabad. He did my M.Tech in Computer Science & Information Security from Kallinga Institute of Industrial Technology (KIIT), Bhubaneswar in the year 2013. During M.Tech, he worked as Junior Research Fellow. He had published research papers on Image Processing, Security, Applied Engineering and Software Engineering, Steganography, Cryptography. His area of research interest includes Image Processing, Machine Learning, Deep Learning, Data Science, Information Security, Digital Forensics and Computer Networks. He is two times recipient of fellowship awarded by Indian Academy of Sciences, Certification in Machine Learning by IBM (course offered through course era), Certification in Python by Rice University, Texas and many more.

He also served as reviewer in IEEE Access, International Journal British Journal of Mathematics and Computer Science, Microsystem Technologies (International Journal, SPRINGER), Alexandria Journal (International Journal, Elsevier. and served as reviewer in international conferences such as ICICT-2018 (IEEE), ICICT(2018), UPCON-2017, ICCCCS- 2016, SSCC-2016(Springer), CICT-2016/2017(IEEE Conference), ICICT-2015(IEEE Conference), SSCC-2015(Springer Conference), UPCON-2015(IEEE conference), SSCC-2014(Springer Conference), CICN 2014(IEEE Conference) etc.

Dr Avadhesh Kumar Gupta is currently working as Professor and Dean-New Programme Development at IMS Ghaziabad.Formerly he has served IMS Ghaziabad as HOD-MCA for 5 years . He is an outcome based dynamic Academician, Researcher and Administrator with 17+ years Experience, who ensures building Eco-system of institution as holistic approach and translating energy into synergy for transforming institutions. He has published more than 35 Publications in various National and International Journals and Conferences of repute.His area of interest includes Data sciences , Big Data Computing and Business Analytics with inter-disciplinary focus. Earlier he has worked with Amity University, Galgotias University and ITS Ghaziabad in the role of Academicians and Academic Administrators. He possesses proven leadership traits with excellent communication / oratory/ public speaking. Dr Gupta has been awarded with Top Colleges CTO's Award at Digital Edge ICT Conclave 2016 (Supported by Ministry Of Electronics and Information Technology, Government of India) on 11th November ,2016). He has been also awarded with "Guru Dronacharya Award " by Shri Narayan Sanskritik Chetna Nyas Noida on 5th September 2018 at Hotel Crown Plaza , Mayur Vihar ,Delhi. He has participated as panelist speaker, expert speaker and resource person in various conclaves, workshops, MDP,FDP, Seminars and conferences in various institutes, corporate and universities across country.

Er. Vineet Kumar Singh is currently working as Assistant Professor, Department of Information Technology, Institute of Engineering &Technology, Dr Rammnoher Lohiya Avadh University ayodhya (UP).

Table 1: Comparisons of DNA Cryptography, Traditional Cryptography and Quantum Cryptography

Parameter	Traditional	DNA	Quantum
Growth	Very old technique	Method is costly and under study.	Practice is hard. Real time realization is difficult.
Confidence	Realized only with estimating safety excluding the one-time pad.	The quantum cryptography is absolutely secured till date	The claiming & safety level of this concept are under study till date.
Significance	In this method, the authentication, digital signature, both the encryption of public and private keys can be executed for its objective.	Beneficial in the real transmission of data process. But, inconvenience of saving the safe data makes it impracticable to carry out the digital signature and public key encryption like the traditional method.	At present, the cipher text in DNA technique can be transmitted only through tangible ways. DNA we can also take the advantage of yielding cash vouchers, memorable agreements and proof of identity.

Table2: Comparison of Secret Communication Techniques

Steganography Techniques	Cover Media	Embedding Techniques	Advantages
Video Hiding	Video		
1.Spatial Domain Steganography Techniques:			
LSB(Least Significant Bit)		This method is used the least significant bit of every pixel in one image to hide the most significant bit of another	Simplest & easiest way of hiding information
2.Frequency Domain Steganography Techniques:			
2.1.DCT (Discrete Cosine Transform)		Embeds the information by altering the transformed DCT co-efficient	Hide data can be distributed more evenly over the whole image in such a way to make it robust
2.2.DWT (Discrete Wavelet transform)		This technique work by talking many wavelet to encode a whole image	Coefficient of wavelet are altered with the noise within tolerable level

Table 3. Encryption execution time of some technique in second [29]

Bits	Hybrid	Compression and Encryption	RSA based singular cubic curve with AVK	DNA sequence
256	0.004	0.003	0.004	0.003
512	0.005	0.002	0.005	0.002
1024	0.003	0.002	0.005	0.001
2048	0.004	0.002	0.011	0.001

Table 5. PSNR and MSE value for all selected frame

Frame Number	PSNR(db)	MSE
1	Infinite	0.00
2	78.4	0.00
3	81.4	0.00
4	76.4	0.00
5	81.3	0.00
6	70.3	0.01
7	70.2	0.01
8	71.3	0.01
9	72.5	0,01
10	74.0	0.01
Average Values	Infinite	0.005

Table 6. Comparison between XOR technique and proposed technique [30]

Frame Number	XOR		Proposed work	
	PSNR(db)	MSE	PSNR(db)	MSE
1	67.10	0.0127	78.3	0.00
2	67.00	0.0130	78.4	0.00
3	67.52	0.0115	81.4	0.00
4	67.12	0.0126	76.4	0.00

5	67.06	0.0128	81.3	0.00
6	67.28	0.0121	70.3	0.011
7	67.49	0.0116	70.2	0.010
8	67.10	0.0127	71.3	0.0113
9	67.03	0.0129	72.5	0.010
10	67.24	0.0123	74.0	0.011
Average Values	67.9	0.0124	72.91	0.0106