International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Securing Data in Images Using Cryptography and Steganography Algorithms

[1]Dr. Pooja Bagane, [2]Dr. S. Venkatesh, [3]Dr. John Babu Guttikonda, [4]Arti Badhoutiya, [5]Arun Pratap Srivastava, [6]Akhilesh Kumar Khan, [7]A. Deepak, [8]Dr. Anurag Shrivastava

Submitted: 10/12/2023 **Revised**: 22/01/2024 **Accepted**: 01/02/2024

Abstract: In today's world, there has been a tremendous increase in the usage of the internet and different kinds of networks to transfer data from one place to another with accuracy and speed. With this rapid growth of the internet and increase in digitalisation, we have entered a time where colossal amounts of data that are transferred via the networks are at constant risk. Transference of data across insecure pathways puts the security of the data in jeopardy. Cryptography and Steganography are two of the many methods that help secure data and protect it from being accessible to intruders or third parties while transmitting it over an open channel or any network. In this paper, a Hash Least Significant Bit (H-LSB) along with Vigenère cipher algorithm has been proposed for providing additional security to data. The paper proposes a system which uses a multi-layer security technique using cryptography and steganography that aims to enhance data security, making it safe and more secure to transfer across open channels or other networks.

Keywords: *Cryptography, Steganography, Vigenère Cipher, Hash based LSB, Encryption, Decryption, Embedding process*

1. Introduction

Information security during transference has become a requisite in recent times. Cryptography and steganography are two methods that help transfer or share the information from one user to another in a concealed manner.

Cryptography is a technique that uses plaintext and modifies it into something that only the intended receiver can decipher using the encryption key. Without the encryption key, the message cannot be decrypted. Today, there are many cryptography techniques which are capable of encrypting data, one of them is the Vigenère cipher algorithm. Vigenère cipher has the ability to convert the information to a form that cannot be understood by an intruder or third party. In cryptography, it is always clear to any intermediate person that the information being transferred is in encrypted form and that the encryption key used is known only to the sender and the receiver. Due to this, cryptography alone is not enough to protect information or data from intruders or unauthorized users.

To conceal data, there is another method used called steganography. Steganography is the art of concealing information in an image with no traceability in a manner that no one except the intended recipient will know if there is any information hidden in the image being transferred. It is hidden in such a way that it appears as if no message is hidden in it. This method is used to transmit sensitive information over open/insecure channels.

This paper proposes a system which uses both of the above-mentioned techniques to provide multi-layer security. Our system has been designed to encrypt the information and embed it in an image to protect it. The system takes the information from the user and encrypts it using the Vigenère cipher algorithm. This encrypted message is then embedded in an image using a Hash based (3,3,2) LSB insertion method. The system ensures that there is no modification done to the information and ensures almost zero distortion to the original image.

2. Literature Review and Research Gaps

2.1 Literature Review

G. Prashanti and K. Sandhyarani, et al. [1] proposed employing LSB Steganography to hide data. They

[1]*Department of Computer Science, Symbiosis Institute of Technology, (SIT) affiliated to Symbiosis International (Deemed University), Pune, India*
poojabagane@gmail.com
[2]*Assistant Professor, Department of Data Science and Business Systems School of Computing SRM Institute of Science and Technology kattankulathur, Chennai*
venkyjep2019@gmail.com
[3]*Professor & Principal, Department of CSE, Vijaya Engineering College, Tanikella, Khammam – 507305, Telangana*
johnbabug@gmail.com
[4]*Department of Electrical Engineering, GLA University, Mathura*
arti.badhoutiya@gla.ac.in
[5]*Lloyd Institute of Engineering & Technology, Greater Noida*
apsvgi@gmail.com
[6]*Lloyd Law College, Greater Noida*
hod@lloydlawcollege.edu.in
[7]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamilnadu*
deepakarun@saveetha.com
[8]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu*
**anuragshri76@gmail.com*

talked about how enhancements like high resilience, large embedding capacity, and un-detectability of buried information improved steganographic outcomes. During this approach, two novel strategies were also proposed. The hidden messages were embedded in the cover picture using the first approach, and a secret gray scale image was embedded in another grayscale image using the second technique. Four state tables were utilized to generate pseudo random numbers, which were then used to incorporate the secret information.

