Proceedings of the Second International Conference on Artificial Intelligence and Smart Energy (ICAIS-2022)
IEEE Xplore Part Number: CFP22OAB-ART; ISBN: 978-1-6654-0052-7

Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique

Dr. Manish Kumar
Department of CSE
Arya Institute of Engineering & Technology,
Jaipur, Rajasthan, India
manishkrmukhija82@gmail.com

Aman Soni
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
amansonirj0203@gmail.com

Ajay Raj Singh Shekhawat
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
ajayshekhawat49969@gmail.com

Akash Rawat
Department of CSE
Arya College of Engineering and Research Centre,
Jaipur, Rajasthan, India
akrt1192@gmail.com

2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS) | 978-1-6654-0052-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAIS53314.2022.9742942

Abstract: **In the present innovation, for the trading of information, the internet is the most well-known and significant medium. With the progression of the web and data innovation, computerized media has become perhaps the most famous and notable data transfer tools. This advanced information incorporates text, pictures, sound, video etc moved over the public organization. The majority of these advanced media appear as pictures and are a significant part in different applications, for example, chat, talk, news, website, web-based business, email, and digital books. The content is still facing various challenges in which including the issues of protection of copyright, modification, authentication. Cryptography, steganography, embedding techniques is widely used to secure the digital data. In this present the hybrid model of LSB steganography and Advanced Encryption Standard (AES) cryptography techniques to enhanced the security of the digital image and text that is undeniably challenging to break by the unapproved person. The security level of the secret information is estimated in the term of MSE and PSNR for better hiding required the low MSE and high PSNR values.**

Keywords : Steganography, Cryptography, Hiding, Stego Image, Encrypted Image, Decrypted Image.

I. INTRODUCTION

In the time of data innovation, the internet is the main piece of data trade or most well-known way for transferring or sharing the information data [1]. This advanced information incorporates text, pictures, sound, video etc to move over the public organization. The greater part of these advanced media appears as pictures and are a significant part in different applications, for example, talk, news, sites, online business, email, digital books etc [2]. This digital content really faces different troubles, including confirmation, copyright protection issues and more. Various procedures like encryption, hiding, embedding etc can be used to get this advanced information or data. For computerized correspondence applications the image encryption is a significant examination point in the area of cryptography and network security [3]. Here, utilizing the technique, the original digital data is changed over to encrypted data that is totally differing then the original data. For the purpose of the encryption different types of the algorithms and encryption techniques are used.

The image is that the commonest mode of communication utilized in numerous fields like medical, research, industry, military zone, etc. an oversized image transfer can occur in an unsecure web network. Therefore, an applicable lock is needed for the image to forestall unauthorized access to big data. The advantage of the photo is that it covers additional information of the multimedia device and has to be covered [4]. Secret writing can be a reasonable safety method for an image, provides protection through transferring and storing the digital data over the Internet.

II. LITERATURE SURVEY

in [1] different kind of the data hiding methos are presented which provide the security to the digital data using the different steganography techniques. In [2] present a hybrid model of LSB hiding and genetic algorithm encryption technique to provide the security to digital information. For security of the digital data combination of steganography and cryptography is used [3-4, 6]. MSE and PSNR Value is get the 0.055199 and 60.7115, 0.12489 and 57.1654 respectively in [4] and [6]. RSA is one of the best asymmetric algorithms that are very difficult to creak by the unauthorized person, it is mainly used for provide the security to the digital data by encryption decryption operations [5]. In [7] present the CNN based watermarking technique for image security that provide the robustness security to the digital image.

III. OVERVIEW OF CRYPTOGRAPHY

In the cryptography mainly two operations are done at the sender end encryption and at the receiver end decryption. Encryption is the process in which the original data are changed into the totally differ from the original data and in decryption process get the original data from the encrypted

data. For encryption and decryption purpose different types of the algorithm are used like Advanced Encryption Standard algorithm, Genetic algorithm, Choas Mathematical algorithm, RSA algorithm and more [5]. These cryptography algorithms and techniques are categorized into symmetric and asymmetric.

A. Symmetric Key Cryptography

Between the sender and receiver only one key is used for digital data encryption and decryption purpose in symmetric key cryptography.

