JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A BLENDED APPROACH OF DATA HIDING USING CRYPTOGRAPHY AND STEGANOGRAPHY: THE METAMORPHIC CRYPTOGRAPHY

[1]Ms. Namrata Jogi, [2]Dr. Maithili Arjunwadkar
[1]Assistant Professor, [2] Director
[1]Department of BCA, Modern College of Arts, Commerce and Science, Shivajinagar, Pune, MS, India ,
[2] Modern Institute of Business Studies, Nigadi, Pune, MS, India

Abstract: This is an era of digital communication that is communication over internet. In today's day to day life data /information security over the network transmission take a most important fear of getting have or tempering illegal use or copyright violation etc. For protecting such information (audio/ image/ text/video) from above fear the data can be send in hidden format by using various Steganography techniques with addition of a Cryptography benefits which make data unreadable. Metamorphic Cryptography is the combination of a Cryptography and Steganography which is double layer security. In Steganography we can hide message in medium like audio/ image/ text/video but it is not enough to protect data, but in cryptography we make data in unreadable format by using various encryption-decryption technologies. This paper discusses Metamorphic Cryptography and their various approaches.

Keywords: Cryptography, Steganography, Metamorphic Cryptography, Video Steganography.

I. Introduction

Securing information over internet is important task, as we all are doing online transactions, transferring or exchanging information, conversations with various social media platform, applications such as video-on-demand, video conferencing, broadcasting etc. [8]. It is important to make them safe from the intruders [10]. Previously we are using 2 approaches cryptography and Steganography. In Cryptography one can encrypt the data by using various algorithms with key (public or private). Steganography is art of hiding the things [4]. Both the techniques have their benefits and drawbacks. For example, if we are sending some important thing like gold and implementing the concept of cryptography, which enforcing on the encryption i.e., certain major is to be taken to secure data, in case of gold we will put this gold in box, put locks and then put the box in truck and tight the box with chains and appoint the security guard, so the monitor the security, drawback of cryptography due to lots of security intruder can identified something important is sending and try to steal it. Now if we consider same example for steganography, it is the art of hiding the things, here we do not apply any lock, not security guards for gold, just put gold in truck and put some leaves and raw material, useless things over gold and send the truck from one place to another. The drawback of steganography, if the intruder senses some important is going on then they steal it very easily. Steganography is good till the intruder don't know about information [17]. Metamorphic Cryptography is the combination of cryptography and steganography, in which information is first encrypted and the hide in a medium like text, image, video, audio. It will provide double security to information.

II. Cryptography

Cryptography is the process of converting secret message into unreadable format, it can only decode by the key. The main objective of the cryptography is to make file (text/audio/image/video) secure by converting it into cipher text by using cipher algorithms which uses transposition and/or substitution methods. For decoding the secret data / message key is required which is only known to the sender& receiver. **Encipher (encode)** is the process of converting secret data to cipher text using an algorithm and a key whereas **Decipher (decode)** the process of converting cipher text back into secret message using an algorithm and a key.

Cryptanalysis the study of principles and methods of transforming coded message back into readable message without knowledge of the key [25].

Various techniques are available for cryptography. The selection of right cryptographic technique is depended on time (How much time will be needed for encrypting and decrypting
the data), memory (How much memory will be needed), security (Selected encryption technique should meet the confidentiality, integrity of the data), nature of data (How much data is important on that basis symmetric or asymmetric or both techniques suitable), type of data [18]. (In case of video files, the privacy is more valuable with consideration of time, memory, security it will suggest hybrid encryption method i.e., symmetric + asymmetric can provide all security objectives.)

Performance of cryptographic algorithms depends on tunability, Computational Speed, Key Length Value, Encryption Ratio, Security Issues [18].