Kazem Qazanfari and Reza Safabakhsh, et al. [2] provided an enhanced version of the LSB approach in which they distinguished between sensitive pixels and safeguarded them from additional bit embedding, resulting in lesser co-occurrence matrix distortion. The DCT coefficients of JPEG 3 format photos were also preserved using this approach. In comparison to the prior LSB methodology, this new method produced less traces in the co-occurrence matrices.

N. Akhtar [3] described and implemented an upgraded version of the classic LSB image steganography approach, in which they used the bit inversion method to increase the quality of the steganography picture. They discovered two strategies for bit inversion. Both systems were based on bit inversion techniques, in which the LSBs of carrier image pixels only appeared with a specified pattern of pixel bits if they were inverted. In comparison to the previous LSB technique, this resulted in less pixel mutation.

H. Yang et al. [4] proposed a novel adaptive LSB-based picture steganography algorithm. To increase steganography image quality, it employs the pixel correction approach. This adaptive LSB approach yields a large amount of hidden capacity. To disguise the data, he employed a common bit pattern. As a result, the LSB pattern bits of pixels and the message are changed.

S. M. M. Karim et al. [5] suggested a strategy for securing secret data that was extremely effective. They employed a secret key and an LSB technique. The sensitive information was hidden behind this secret key, which was saved on various LSB bits of the picture. The embedding method in this steganography technology employed RGB real colour photos. The secret information was embedded in the LSB of the cover picture using this approach, and a secret key was used to encrypt the secret information to prevent unwanted access.

2.2 Research Gaps in Encryption systems using cryptography

These gaps are usually found in systems that use only cryptography. As time passes, all cryptographic systems become more susceptible as a result of assaults. And thus, encryption technologies that were deemed strong in one time will almost certainly become weak in subsequent periods.

3. Proposed Methodology

3.1 Encryption phase

The algorithm for cryptography is implemented first. The information that the user wants to secure is taken from the user. Using an encryption key, the information is converted into an encrypted message. This is done using the Vigenère cipher algorithm. It is a kind of polyalphabetic cipher. A polyalphabetic cipher is a cipher that uses multiple cipher alphabets. Each key consists of m characters called keywords. The cipher encrypts m characters at a time. The information is encrypted using a cipher key into ASCII code. This encrypted message is the message that will be hidden in an image. The encrypted message is taken and an original image file is taken from the user and is fed into the steganographic encoder as input.