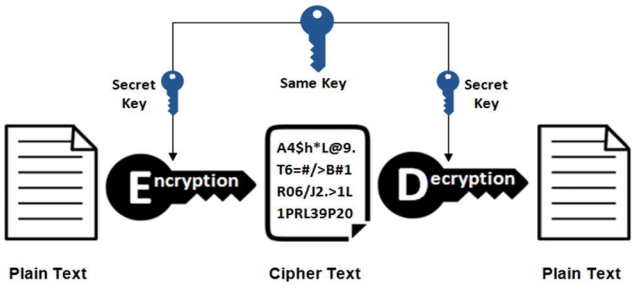

Fig. 1.Symmetric Key Cryptography

B. Asymmetric Key Cryptography

Between the sender and receiver different key are used for digital data encryption and decryption purpose in asymmetric key cryptography. These key are called public and private key.

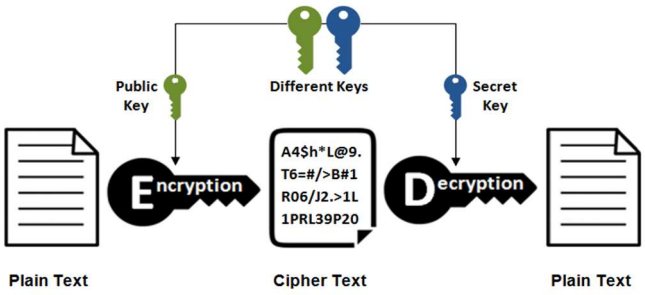

Fig. 2.Asymmetric Key Cryptography

IV. Overview Of Steganography

From the two Greek words the word Steganography comes that words are stego and graphic. The word stego means cover and the word graphic means meaningful writing. So it means that the meaningful writing hidden in the cover is called Steganography [6]. Basically Text, image, audio and video these four types of steganography is categorized [8].

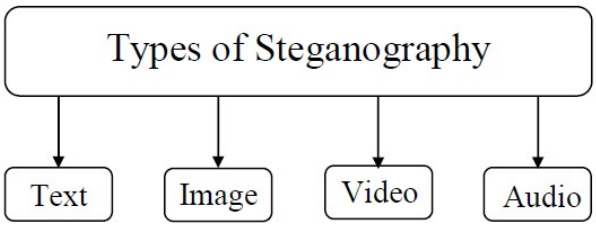

Fig. 3.Types of Steganography

V. Least Significant Bit (LSB) Technique

There are various methodologies of performing Steganography, but the most frequently used is the LSB algorithm. This method alters the LSB of dissimilar bytes with a bit from the message that will be concealed. The main advantage of using LSB is its easy implementation and it also permits high perceptual transparency. The message-hiding ability of the LSB technique is highly secure [9-10].

LSB is the most acceptable and simple approach used in steganography. This technique makes use of LSB of the original cover image's pixels. The LSB steganography technique uses the LSB substitution procedure. The resulting image is termed as "Stego Image" which is similar to the original image having hidden data into it.

1	0	0	1	0	1	0	**1**

Binary data contain LSB and MSB bits. Least significant bits (LSB) are the one which is present at the rightmost side of the binary data and the most significant bits (MSB) are the one which is present at the leftmost side of binary data.

The reason behind using the LSB technique is that if we change the LSB bit it will have less impact on the final result. In contract, if we flip the MSB bit it will have a large impact on the final image.

VI. AES Cryptography Technique

AES has been adopted by the US Government and is currently used worldwide. It replaces the information encoding normal, revealed in 1977. The rule represented by AES may be a bilaterally symmetrical key technique, which implies that identical secret's accustomed write in code and rewrite the information.

In the US, on Gregorian calendar month twenty six, 2001, government agency proclaimed the name America FIPS tap house 197 (FIPS 197) within the us. This announcement followed a five-year standardization method throughout that the chosen Rijndael Fig was obtained because the most applicable.

Each tour includes many process steps, together with those supported constant secret writing key. A group of reverse tours is applied to convert the encoded text back to unformatted native text victimization constant secret writing key.

Symmetric AES writing in cluster, there are 3 varieties of key length during this committal to writing method: 128 bit, 196 bit and 256 bit, packet size is 128 bit, and the algorithmic rule has smart flexibility. This is often why it's wide employed in the program. The length of 3 keys of the AES algorithmic rule, 128 bits. Key length is often used. In key length, ten times recurrent calculation within the internal algorithmic rule. Till the ultimate spherical, every spherical consists of 5 parts: S-Box, Shift Rows, Shift Column, and therefore the main addition stage [6, 11].

