International Conference on Innovative Computing and Communication (ICICC 2020)

A survey based on Enhanced the Security of Image using the combined techniques of steganography and cryptography

Mr. Ravi Kumar[1], *Ms. Namrata Singh[#2]

1-MTech 3rd Semester, Department of Computer Science and Engineering, Naraina VidhyaPeeth Engineering & Management Institute, Panki, Kanpur (U.P.), 208003 India, **aryamtech1214@gmail.com**
2-Assistant Prof. Department of Computer Science and Engineering, Naraina VidhyaPeeth Engineering & Management Institute, Panki, Kanpur (U.P.), 208003 India. nam2817120@gmail.com

ABSTRACT:

Steganography is a science and art of concealing the secret data using a cover medium. Cover medium can be of any type like (Text file, Audio File, Image file, and Video File) we can take any one of them to hide our secret data. Several techniques comes under the Steganography which have different pattern to hide the data. Whereas Cryptography is also an art to provide the security of your secret data by various encryption techniques. Several techniques comes under the Cryptography which have also used different methods to provide the security of data. In this paper, I am survey the combined technique used under Steganography and Cryptography through which we can prove more security to our secret data.

Combination of both (Steganography and Cryptography) called metamorphic cryptography which provide a sealed and make more secure your confidential data to decrypt by the attackers.

Keywords— Steganography, Cryptography, Metamorphic Cryptography, LSB, Chaotic Sequence, XOR. Symmetric key, Asymmetric Key. RSA.

INTRODUCTION:

From ancient times to the present years, secure and hidden communication is the Fore mostly requirement of the people. Therefore steganography is becoming very popular by people due to the security issues over internet It is very significant to keep them safe from an unknown access. In this paper I have discussed various steganography techniques and its working and the concept of cryptography techniques.

In this paper, I am just trying to find out which combination of steganography and cryptography techniques work well with some extra operation. Because we know that only concealing the secret data is not enough to provide the security also very significant or we can say that security also play a very significant role. So should use the combined technique of cryptography for encryption and steganography for concealing the secret data.
Some encryption key are used under the cryptography which also comes under the symmetric and Asymmetric key. Some cryptography techniques comes under the symmetric key and some comes under the Asymmetric key in this paper, I am trying to discuss some of them and find out which combination will be best to secure our secret data.

In metamorphic cryptography the plain text is changed into cipher text which is in unreadable form of your confidential message before to conceal into cover medium. Here we try to maintain the quality cover medium after embedding the confidential message so that it become very tough to find it visually or by checking it on various quality parameters like PSNR, MSE, BER, SNR, SSIM.
For the best image quality the value of PSNR (Peak Signal to Noise Ratio) should be higher and MSE (Mean Square Error) value should be lower. The quality of cover medium affects after concealing the data into it because of distortion. SO we always try to minimize the distortion by different distortion techniques which we will discuss in our next paper.
We should always try to secure our data on multilevel so in this paper, I am trying to find out the combination of hiding and encryption techniques with the use of some extra operation through which we can provide multilevel secrecy to our secret data.
Chaotic Sequence is used to encrypt the data.

Formula for the chaotic sequence is stated as follows:

$$X_n = \mu * X_n * (1 - X_n)$$

Where Xn is a number lies between '0' and one that represents the ratio of existing population to the maximum possible population. The values of interest "μ" parameter lie in the interval (0, 4) [3].

1. LITERATURE REVIEW

In [1], authors explore the steganography, its history, features, tools and various techniques like LSB, and XOR used for hiding messages in an image.
In [2], authors explore the steganography, and it's hiding techniques its history, features, tools used for hiding messages in an image.
In [5], authors explore the encryption and decryption keys and used of chaotic sequence and how to recover the hiding message, in digital image.
In [6], authors describes the basics concepts of steganography and cryptography, comparison of both, types of each of them.
In [7] authors describes the basics concepts of steganography and cryptography, comparison of both, types of each of them.
In [8], authors describes the basics concepts of steganography and cryptography, comparison of both, types of each of them and used them for hiding messages in an image.
In [9], authors explore Advancement in Communication.

In [10], authors explore the using different steganographic techniques along with the cryptographic techniques. Steganography conceal the existence of the information whereas cryptography makes the data unreadable making the communication robust.