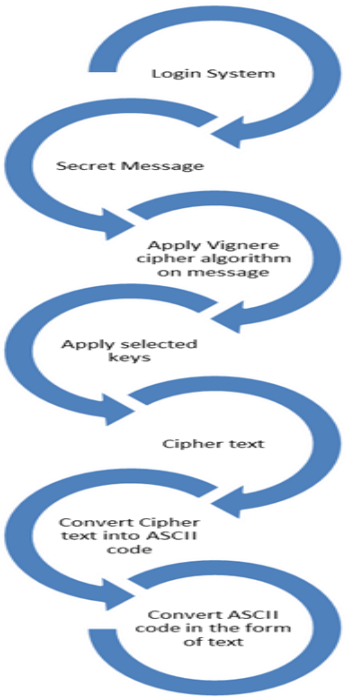

Fig 1: Flowchart illustration of encryption phase for cryptography

3.2 Embedding phase

Embedding of the encrypted message in the given image file is done by using Hash based Least Significant Bit that replaces the least significant bit. It is the most popular steganography method to embed data in an image file. The least significant bit technique is a technique in which the last bit of each pixel is modified and replaced with the encrypted message data bit. A hash function is used to select positions to hide data. The proposed technique takes eight bits of encrypted message at a time and embeds it in the least significant bit of the RGB (Red, Green, Blue) pixel value in the order of 3, 3, 2 respectively. Three bits of the encrypted message are embedded in red pixel LSB, three bits of the encrypted message are embedded in green pixels and 2 bits of the encrypted message are embedded in blue pixels LSB. The eight bits are inserted in this order since the chromatic influence of blue color to the human eye is more than red and green colors. 2 bits are chosen by the distribution pattern to be hidden in blue pixels. Thus, the quality of the image is not tampered with and there is almost zero distortion. This process continues till the entire encrypted message is embedded in the image.

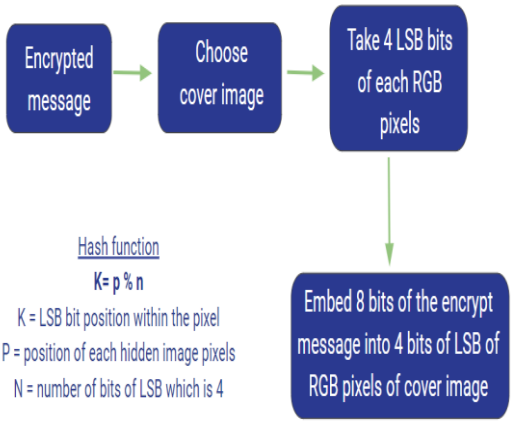

Fig 2: Flowchart illustration of embedding phase

3.3 Decryption phase

To detect the positions of the LSB's where the encrypted message bits have been embedded, the hash function is used again. The bits are extracted from the position in the same order as they were embedded, when the position of the bits had been specified. The encrypted message will be obtained. Using the decode function of base64 and encryption

key, the receiver will be able to decrypt the information.

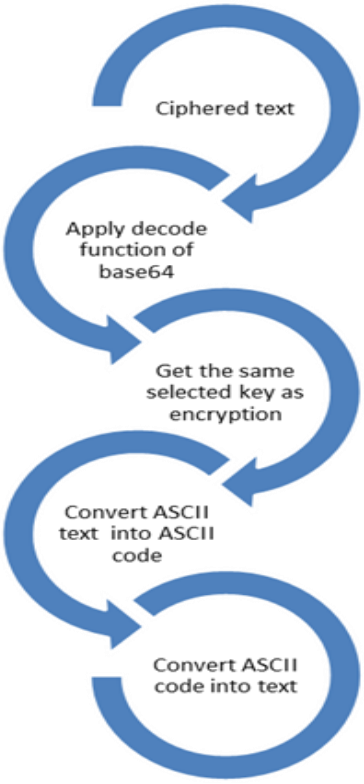

Fig 3: Flowchart illustration of decryption phase of cryptography

4. Implementation Details

4.1 Vigenère Cipher

Encryption

The plaintext(P) and key(K) are added . This answer modulo 26 is done.

Ei = (Pi + Ki) mod 26

Decryption

Di = (Ei - Ki + 26) mod 26

Encryption Code for base64 :

```
enc = []
  for i in range(len(clear)):
  key_c = key[i % len(key)]
  enc_c = chr((ord(clear[i]) +
                              ord(key_c)) % 256)
  enc.append(enc_c)
  return
base64.urlsafe_b64encode("".join(enc).encode()).decode
()
```

Decryption Code for base64:

```
dec = []
enc = base64.urlsafe_b64decode(enc).decode()
for i in range(len(enc)):
 key_c = key[i % len(key)]
 dec_c = chr((256 + ord(enc[i]) -
                              ord(key_c)) %
256)                    dec.append(dec_c)
return "".join(dec)
```

4.2 Algorithms

Encryption using Vigenère Cipher

Step 1: Start

Step 2: Get plaintext from the user.

Step 3: Get the encryption key

Step 4: Plaintext(P) and key(K) are added

This answer modulo 26 is done

Ei = (Pi + Ki) mod 26

Step 5: Conversion of ciphered text into ASCII text.