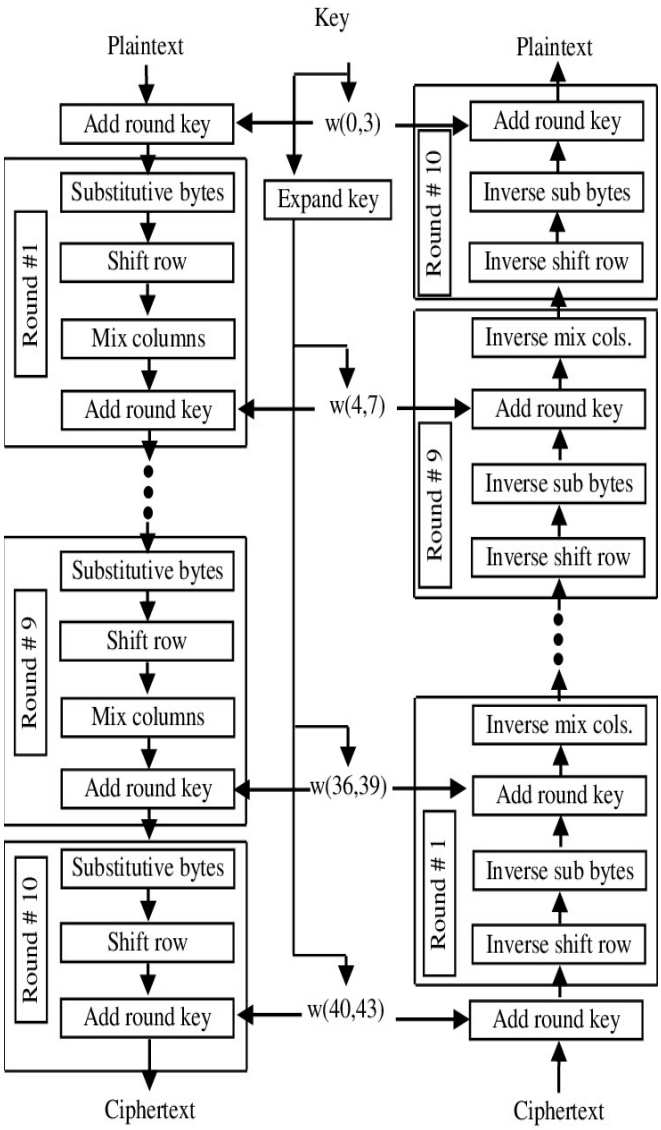

Fig. 4.Flowchart of Propsoed Technique

VII. Proposed Technique

In this proposed work hybrid model of steganography and cryptography is used to enhanced the security to the digital data which mean that it provides multi layers of protection which is very difficult to crack by the unauthorized person.

In proposed work first hide the secret text data into the cover picture using the LSB steganography technique and resultant obtained the stego picture. The stego picture showed same as the cover picture however it comprises of the secret text data moreover. Presently in the wake of getting the stego picture ascertain the worth of MSE and PSNR values where low MSE and high PSNR values esteem is required for better hiding. Now apply the cryptographic techniques in the stego picture and get the encrypted or scrambled picture. For encryption purpose AES algorithm is used. By using this proposed technique achieve the very high level and robust security of secret text and image that is extremely challenging to break by the unapproved person.

In the Fig 5 displayed the proposed used technique flowchart.