Some Cryptography techniques are as follows [5]:

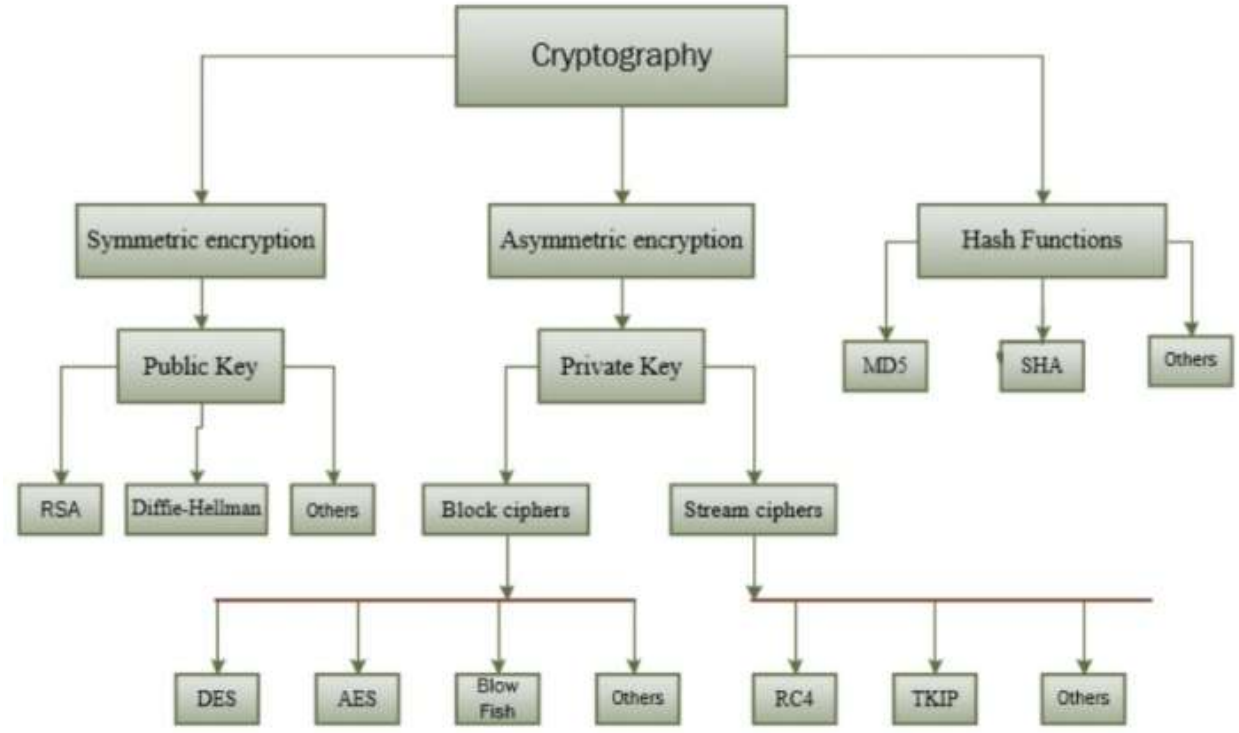

Fig 1: Cryptography Techniques

III. Steganography

Steganography is the art of hiding data or information in the medium like audio or video or text or image [22]. Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text, video) with bits of different and invisible information. Hidden information can be any other regular computer file (text, audio, video, image) or encrypted data (text, audio, video, image). Steganography hides the information in cover or medium in such way that only the receiver can find it.

Types of Steganography:

1. Text Steganography: In its data or information hide inside the text files. In this technique, the secret data is hidden behind every n^{th} letter of every word of text message. Various methods are used for hiding data in text file. Some methods are Format Based Method, Random and Statistical Method, Linguistics Method [20,4].

2. Image Steganography: Hiding the data by using the image as cover is referred as image steganography. In image Steganography pixel strength is used to hide the data. In digital steganography, images are mostly used as cover because there are number of bits presents in digital representation of an image [20,4].

3. Audio Steganography: It hide data in audio files. This technique hides the data in AU, WAV, MP3 resonate files. There are different methods of audio steganography. These methods are Low Bit Encoding, Phase Coding, Spread Spectrum [20,4].

4.Video Steganography: It is a technique of hiding files or data (text, audio, image, video) into digital video format. In this case video (combination of frames) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) changes the values (e.g., 7.667 to 8) which is used to hide the data in each of the frame in the video, which is undetectable by the human eye. Mp4, H.264, AVI, MPEG are the formats used by video steganography [20,4].

5. Network or Protocol Steganography: It means hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc., as cover. In the OSI layer network model there are covert channels in which steganography can be used [20,4].