Example:

Input text: Symbiosis

Output text: gwpXCnMKiwqbCnMKm

Embedding encrypted message in image

Step 1: get the ASCII ciphered text in the steganographic coder

Step 2: Choose image in PNG format

Step 3: Take last 4 LSB bits of each RGB pixel (Red, Green, Blue)

Step 4: Embed 8 bits of encrypted message into 4 bits of LSB of RGB pixels of image.

Step 5: Save image (PNG format) to desired folder

Decryption of encrypted message from image and using Vigenère Cipher

Step 1: Obtain the image in which the message is encrypted

Step 2: Detect 4 LSB bits of each RGB pixels from this image

Step 3: Apply hash function to obtain the position of LSB with hidden data

Step 4: Retrieve the bits in the order 3,3,2 respectively.

Step 5: Convert the bits into ASCII code

Step 6: Apply Vigenère Cipher to decrypt the retrieved data (encrypted message)

5. Results and Discussion

Based on the proposed methodology, we have developed a system. Pre-requisites of using this system are: Information that needs to be secured, an image that can be used in steganography.

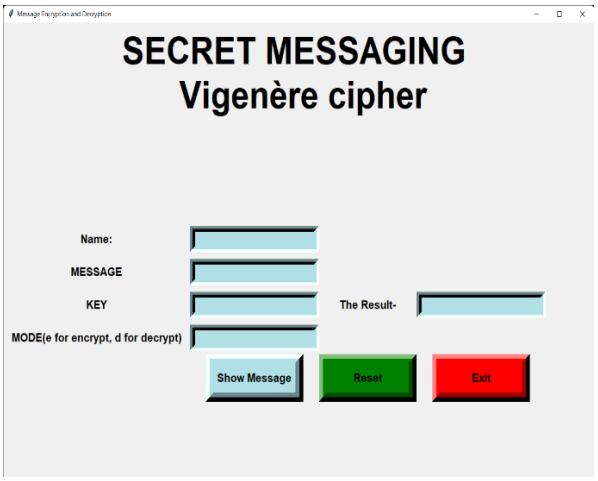

Fig 1: Launching Cryptography Application

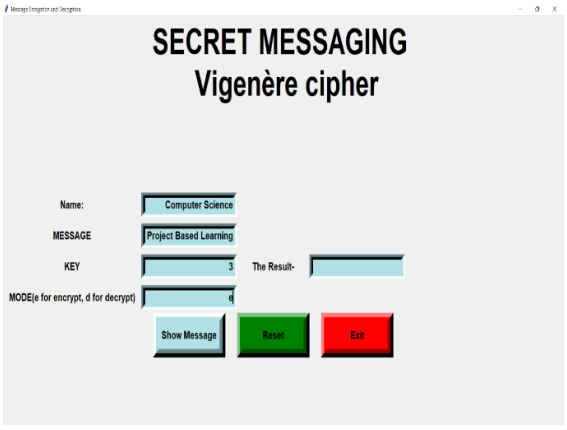

Fig 2: Input the information to be secured and input encryption key.

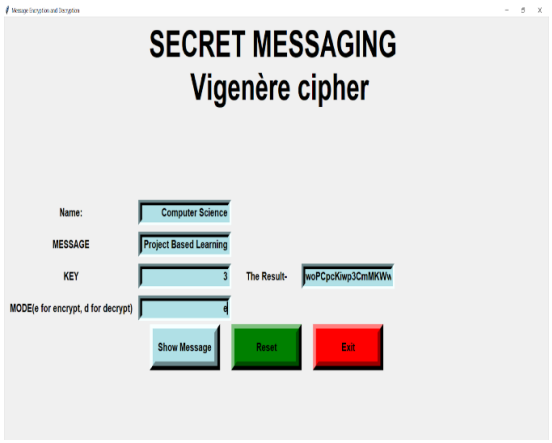

Fig 3: The encrypted message is displayed.