In [11], authors explore the steganography, cryptography and the different types of techniques used in steganography like LSB, DCT, DWT, using image as a cover medium.
In [12], authors explore the steganography and cryptography defines RSA algorithm for encryption and embedded encrypted data in an image using DCT steganographic technique.
In [13], authors discuss the detailed survey on the steganography techniques and encryption algorithm with their advantages and disadvantages.
In [15], this paper explore a survey on video steganography and its different techniques along with the applications, limitations and comparison.
In [18], authors explore the steganography and cryptography try to secure data by merging the techniques of cryptography in steganography.
In [19], authors proposed a combined system of steganography and cryptography the effect of these two methods to enhance the security of the data.

2. STEGANOGRAPHY

To conceal the confidential message in the cover file (Image, Video, Audio, Text, etc.) that process is called steganography. In steganography the changes are done in the cover file without amending or distorting the message here the cover file undergoes changes. So if the existence is compromised then the secret information is also compromised. Fig. 1 shows the flowchart for the steganographic process. [6].

In this Fig.1 Single Key is introduced which is used to encode/decode the confidential message where the stego-object is the file obtained after conceal the confidential information in the cover file.[7] At the time of decoding the confidential information original cover file is required to regenerate the secret message. [8]

2.1 STEGANOGRAPHY TYPES Fig [1]

- **Image Steganography**: Here an image is used as the cover file the LSB of the image is replaced with the secret message bits.
- **Video Steganography**: In this type video file is used as the cover file increasing the payload of the system which means we can hide more data in video as a video comprises of multiple frames and audio.
- **Audio Steganography**: In this steganography the audio file is used as the cover file. Concealing message in audio is typical as the range of frequencies audible to human are vast so this method is challenging.
- **Text Steganography**: In this steganography the secret message is hidden in the text. It can be done by any means by adjusting the vertical spacing between the lines or between the words or even adjusting the vertical and horizontal length of alphabets.

Above mentioned are the type of steganography now there are various techniques of steganography shown in the Fig. 1 below: [8]

2.2. BASIC MODEL OF STEGANOGRAPHY Fig [2]

Payload: The Secret message which is meant to be sent/transmitted safely is known as Payload. [6]

Cover-file: Cover file is basically the file, which is used to hide or conceal the secret message. It may be image file, video file, text file, and audio file.

Stego-file: Stego-file is the object which carries the encrypted secret message

Stego-key: Stego-key is the key used for encrypting and decrypting the secret message from the stego-file.

Concealing algorithm: Concealing algorithm is the algorithm used to hide or conceal the secret message in the cover medium/object.

Extracting algorithm: It is an algorithm used to unhide/uncover the message or can say that to get the message back from the stego file.

Suppose we want to hide the text messages so we can hide this by choosing the text file, Audio file, Video file, and Image file as a cover medium.

In the same way, suppose we want to hide the image messages we can hide this by choosing the image file and video file as a cover. When we use Text as a cover medium it is known as Text Steganography and when
we use Audio as a cover medium it is known as Audio Steganography and when we choose Video as a cover medium it is known as Video Steganography. [9][10].

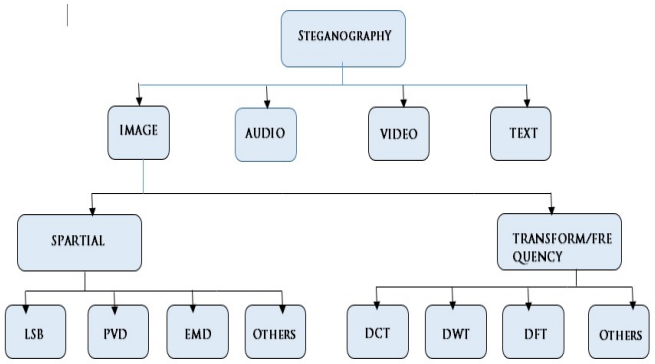


Fig [1]. TYPES OF STEGANOGRAPHY

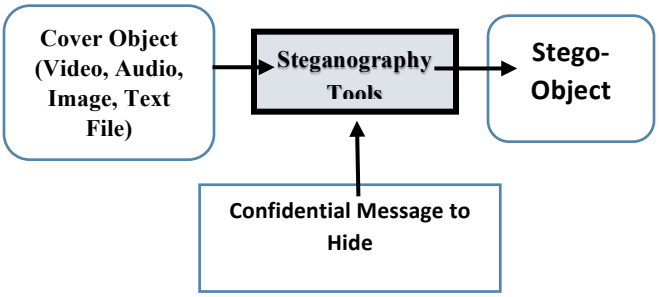


Fig [2]. BASIC MODEL OF STEGANOGRAPHY

2.3 PARAMETERS OF STEGANOGRAPHY

We can evaluate the quality of steganography by using the quality parameters. Which are calculated by the formulas as listed below:
Following equations:

- SNR = 10 $log_{10}(P_{Signal}/P_{noise})$-------- (1)
- $\text{PSNR} = 10\log_{10}\frac{(256)^2}{MSE}$ ---------(2)
- $MSE = \frac{\sum_{MN}[img1(m,n)-img2(M,N)]^2}{\text{M}*\text{N}}$ ---- (3)

Where in the input images M and N are the number of rows and columns respectively in Eq. (3)

Where Psignal and Pnoise are average power of both signal and noise in Eq. (1).

In Equation (3) represents a noise-free M×N monochrome image *x* and its noisy approximation *x*_ [4, 5].

3. CRYPTOGRAPHY

The main objective of cryptography is to hide information so that only the intended recipient(s) can "unhide" it. In crypto terms, the hiding of information is called *encryption*, and when the information is unhidden, it is called *decryption* .In cryptography the message is disguised or distorted using different methods to make it unreadable which can only be decoded using the key used.

The main aim of cryptography is make the message unreadable. In cryptography a key is required for both encryption and decryption. Fig. 3.1 below shows the basic model of the cryptography. [6, 11]
Cryptography is categorized on the bases of the key used for encryption: [11, 12, 18]

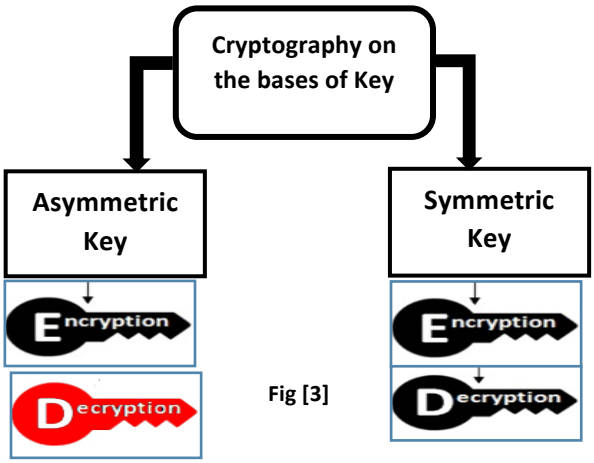


Fig [3]

- **Asymmetric Key**: In this two different keys are used one for the encryption and second for decryption of the information one key can keep public and one secret.
- **Symmetric Key**: In this single key is used for both encryption and decryption this key should be kept secret as it is used for the decryption of the information.

3.1 BASIC MODEL OF CRYPTOGRAPHY Fig [3.1]

Plain Text: The Secret message which is meant to be sent/transmitted safely is known as Plain Text.

Encryption algorithm: It is an algorithm which is used to encrypt the secret plain text into encrypt form.

Key: Which is used for both encryption and decryption of message.

Cipher Text: Cipher text is the encrypted form of plain text.

Decryption algorithm: It is an algorithm which is used to decrypt the cipher text into original form.

4. COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY Fig [4]

As we know that Steganography and cryptography both are differ in steganography that involves transforming the message which is hide into the cover medium so as to make its meaning obscure to malicious people who intercept it. While in cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography techniques that has been used and he is able to read the embedded message. According to [13], steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. Once the encoding system is known, the steganography system is defeated [3]. So from my point of view, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done and then embed the cipher text in the cover medium (Video fie, Audio file, Image file, Text file) or any other media with the help of encryption key. The combination of these two techniques will enhance the security of the data embedded. This combined technique will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel [23]. The fig [4] explain the combined chemistry of cryptography and steganography.