Some factors Affect Steganography techniques. Effectiveness of steganography technique can be determined by comparing stego-image with the cover. Some factors determine the efficiency of a technique. These factors are:

1) Robustness: Robustness means the ability of embedded message to remain same if the stego - image undergoes some operations, like cropping or decimation, linear and non-linear filtering, lossy compression, sharpening or blurring, rotations and scaling, addition of random noise [21].

2) Imperceptibility: It means imperceptible of a steganographic algorithm. Because it is the first and last requirement, as the strength of steganography known for the ability to be undiscovered by the human eye [21].

3) PSNR (Peak Signal to Noise Ratio): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the exactness of its representation. This ratio measures the difference between the original and a compressed image. The greater value of PSNR represents the better quality of the compressed image [10,21].

4) MSE (Mean Square Error): It is the average squared difference between a reference image and a distorted image. If less value of MSE, then more efficient the image steganography technique. MSE is calculated with pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count [10,21].

5) SNR (Signal to Noise Ratio): It is the ratio of the signal power and the noise power. It differentiates the level of a desired signal to the level of background noise [10,21].

Following figure shows the types of Steganography [3]:

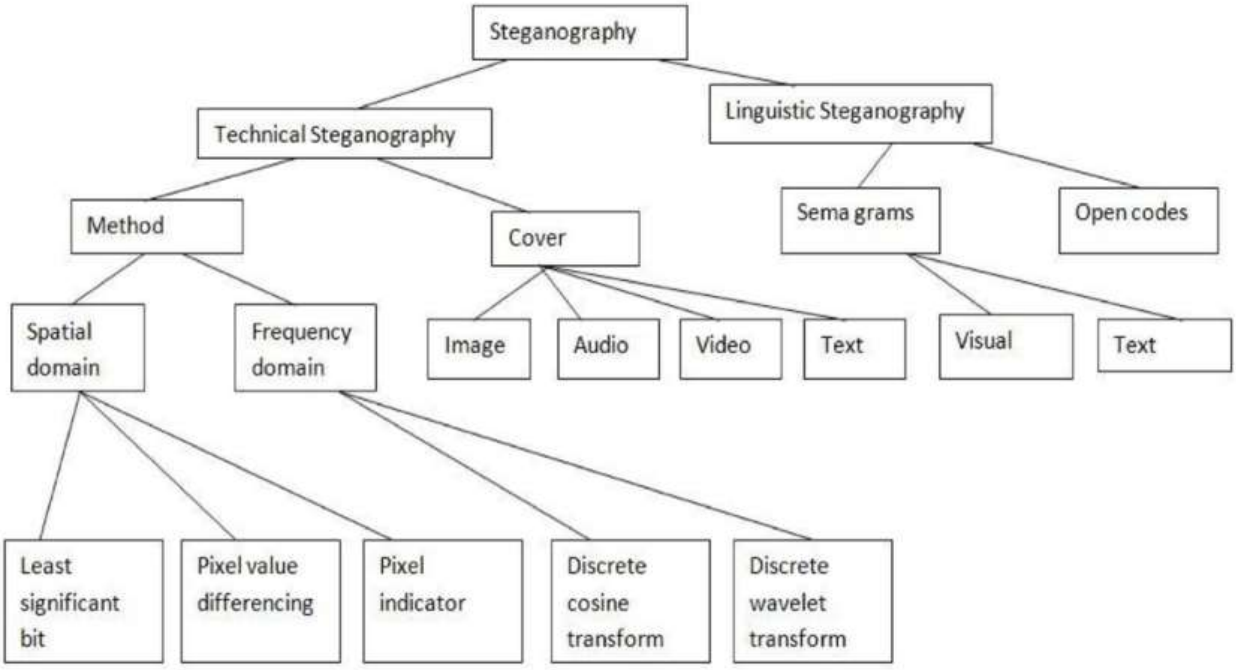

Fig 2: Steganography Types

IV. Literature Review

Vikash Yadav and Indresh Kumar Gupta (2019) stated the strength of both concepts has been used. DNA concept is used to encryption of the message (text). After message (text) is encrypted, it is ready to be hidden in the cover medium which is video, audio or text. Image is used as cover medium. KIMLA concept has been used to hide the encrypted text in cover image. MatLab2017b has been used to simulate the proposed algorithm. Various types of images have been used to observe the detection in cover medium. KIMLA algorithm produces very less distortion in required image. Simulation results show that proposed algorithm is quite efficient in terms of robustness, security and payload capacity.

Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, Vineet Kumar Singh: This paper represented how metamorphic cryptography concept is implemented. DNA (Deoxyribonucleic Acid) based cryptography is used to achieve cryptographic strength. Plaintext message which contains important information is transferred into its corresponding ASCII values. An obtained ASCII value is then altered into corresponding binary values. Apply binary index compression technique on binary values. Applying compression technique reduces message up to 50% which enhance payload capacity. Output of the above steps is transferred into DNA nucleotides sequences. Steganography is implemented with the help of Least Significant Bit 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.

Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, Vineet Kumar Singh (2019): This paper focuses only on the types of steganography that uses audio as a cover medium. The technique index based chaotic sequence is used for encryption. It carries two steps which make the cryptanalysis and steganalysis further more difficult as compare to simple LSB method. First step is encrypting the secret text using index based chaotic sequence. Second step is hiding encrypted data generated

by first step using the concept of LSB with XOR method. It gives extra level of security by creating less distortion in audio file and also maintaining high embedding capacity.

M. Gajalakshmi, R. Vidya (2018) : This paper proposed a model for plain text message which will send using XOR operation for encrypting file. It uses histogram shift method and achieves good and stable PSNR value. Authors also trying to reduce the previous execution time and to give the better result in PSNR value with better security and also by including watermarking technique it achieves high security in data transmission.

Mr. Akash V. Malasane, Prof S. P. Bhonge (2015) : This paper defines basic model of proposed methodology, In which first of all we used the block cipher application, like AES (Advanced Encryption Standard) which is apply to data for encryption and it will fed to a LSB (Least Significant Bit) with a frame selection using LSB technique for Steganography for hiding message and this block connected to input video applying and we will get a result in a hidden format i.e. video will provide higher level of security if compare to text , image , audio as cover.

Atul Haribhau Kachare, Mona Deshmukh (2014) : in this paper author takes input in the string format. The string is then converted in ASCII codes. On other side audio or speech is taken as input and encoded using Steganography technique to obtain intermediate text which is ready to transmit over network. At receiver end cover speech and text are acts as input on which segmentation and framing apply on cover speech signal. Perform XOR operation on LSF parameters and the ASCII values of intermediate text. Finally obtain the cipher speech.

Thomas Leontin Philjon. , Venkateshvara Rao. N: The message is converted into a cipher image using a key, hided into another image using Steganography by trasferring it into an intermediate text and finally converted once again into an image. The proposed method thus achieves a high degree of security for information.

Akash V. Malasane, S. P. Bhonge (2013): In this paper first of all the block cipher application, like AES (Advanced Encryption Standard) which is apply to secret message and it will inputted to a LSB (Least Significant Bit) with a frame selection using LSB technique for steganography and this block connected to input video and we will get a result in a hidden. Each frame of the video is first Encrypted using Symmetric Key cryptography; each frame of the encrypted video is further hide with cover image resulting into Steganography image. In such a way all frames of encrypted video is steganography. Finally, the set of all Steganography images (Steganography Encrypted Video or stegano video) is sent to the receiver. In metamorphic encryption technique used two videos first one is embedded video called as video1 and second one is the embedding video called as video2 from this proposed method we do the v1 video will be hidden in the v2 video, video is defined as the collection of images or frames. In this proposed paper we are concentration on hide information or data in Video form using metamorphic encryption technique so that it will provide high degree Security for the important messages that can be transmitted over the network securely.

Dhananjay M.Dumbere, Nitin J.Janwe(2019) : The secret video is encrypted using AES algorithm and further encrypted video is embedded with cover video using LSB Algorithm, it gives double layer security to video files being transmitted over the network. Stego-Encrypted Video is transmitted over the network to the destination where the receiver decodes the Stego-Encrypted video which separates encrypted secret video and covers video and later decrypts the encrypted secret video into Secret video. Here proposed metamorphic cryptography approach is implemented Matlab.

Table 1 : Different techniques of Metamorphic Cryptography.