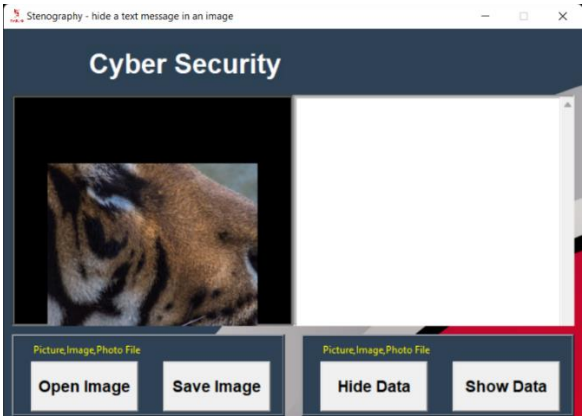

Fig 4: Launch steganographic coder and open image

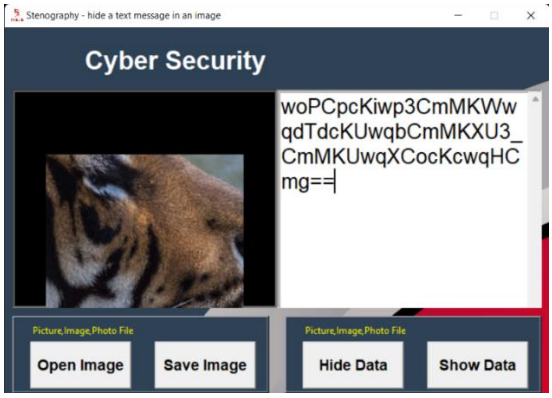

Fig 5: Input the encrypted message to hide in the image

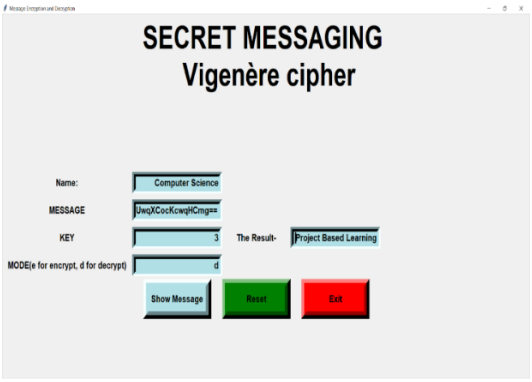

Fig 7: Decryption of message

After the hidden image is saved, in the same steganographic coder, the new image is input. When we click on show data, it shows the encrypted message. This is input in the cryptography application and we get the original message that was encrypted.

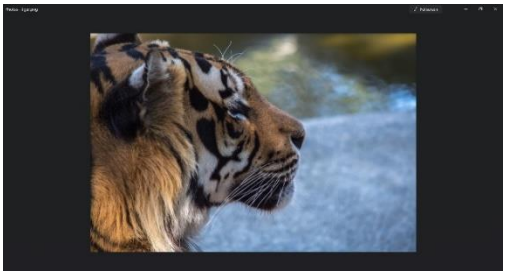

Fig 8: original image taken

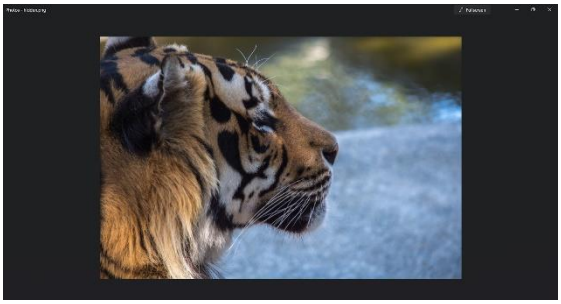

Fig 9: image after the encrypted message is hidden in it

Comparison between figure 8 and figure 9 shows that there is almost zero distortion in the image. This will make it harder for any intruder to catch on that there is any message hidden in the image.