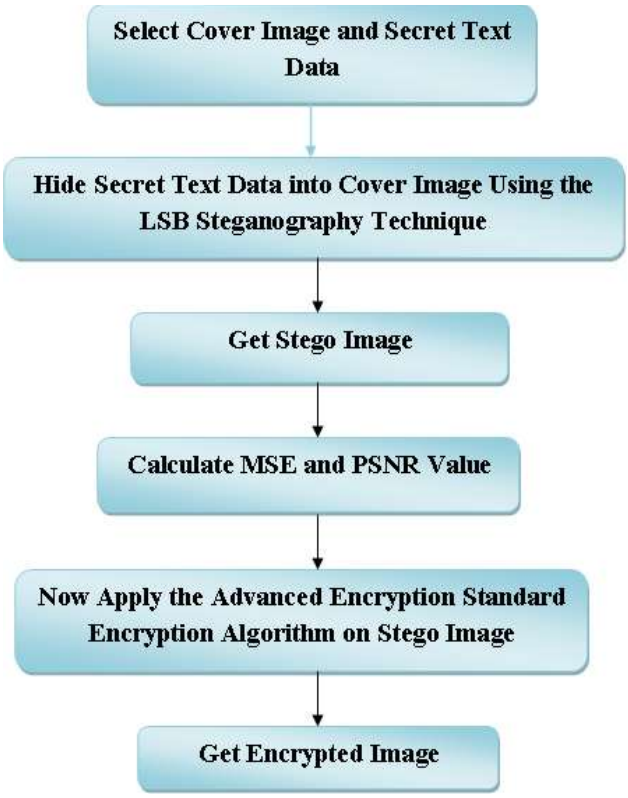

Fig. 5.Flowchart of Propsoed Technique

VIII. Result of Proposed Technique

In the fig 5 showed the flowchart of the proposed plan method for picture and text data security. Presently first select the cover picture of nature view (displayed in the Fig 6) and in Fig 7 displayed the secret text data.

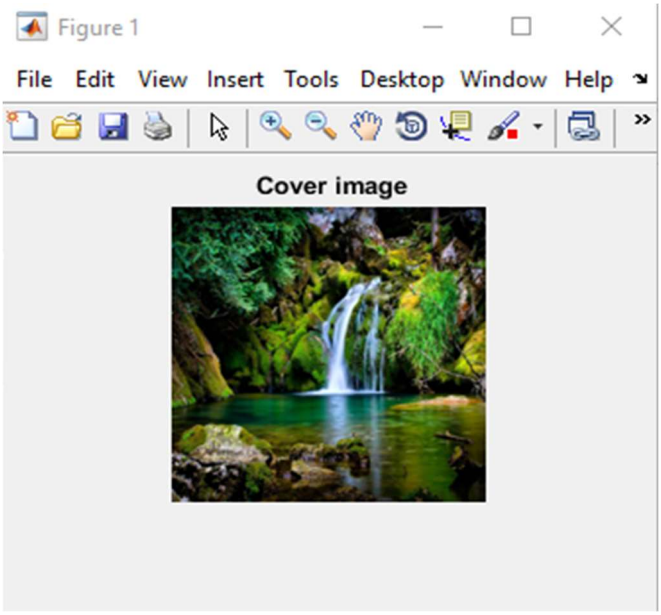

Fig. 6.Cover Image of Nature View

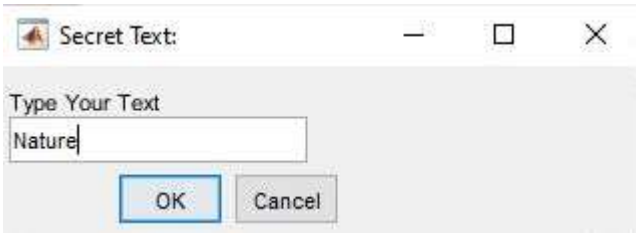

Fig. 7.Secret Text

Now apply the LSB Steganography algorithm on Secret Text and Cover image. In the wake of applying LSB steganography method gets the stego picture that is shown same as the cover picture yet it additionally comprises of the secret text. The Stego Image is shown in the Fig 8.

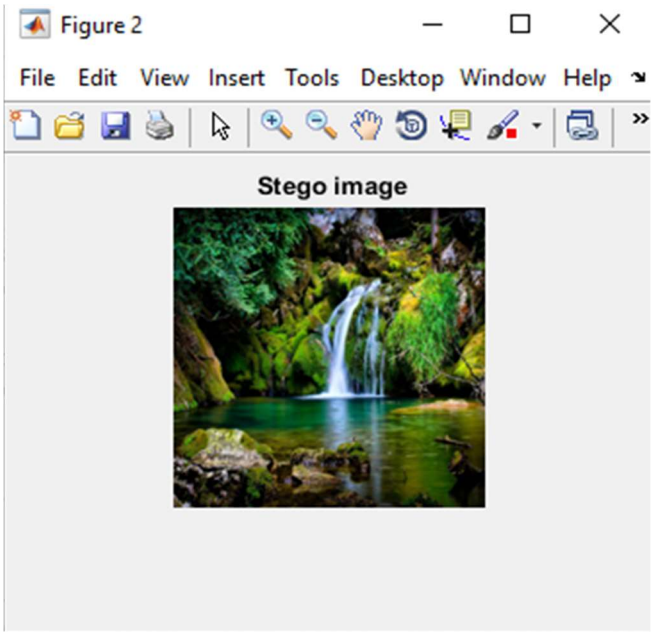

Fig. 8.Stego Image

When get the stego image calculate the MSE and PSNR value which is displayed in Fig 9. Using proposed technique got the MSE value is 0.0019922 and PSNR value is 75.1375.