Sr No	Author Name	Secrete Data	Cover Medium	Cryptography Technique	Steganography Technique
1	Vikas Yadav (2019)	Text	Image	DNA Concept	KIMLA ALGO
2	M. Gajalaskhmi (2018)	Text	Image	Not Available	Not Available
3	Thomas Philjon (2011)	Text	Image	Not Available	Not Available
4	Munesh Chandra Tiwari (2019)	Text	Video	DNA Sequence	LSB
5	Akash Malasane (2015)	Text	Video	AES	LSB with frame selection
6	Munesh Chandra Tiwari (2017)	Text	Audio	ASCII format-->binary fomat--> index based chaotic sequence	LSB with XOR
7	Atul Haribhan Kachare(2014)	Text	Audio	ANY ALGO -->ASCII format-->XOR OPERATION	Calculate LPC-->LSF Parameters->
8	Akash Malasane (2013)	video	Video	AES	LSB
9	Dhananjay M Dumbere (2019)	video	Video	AES	LSB
10	Donga HitendraNanjibhai (2019)	Image/Text/Audio	Image	Blowfish	LSB (7 Bit)
11	Kapil Kapoor	Text	Audio	AES	LWT-DCT
12	Susmits Soni (2014)	Text	Image	Not Available	LSB
13	K. Dhanasekharan(2018)	Text	Image	AES (Honey Encryption)	LSB
14	Orooba Ismaeel (2016)	Text	Image	Trasportation Cipher Method	LSB
15	Shivani, virendra kumar (2015)	Text	Text	Index Based Chaotic Sequence	Abbreviation Method
16	Ako Muhammad (2016)	Text	Image	Affine Cipher Algo	H-LSB

V. Proposed system

The proposed system will provide extra secure data transmission using double layer security with cryptography and Steganography for the video as secret message and video as cover. One by each frame of the secret video is first encrypted, then concealed with a cover video frame, resulting in a Steganography video. All frames of encrypted video are concealed in this way. Finally, the recipient receives the entire collection of Steganography video (concealed Encrypted Video).

VI. Conclusion

We studied existing paper's technologies and algorithm. In this paper we have described the Metamorphic Cryptography techniques in order to provide privacy or security, to sensitive data, which need to be protected before transmission or distribution. From observation it is found that the video is the best when it used as cover medium, as a comparison to image, audio, and text. While doing literature review study got to know that more researchers worked on encrypted data send in various covers like image, audio, text and few worked on encrypted video send with video as medium but there is scope of work for sending video data in hidden encrypted format over network with video as cover as both of authors used same technique for encryption and encoding (AES and LSB).

References:

1. Ki-Hyun Jung (2019) "A Study on Machine Learning for Steganalysis." *Kyungil University*. DOI: 10.1145/3310986.3311000

2. Namrata Singh (2018) "Metamorphic Cryptography" *International Journal of Computer Applications* (0975 – 8887) Volume 182 – No.3, DOI: 10.1109/ICRAIE.2018.8710399.

3. Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, Vineet Kumar Singh (2019) "Video Steganography using Concept of DNA Sequence and Index Compression Technique" *International Journal of Engineering and Advanced Technology (IJEAT*)ISSN: 2249-8958, Volume-8 Issue-5, DOI: D6368048419.

4. Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal (2014) "A Crypto-Steganography: A Survey" IJACSA) *International Journal of Advanced Computer Science and Applications*, Vol. 5, No. 7, DOI: 10.14569/IJACSA.2014.050722

5. M. Gajalakshmi and R. Vidya (2018) "A Review on - Data Hiding using Cryptography and Steganography" *International Journal of Computing Algorithm Volume*: 07, Issue: 01, Page No.24-28 ISSN: 2278-2397,
https://www.researchgate.net/publication/328216431_A_review_on_data_hiding_using_cryptography_and_steganography.

6. Orooba Ismaeel Ibraheem Al-Farraji (2016) "Combination between Steganography and Cryptography in Information Hiding by Using Same Key." *International Journal of Engineering Research and General Science* Volume 4, Issue 6, ISSN 2091-2730, DOI: https://www.researchgate.net/publication/328872949_Combination_between_Steganography_and_Cryptography_in_Information_Hiding_by_Using_Same_Key.