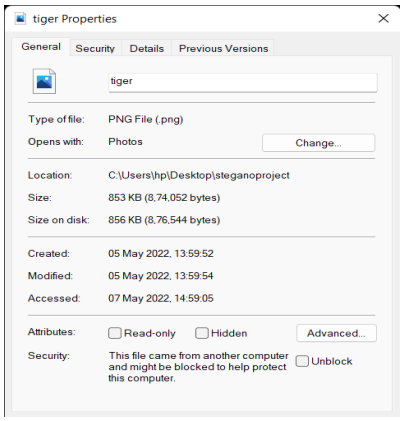

Fig 10: Details of original image

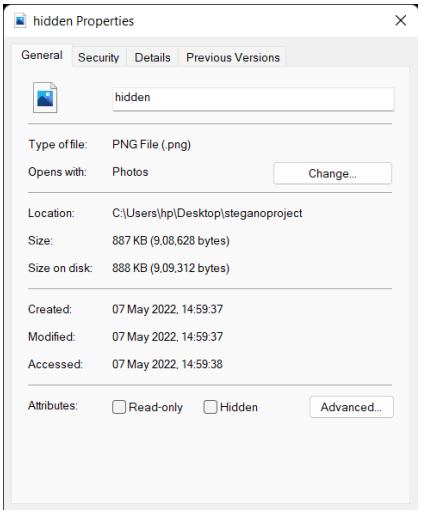

Fig 11: Details of image in which the encrypted message is hidden.

Figure 10 and figure 11 show that both the images have different file sizes. The image file named hidden has a larger size than the image named tiger which is the original image. This indicates that there is some information that has been encoded or hidden in the image named hidden (figure 11)

6. Conclusion

In this paper, cryptography and steganography techniques have been proposed for providing greater security to data. With the proposed system, data is secured with multi-layer security and can be transferred via open channels or any other networks. The main focus of this paper is to develop a system that has enhanced security capabilities for hiding secret communications from attackers. The has the ability to safeguard communications by encrypting data using a mix of Vigenère cipher and least significant bit steganography techniques in our system application. It encrypts information so that only the sender and intended recipient of the message can see it. To decode the secret communication, the recipient is given a unique key. In an insecure network environment, this protects data sent between the sender and the recipient from being hacked by an intruder. After the secret data is embedded in the image after steganography, we receive a new image in our system which has no visible changes in image quality. It makes for an effective way for concealing ciphered data within an image. To evaluate the system, we tested a number of images with different sizes of data to be hidden with the proposed algorithms. According to the test we found that the system is capable of providing improved security and a simple approach to encrypt, embed, and decrypt secret communications with almost zero change in the quality of the image. Thus, this system is very efficient in providing enhanced security.

References

[1] M. Mukhedkar, P. Powar and P. Gaikwad, "Secure non real time image encryption algorithm development using cryptography & steganography," *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1-6, doi: 10.1109/INDICON.2015.7443808.

[2] S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar, "Enhancing security of images by Steganography and Cryptography techniques," *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp. 531-534, doi: 10.1109/INTECH.2016.7845050.

[3] M. Dahiya and R. Kumar, "A Literature Survey on various Image Encryption & Steganography Techniques," *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 310-314, doi: 10.1109/ICSCCC.2018.8703368.

[4] Jui-Cheng and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption," *2000 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2000, pp. 49-52 vol.4, doi: 10.1109/ISCAS.2000.858685.

[5] R. I. Masya, R. F. Aji and S. Yazid, "Comparison of Vigenere Cipher and Affine Cipher in Three-pass Protocol for Securing Image," *2020 6th International Conference on Science and Technology (ICST)*, 2020, pp. 1-5, doi: 10.1109/ICST50505.2020.9732873.

[6] L. Voleti, R. M. Balajee, S. K. Vallepu, K. Bayoju and D. Srinivas, "A Secure Image Steganography Using Improved Lsb Technique And Vigenere Cipher Algorithm," *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2021, pp. 1005-1010, doi: 10.1109/ICAIS50930.2021.9395794.