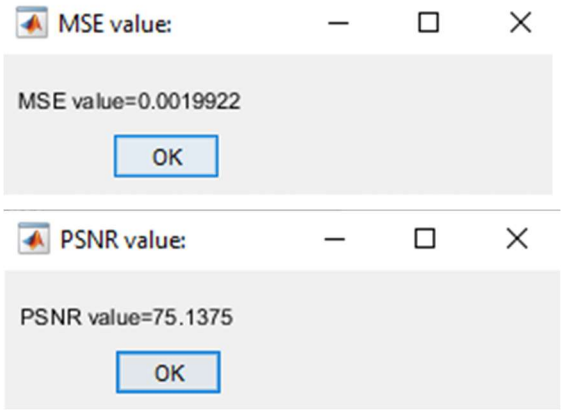

Fig. 9.Obtained MSE and PSNR Value

Now apply the AES algorithm on the stego image and get the encrypted or scrambled picture that is thoroughly vary then cover image and stego image. The encrypted image is displayed in the fig 10.

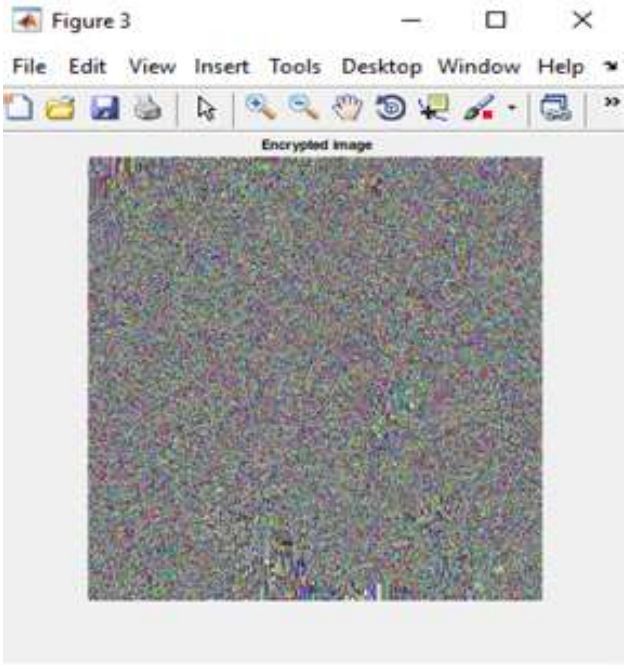

Fig. 10.Encrypted Image

These all the process done at the sender end, in which the secret text data and cover image are send to the one person to another person securely. At, the receiver end done the reverse of this process in which get the decrypted cover image, and decoded secret text data. In Fig 11 displayed the decrypted cover image and in fig 12 displayed the secret text data (Nature).