7. Rajeev Gupta, Dr. Vivek Sharma (2017) "A Vision on Text Steganography with proper Investigation Report to Identify the Associated Problem." *International Journal of Computer Trends and Technology (IJCTT)* – Volume 54 Number 1, ISSN: 2231-2803 DOI: 10.14445/22312803/IJCTT-V54P108.

8. Dhananjay M. Dumbere, Nitin J. Janwe(2013) "A Review on Metamorphic Cryptography for Video Files." *IJCSN International Journal of Computer Science and Network,* Volume 2, Issue 6,
ISSN (Online): 2277-5420 ijcsn.org/IJCSN-2013/2-6/IJCSN-2013-2-6-150.pdf.

9. Vikash Yadav and Indresh Kumar Gupta (2019) "A hybrid approach to metamorphic cryptography using KIMLA and DNA concept." Int. J. Computational Systems Engineering, Vol. 5, No. 4, DOI: 10.1504/IJCSYSE.2019.101717.

10. Namrata Singh (2018) "A Survey on Metamorphic Cryptography Concepts and Techniques." *3rd International Conference and Workshops on Recent Advances and Innovations in Engineering, (IEEE Conference Record # 43534)* DOI: 978-1-5386-4525-3/18.

11. Dhananjay M. Dumbere, Nitin J.Janwe(2019) "Metamorphic Cryptography: A Technique for Providing Security on Video Files*" International Conference on Innovation & Research in Engineering, Science & Technology ISSN (e): 2250-3021, ISSN (p): 2278-8719* DOI: http://iosrjen.org/Papers/Conf.ICIREST-2019/Volume-18/6.%2028-38.pdf.

12. Akash V. Malasane, S. P. Bhonge (2015). "Secure Information Transmission Based on Cryptography Fused with Steganography by using Metamorphic Video Encryption." International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

13. Thomas Leontin Philjon., Venkateshvara Rao. (2011) "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption." IEEE-International Conference on Recent Trends in Information Technology, DOI: 978-1-4577-0590-8/11.

14. Mr. Akash V. Malasane, Prof S. P. Bhonge (2015) "A REVIEW PAPER ON SURVEY OF THE SECURE DATA BY USING METAMORPHIC ENCRYPTION" *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*. ISSN: 2277-9655

15. Munesh Chandra Trivedi, Shilpi Mishra and Virendra Kumar Yadav (2017)" Metamorphic cryptography using strength of chaotic sequence and XORing method "Journal of Intelligent & Fuzzy Systems 32 (2017) 3365–3375 DOI:10.3233/JIFS-169277

16. Atul Haribhau Kachare, Mona Deshmukh (2014) "Meatmorphic Cryptography: Fusion of cryptography and Steganography" International Journal of Science and Technical Research (IJETR) ISSN: 2321-0869.

17. D. Chandrasekhar Rao, Amiya Kumar Rath, M. R. Kabat. "CRYPTOGRAPHY AND NETWORK SECURITY LECTURE NOTES." Veer Surendra Sai University of Technology. (Youtube video).

18. Kritika Acharya, Manisha Sajwan, Sanjay Bhargava (2014). "Analysis of Cryptographic Algorithms for Network Security." *International Journal of Computer Applications Technology and Research Volume 3–Issue 2.*

19. Shivania, Virendra Kumar Yadava Saumya Bathamb(2015). "A Novel Approach of Bulk Data Hiding using Text Steganography." *3rd International Conference on Recent Trends in Computing* ISSN: 1877-0509, doi: 10.1016/j.procs.2015.07.457.

20. Harpreet Kaur1, a and Jyoti Rani (2016). "A Survey on different techniques of Steganography." *MATEC Web of Conferences 57*, DOI: 10.1051/matecconf/20165702003.

21. Kapil Kapoor (2019) "Data Security with combination of Cryptography and Audio Steganography.*" National College of Ireland*.

25. Prof. D. Chandrasekhar Rao Dr. Amiya Kumar Rath, Dr. M. R. Kabat." CRYPTOGRAPHY AND NETWORK SECURITY LECTURE NOTES." *Veer Surendra Sai University of Technology.*