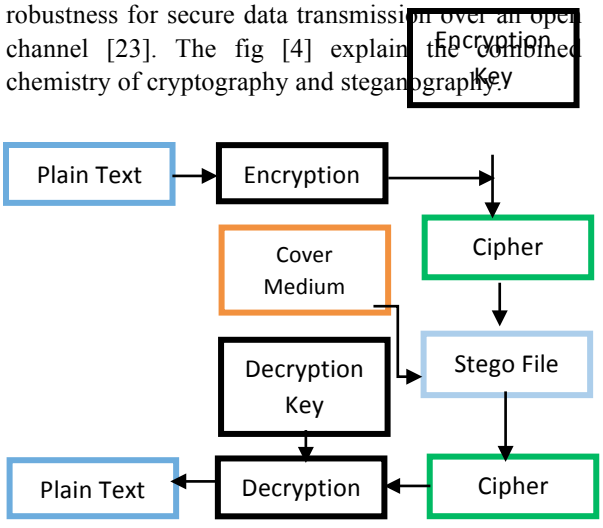


Fig [4] combination of steganography and cryptography

form (text, image, audio, video) it is, what cover medium you have selected, what technique you had used etc. Practically I had observed that the maximum number of redundant bits are present in the video file, then in the audio file, then in the image file and then in the text file, and of course the size of the files is also mattered a lot.

Video file > Audio file > image file > text file

We should always try instead of downloading the text file, image file, audio file, or video file using your own files as a cover medium. It is more secure because it is your files, only you know the details of your files. These files may also in the different extension or formats of text files, image files, audio files and video files. And also after concealing a secret message, you can also edit that particular file.

Several techniques comes under the steganography which are used to hide data. LSB is one of the techniques which comes under the steganography in which secret data bits are hide into the LSB of cover medium which also comes under the Image steganography. The payload capacity of LSB technique is very high. In which first the secret data convert into the binary bits and each binary bits are replaced by the LSB of cover image. Through which we can hide our data and after the embedding the file which is embedding file also known as stego-file to find out the original message from the stego-file first we find the LSB of stego-file and convert each 8-bits into the character and get back the original message. DCT and DWT are also some techniques comes under the image steganography in which first the spatial Domain convert into the frequency domain in this the coefficient of the pixels are used to hide the secret data. Here the techniques comes under the frequency domain are better to conceal but it comes under the lossy compression and low data hiding capacity in comparison of LSB which is comes under the spatial domain has high data capacity. Invisibility is also very high in LSB technique Integrity capacity is also very hish in LSB. Integrity means the protection of data from unauthorized changed. [15][16]

When we discuss the cover file we should always try to tale a cover medium which has a maximum redundant bits. Redundant bits are the bits or bytes that move or generate during the data transfer.in a video file, there are n numbers of frames or images. If we talk about the lump sum figure then there are 536 frames or images in a 10 sec video file. The more the frame is in the video file, the more the redundant bits will be available for hiding the secret message. In a video file, there is also a choice of whether you want to hide your secret message in each frame or in a particular selected frame, both are possible.

When we discuss the Cryptography there are two types of keys comes under this. Fig [3] Symmetric key where single key is used to for both encryption and decryption of confidential data.
In Asymmetric key where two key are used one for encryption the data which is keep public and another is used to decrypt the encrypted message which keep safe. The techniques comes under the Symmetric key are DES, 3-DES, and AES.
DES (Data Encryption Standard) in which the key size is very important here the 56 bits size of key is used to encrypt the plain text into cipher text where the encryption process is done via number of rounds which are 16 (16 Round) in which each input is depend on the output of the find round after 16 round the encrypted message we get means a cipher text comes after 16 round of encryption. In 3-DES, from the name we can check that it is 3 times more secure than the DES here the number of round are 48 and the key size is 112 or 168. But it is slower than the DES so a new technique comes known as AES (Advanced Encryption Standard) in which the number of keys depend upon the number of rounds here there are three types of round if we take 10 round to encrypt the data e take 128 bits of key where data are divided into fixed length data (128-bits), when we take 12 round we take 192 bits of key and when we take 14 round for encryption we take 256 bits of key size to encrypt the data. [15]
RSA encryption algorithm comes under the Asymmetric Key. The name of the algorithm comes after the Surname of the inventers which are (Ron **Rivest,** Adi **Shamir** and Len **Adleman),** in this, technique two keys are used one for encryption and another for decryption here the key size is used in 1024 or 2048 bits in size. Here entire data is encrypted at once mainly used for exchanging the little information such as symmetric keys. [16][15]
We can also use the XOR operation during the embedding process of creating the random key or any other types which provide more security and increase the security level. [16]

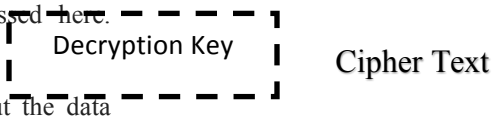
So now metamorphic cryptography is even more secure than both steganography and cryptography individually. In this, I am talking about both steganography and cryptography. There are various hiding and encrypting techniques to provide security to our secret message via using both steganography

and cryptography respectively are discussed here. [17]