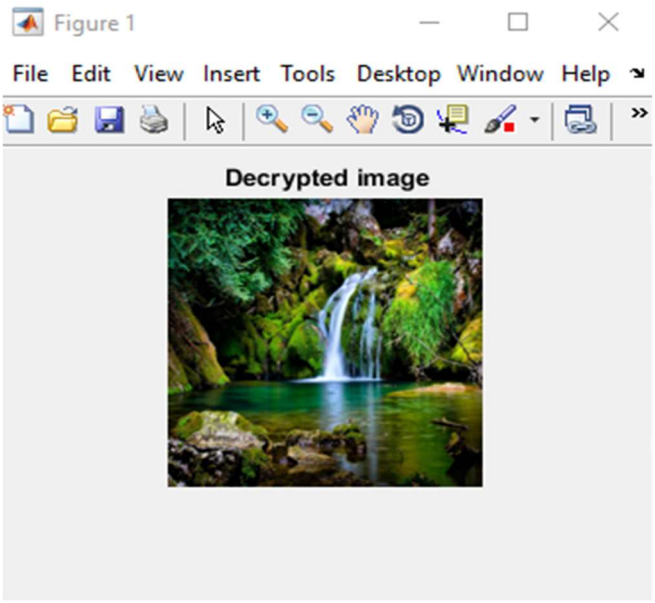

Fig. 11.Decrypted Image

Fig. 12.Decoded Secrt Text Data

IX. Conclusion

In the proposed work the crossover model of the steganography and cryptography is utilized to give greater security to the digital data which imply that it gives multi-facets of assurance which is truly challenging to break by the unauthorized person. For stegnography purpose LSB technique is used and for cryptography purpose AES algorithm used. Using proposed technique got the MSE value is 0.0019922 and PSNR value is 75.1375. For better hidding low MSE and high PSNR parameters value is required. In this proposed work acquired higher MSE and lower PSNR value then the past work done and displayed it in Table 1. So enhance the security of the secret text data by using the proposed technique. In proposed work provide the two layer security to the secret text data using hiding and encryption. By using this proposed technique achieve the very high level and robust security of secret text and digital image that is extremely challenging to break by the unapproved person.

TABLE 1. COMPARATIVE ANALYSIS OF MSE AND PSNR WITH PREVIOUS WORK AND PROPOSED WORK

Ref No.	Year	Used Algorithm/Technique	MSE Value	PSNR Value
4	2021	DCT, LSB	0.055199	60.7115
12	2021	LSB	0.176664	56.053304
13	2021	DCT, XOR, Arnold	0.074	59.47
6	2020	LSB	0.12489	57.1654
Proposed Work		**LSB, AES**	**0.0019922**	**75.1375**

References

[1] Dr. Harish Nagar Manish Kumar, Dr.Sunil Kumar,"Comparative Analysis of Different Steganography Technique for image or Data Security", International Journal of Advanced Science & Technology (IJAST), Vol.-29, Issue-4, 2020.

[2] Soni G.K., Rawat A., Jain S., Sharma S.K., "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique", Smart Systems and IoT: Innovations in Computing. Smart Innovation, Systems and Technologies, vol 141, 2020.

[3] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1153-1157, 2021.

[4] Arpita Tiwari, Gori Shankar and Dr. Bharat Bhusan Jain, "Digital Image and Text Data Security Improvement Using the Combination of Stenography and Embedding Techniques", Design Engineering, Issue-7, pp-8592- 8599, 2021.

[5] Gaurav Kumar Soni, Himanshu Arora and Bhavesh Jain, "A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm", Springer International Conference on Artificial Intelligence: Advances and Applications 2019 Algorithm for Intelligence System, pp. 83-90, 2020.

[6] Matted S., Shankar G., Jain B.B., "Enhanced Image Security Using Stenography and Cryptography", Springer Computer Networks and Inventive Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 58, 2021.

[7] Dhaya, R. "Light Weight CNN based Robust Image Watermarking Scheme for Security", Journal of Information Technology and Digital World 3, no. 2, pp. 118-132, 2021.

[8] Manish Choubisa and Gaurav Kumar Soni Vipin Singh, "Enhanced Image Steganography Technique for Hiding Multiple Images in an Image Using LSB Technique", TEST Engineering & Management, Vol-83, May-June 2020.

[9] Areesha Anjum and Saiful Islam, "LSB Steganalysis Using Modified Weighted Steno Image Method", IEEE 3rd International Conference on Signal Processing and Integrated Networks (SPIN), PP-630-635, 2016.

[10] Swati Bhargava and Manish Mukhija, "Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography", ICTACT Journal On Image And Video Processing, Volume: 09, Issue: 03, pp. 1940-1946, Feb 2019.

[11] Qi Zhang and Qunding, "Digital Image Encryption Based On Advanced Encryption Standard (AES) Algorithm", IEEE Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control, pp-1219-1221, 2015.

[12] Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur and Pulung Nurtantio Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility", Journal of King Saud University –Computer and Information Sciences, PP-1-10, 2021.

[13] Manish Kumar, Dr. Sunil Kumar and Dr. Harish Nagar, "Enhanced Text and Image Security Using Combination of DCT Steganography, XOR Embedding and Arnold Transform", Design Engineering, pp. 732 - 739, 2021.