[7] Bhatt Santhosi, Ray Arghya, Ghosh Avishake, Ray Ananya, “Image Steganography and Visible Watermarking using LSB Extraction Technique”, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), 2015.

[8] Karim Masud S.M, Rahman Saifur Md, Hossain Ismail md, “A New Approach for LSB Based Image Steganography using Secret Key”, Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 201 I) 22-24 December, 2011, Dhaka, Bangladesh.

[9] Thangadurai K, Devi Sudha G , “An analysis of LSB Based Image Steganography Techniques”, International Conference on Computer Communication and Informatics (ICCCI -2014),Jan. 03 – 05, 2014.

[10] Jain Mamta, Lenka Kumar Saroj, “Digital Image Steganography using RGB Color Model: A Review”, International Journal of Applied Engineering Research (IJAER).

[11] Kavita Kadam, Ashwini Koshti and Priya Dunghav.” Steganography Using Least Significant Bit Algorithm”, Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun (2012): 338-341

[12] Kousik Dasgupta , J.K. Mandal and Paramartha Dutta.” Hash Based Least Significant Bit Technique For Video Steganography(HLSB)”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April (2012):1-11.

[13] Neil F. Johnson and Sushil Jajodia.” Exploring Steganography: Seeing the Unseen”, IEEE Computer, Vol. 31, Issue No. 2, Feb. (1998): 26-34.

[14] Ekta Walia , Payal Jain and Navdeep.” An Analysis of LSB & DCT based Steganography”, Global Journal of Computer Science and Technology, Vol. 10 Issue 1, April (2010):4-8.

[15] Roza Hikmat Hama Aziz."Improving Courier Service Reservation System: Reliability and Performance", Asia Journal of Natural & Applied Sciences, Vol. 4 (4), December (2015): 20-36.

[16] P, Kumar and V, Sharma." Information Security Based on Steganography & Cryptography Techniques: A Review". International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 10, October (2014):247-250.

[17] A, Anagaw and V. Sreenivasarao." A Modified RSA Encryption Technique Based on Multiple public keys". International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June (2013):859-864

[18] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson's Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[19] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In *Healthcare Analytics*, 2023, 4, 100219

[20] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 720–729

[21] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In *Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges*, 2023, pp. 305–321

[22] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In *International Journal of Intelligent Systems and Applications in Engineering*, 2023, 11(6s), pp. 765–774

[23] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In *Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023*, 2023, pp. 1716–1721

[24] R, Poornima and Iswarya R.J. "An Overview of Digital Image Steganography". International Journal of Computer Science & Engineering Survey 4.1 (2013): 23- 31.

[25] Rashid, Aqsa, Malik Missen, and Nadeem Salamat. "Analysis Of Steganography Techniques Using Least Significant Bit In Grayscale Images And Its Extension To Colour Images" Journal of Scientific Research & Reports (JSRR) 9.3 (2016): 1-14.

[26] Nameer N. EL-Emam." Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm". International Journal of Computer, Electrical, Automation, Control and Information Engineering. Vol:2, No:11, (2008):3806- 3817.

[27] S. E. El-Khamy, N. O. Korany and A. G. Mohamed, "A New Fuzzy-DNA Image Encryption and Steganography Technique," in *IEEE Access*, vol. 8, pp. 148935-148951, 2020, doi: 10.1109/ACCESS.2020.3015687.

[28] Ako Muhammad Abdullah, Roza Hikmat Hama Aziz. "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm " *International Journal of Computer Applications (0975 – 8887)* Volume 143 – No.4, June 2016

[29] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods" *ScienceDirect*, September 2009

[30] Aized Amin Soofi, Irfan Riaz, Umair Rasheed. "An Enhanced Vigenere Cipher For Data Security" *International Journal Of Scientific & Technology Research* Volume 5, Issue 03, March 2016