In this paper, I have discussed here about the data embedding techniques, encryption techniques, and the combination of both called metamorphic cryptography or crystography in which we learned that the combination of both technique works better in comparison of used them separately.[10] [12] [17]

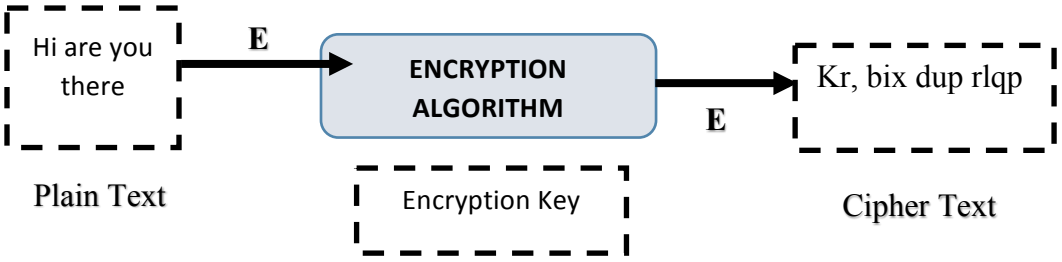
During in my work I have found one thing that when I try to hide some confidential message into another video file, audio file, image file and text file (called cover medium), If the size of the secret message is small, then the image will not be get distorted or less distorted. But if the size of the confidential data is large then there is a maximum chance of getting the distortion or we can say blur. After embedding the confidential message, the frame visually looks like a blur because of the distortion. The unknown person or attacker will easily get to know about it and there will be the maximum chances that he will be able to decode it. So we need to remove distortion from the image so that the unauthorized person or attacker will not be able to guess that there is anything hidden into it at least not by seeing in cover file or medium. [9][16]

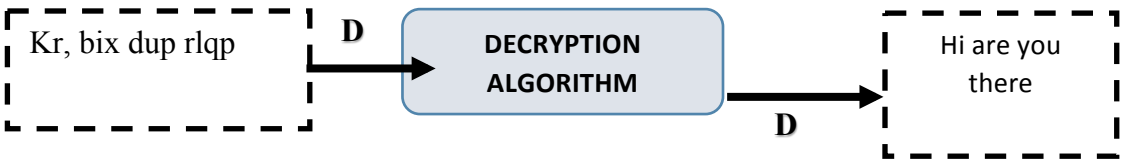
Instead of using the cover medium from the internet or from the public sources, use your own file clicked by your own cell phone, camera or devices. It's make your cover file unique, So that you are the only person who knows about its features, its quality and also you can change it according to your need.



5-CONCLUSION

In this paper, we came to know about the concept of Combination of both steganography and cryptography (Metamorphic cryptography/Crystography), various steganography techniques, the comparison between them, and also how the metamorphic cryptography works better. I also found that the video file is the best when we take it as a cover medium, as a comparison to image, audio, and text. In steganography we can take the LSB technique and for encryption we can take the RSA (Asymmetric Key) with XOR operation which makes your data more secure and tough to decrypt by the atackers. with the combination of any public or private key is used for encryption and also for minimizing the distortion in image, video and also in audio. Instead of using one (steganography, cryptography), use this concept make it more secure.





Plain Text

OBSERVATION TABLE 1.

COMPARISON BETWEEN STEGANOGRAPHY. [6, 7, 11, 13]

S. No.	Steganography	Cryptography
1	Existence of secret information is hidden	Secret message is disguised or written secretly
2	Key is not necessary for encryption	Key is required for encryption
3	Various Cover files are Used (Audio, Video, Text etc.)	It is text based as the message is encrypted
4	Still Under Development for other formats	Most of the algorithms are known
5	Here the cover file is altered keeping secret message intact	Here the message is altered to give it a disguise or make it unreadable
6	Compromised once known about the existence	Compromised once known about the technique used
7	Doesn't require high computing power for decoding	Require high computing cost for decoding
8-Result	Stego File	Cipher Text

FUTURE SCOPE

In my future work I will trying to embed video into the video, keeping in mind that it should have minimum distortion or zero distortion. Instead of using the concept of chaotic sequence for random frame selection and encryption, I will prefer or work on some more encryption techniques and also for random frame selection. In my research, I found that random frame selection is better than sequential frame selection. So I have applied XOR technique for removing the distortion, and also work on different techniques which provide us more security in communication.

REFERENCES:

1. Chandni Arun and Senthil Murugan," Design of Image Steganography using LSB XOR Substitution Method", International Conference on Communication and Signal Processing, April 6-8, 2017. (ICCSP),IEEE-10.1109/ICCSP.2017.8286444

2. Provos, N. & Honeyman, P.,"Hide & Seek: AN Introduction of Steganography", IEEE Security & Privacy Journal. 2003.

3. Abikoye Oluwakemi C.,Adewole Kayode S.,Oladipupo Ayotunde J.,"Efficient Data Hiding System using Cryptography and Steganography",

International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA.

4. Nurhayati, & Ahmad, S. S. (2016). Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm. 2016 4th International Conference on Cyber and IT Service Management. IEEE doi: 10.1109/citsm 2016. 7577468

5. Ogras, H., Turk, M. Digital image encryption scheme using chaotic sequences with a nonlinear function.World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng. **6**(7) (2012).
6. Md. Khalid Imam Rahmani, Kamiya Arora, Naina Pal , A Crypto-Steganography: A Survey, (IJACSA) International Journal of Advance Computer Science and Applications, Vol. 5, No. 7, 2014

7. A. Joseph Raphael, Dr. V. Sundaram, A.Joseph Raphael, Dr.V Sundaram, Cryptography and Steganography – A Survey, International. Journal. Computer. Tech. Appl., Vol 2 (3), 626-630

8. Z. V. Patel, S. A. Gadhiya, A Survey Paper on Steganography and Cryptography, RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ) Volume-2, Issue-5, May-2015 ISSN: 2349-7637 (Online).

9. Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. "A Novel Security Scheme for Secret Data using Cryptography and Steganography", I. J. Computer Network and Information Security, 2012, 2, 36-42, DOI: 10.5815/ijcnis.2012.02.06.

10. Namrata Singh, International Journal of Computer Applications (0975 – 8887) Volume 182 – No.3, July 2018.

11. Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", "International Journal of Engineering Trends and Technology" (IJETT) – Volume 11 Number 8 - May 2014

12. Shailendra M. Pardeshi, "A Survey on Novel Visual Cryptographic Steganography Techniques", International Journal of Computer Applications (0975 – 8887) National Conference on Emerging Trends in Information Technology (NCETIT-2014)

13. A Survey on Cryptography and Steganography, Niveditha R, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

14. Namrata Singh, International Journal of Innovative Research in Science, Engineering and Technology, ISSN (Online): 2319-8753 ISSN (Print): 2347-6710, OI:10.15680/IJIRSET.2017.0602120.

15. Namrata Singh, International Journal of Computer Applications (0975 – 8887) Volume 169 – No.7, July 2017.
16. Namrata Singh, 2017 9th International Conference on Information Technology and Electrical Engineering (ICITEE), Phuket, Thailand.
17. Volume-2, Issue-5, May-2015 ISSN: 2349-7637 (Online) RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ) Research Paper Available online at: www.rhimrj.com 2015, RHIMRJ, All Rights Reserved Page 1 of 5 ISSN: 2349-7637 (Online) A Survey Paper on Steganography and Cryptography Z. V. Patel1st Student, M.Tech. C. U. Shah College of Engineering and Technology, urendranagar, Gujarat (India) S. A. Gadhiya2nd Head, B.E.(IT) C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat (India).

18. Epuru Madhavarao, ChikkalaJaya Raju, Pedasanaganti Divya, A.S.K. Ratnam,"data security using cryptography and steganography", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012.

19. Neha sharma, J.S. Bhatia, Neena Gupta, "An encrypto stego technique based secure dataransmission".

20. Rupali Bhardwaj, Divya Khanna, "Enhanced the Security of Image Steganography Through Image Encryption. 2015 Annual IEEE India Conference (INDICON), 10.1109/INDICON.2015.7443274

21. Piyush Kumar Singh, Ravi Shankar Singh, Kabindra Nath Rai," An Image Encryption Algorithm based on XOR Operation with Approximation Component in Wavelet Transform". Journal of Intelligent Systems 27 (1):81-90 (2018)

22. Arul Thileeban S," Encryption of images using XOR Cipher", International Journal of Advanced Research in Computer Science (ijarcs). Volume 8, No. 7, July – August 2017.

23. Aiswarya, S., & Gomathi, R. (2018). Review On Cryptography and Steganography Techniques in Video. 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). doi:10.1109/iccic.2018.8782409.

24. Piyush Kumar Singh, Ravi Shankar Singh, Kabindra Nath Rai," An Image Encryption Algorithm based on XOR Operation with Approximation Component in Wavelet Transform". 2018 4th International Conference on Computing Communication and Automation (ICCCA) 2018.

25. Subramanyan, B., Chhabria, V. M., & Babu, T. G. S. (2011). Image Encryption Based on AES Key Expansion. 2011 Second International Conference on Emerging Applications of Information Technology. IEEE doi:10.1109/eait.2011.60.

26. Mishra, R., & Bhanodiya, P. (2015). "A review on steganography and cryptography". 2015 "International Conference on Advances in Computer Engineering and Applications". IEEE doi: 10.1109/icacea. 2015.7164679.

27. Joseph, P., & Vishnukumar, S. (2015). A study on steganographic techniques. 2015 Global Conference on Communication Technologies (GCCT). IEEE doi:10.1109/gcct.2015.7342653.

28. Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. "A Novel Security Scheme for Secret Data using Cryptography and Steganography",I. J. Computer Network and Information Security, 2012, 2, 36-42, IEEE, DOI: 10.5815/ijcnis.2012.02.06.

29. Nurhayati, & Ahmad, S. S. (2016). Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm". 2016 "4th International Conference on Cyber and IT Service Management". IEEE doi: 10.1109/citsm.2016.7577468.

30. Abikoye Oluwakemi C.,Adewole Kayode S.,Oladipupo Ayotunde J.,"Efficient Data Hiding System using Cryptography and Steganography", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA.

31. Nandakumar, A., Harmya, P., Jagadeesh, N., & Anju, S. S. (2011). A Secure Data Hiding Scheme Based on Combined Steganography and Visual Cryptography Methods. Communications in Computer and Information Science, 498–505. doi: 10.1007/978-3-642-22714-1_51 (springer).

32. Prema, G., & Natarajan, S. (2013). "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application". 2013 "International Conference on Information Communication and Embedded Systems" (ICICES). IEEE doi:10.1109/icices.2013.6508373.

33. Rangaswamaiah, C., Bai, Y., & Choi, Y. (2019). Multilevel Data Concealing Technique Using Steganography and Visual Cryptography. Advances in Biochemical Engineering/Biotechnology, 739–758. doi: 10.1007/978-3-030-12385-7_53 © Springer Nature Switzerland AG 2020 K. Arai and R. Bhatia (Eds.): FICC 2019, LNNS 70, pp. 739–758, 2020. doi.org/10.1007/978-3-030-12385-7_53

34. A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography – A Survey" IEEE, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630 (IJCT).

35. Joshi, K., & Yadav, R. (2015). A new LSB-S image steganography method blend with Cryptography for secret communication. 2015 Third International Conference on Image Information Processing (ICIIP). doi:10.1109/iciip.2015.7414745 IEEE.

36. Meghrajani, Y. K., & Mazumdar, H. S. (2015). "Hiding secret message using visual cryptography in steganography". 2015 Annual IEEE India Conference (INDICON). doi:10.1109/indicon.2015.7443677.

37. J, G. R., & Ganesh, R. S. (2018). Review of Recent Strategies in Cryptography-Steganography Based Security Techniques. 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET). doi: 10.1109/iccsdet.2018.8821155 IEEE.

38. Philjon, J. T. L., & Rao, N. V. (2011). Metamorphic cryptography — A paradox between cryptography and steganography using dynamic encryption. 2011 International Conference on Recent Trends in Information Technology (ICRTIT). doi:10.1109/icrtit.2011.5972272, IEEE.

39. Kothari, L., Thakkar, R., & Khara, S. (2017). Data hiding on web using combination of Steganography and Cryptography. 2017 International Conference on Computer, Communications and Electronics (Comptelix). doi:10.1109/comptelix.2017.8004011, IEEE.

40. Jonathan Satish, T., Naga Sai Theja, M., Girish Kumar, G., & Thanikaiselvan, V. (2018). Image Encryption Using Integer Wavelet Transform, Logistic Map and XOR Encryption. 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). doi:10.1109/iceca.2018.8474930 IEEE.