

An Efficient Encryption and Decryption Method for Image Steganography

¹Ranjitha R, ²Mallikarjun Shastry PM

¹PG Student, School of C and IT, Reva University, Bangalore, India

²Professor, School of C and IT, Reva University, Bangalore, India

¹ranjitharanju836@gmail.com, ²mallikarjunshastry@reva.edu.in

Article Info

Volume 83

Page Number: 4232-4238

Publication Issue:

May - June 2020

Article History

Article Received: 19 November 2019

Revised: 27 January 2020

Accepted: 24 February 2020

Publication: 12 May 2020

Abstract

In a digital world, data protection has become highly important issues. For secure data transmission, steganography and cryptography are used where steganography is focusing on the existence of a message secret and cryptography is focusing on content message secret combining both technologies will give more protection for data. In this paper, a base64 encoding method is used to encrypt the secret information which will be embedded into the cover image. An android application is built to perform encoding and decoding operations which is user friendly, fast and secure. Image quality is measured using Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and histogram analysis. The experimental result shows that the stego image can store large amount of data while PSNR, MSR, and histogram analysis values proves that stego image quality is almost similar to cover image and distortionless images.

Keywords: *Steganography, LSB, cryptography, Base64.*

1. Introduction

In the current era of digital world, secure data transmission becomes a more challenging task. Cryptography is a technique to protect the security of the information and this makes use of encryption and decryption processes to keep the message secret which means Secret writing. However unauthorized can access the information by changing the information to be transmitted to overcome this problem steganography is used [1]. Steganography is derived from the Greek word steganos which means "Covered" and graphy means "Writing", i.e. covered writing [12]. The basic idea behind steganography is hiding the secret data in some objects. Steganography uses different types of objects to hide the data like image, audio, and video. The most popular one is image steganography because of their frequency on the internet [2]. Image steganography techniques work on two different domains like space domain also known as pixel domain where steganography operation directly performed on the pixel and transform domain, where message embedding is performed in the transformed image [3]. The object which is used to cover the secret information is called cover image on the based compression of image cover image is divided into lossy and lossless compression. Lossy compression is more popular on the website because of Very small file sizes and lots of tools, plugins, and software support it but once

the image is compressed it can't get back to the original image which results in data loss on each compression image will lose its original picture quality. With 50% compression applied image file size decreased by 90%. With 80% compression applied image file size decreased by 95%. [4] e.g. like JPEG image. In lossless compression, the compressed image will never lose their data and slightly decreased in image file size it maintains the same picture quality of the original image. E.g. BMP, GIF, and PNG. JPEG spatial image data transforms into the frequency domain and subjected to lossy compression, on each compression process image loses its data and introduced too much noise in it. When image is converted back to the spatial domain it will be very hard to detect the error using error correction coding. Hence, it was concluded that steganography would not be possible in JPEG images. [5]. The algorithms which are used to overcome this problem is very complicated. Whereas for a PNG and BMP image a simple LSB is applicable without any loss of data on compression. Also, they both fair almost equal in terms of storing capacity and image quality of the final image. Lossy compressed images are complicated for steganography processes it needs extra compression algorithm to maintain the integrity of the data where lossless image are well suitable for steganography processes. Steganography and cryptography are two different processes where

steganography is focused on keeping the existence of a message secret and cryptography focuses on keeping the content message secret [12]. Combination of both methods gives strong steganography algorithm.

In the rest of this paper is organized as follows: Section 2 gives a brief overview of related work and drawbacks of the existing system. Section 3 gives a detailed description of the proposed system. Section 4 implementation of the proposed system. Section 5 results and discussion. Finally, the conclusion is given in section 6.

2. Related Work

A text steganography method in the JPEG image was studied and proposed a system by Abbas Darbani et al. [3]. Here JPEG images are used for steganography because of the smaller size which is suitable for transmission and Least Significant Bit method is used for steganography. Since part of the data will be lost because of the lossless compression nature of the image proposed system where a message is embedded after the discretization stage and two adjust pixel is used and embedding processes are depended on replacement table which will be a major issue. JPEG images are not well suitable for steganography processes.

A new approach of hiding data in BMP image using Caesar Vigenere Cipher Cryptography an experiment is carried out by I Gede Arya Putra Dewangga et al. [6]. In this study, cryptography is used to hide the secret message which is inspired by the Vigenere cipher technique and then the message is inserted into the LSBs to hide one byte of a secret message it uses the eight-byte of the cover image without compromising the file quality. PSNR and MSR values are calculated to measure in cover and stego image qualities.

A survey on LSB steganography between the BMP and JPEG is done by Eltyeb E. Abed Elgaba [7].

A Comparison study is done on lossless compressed images (e.g. BMP, PNG, and GIF) and lossy compressed images (e.g. JPEG) for LSB steganography. Strengths and weaknesses have been observed. BMP image can hide a large amount of data and image distortion will not occur and JPEG image uses less space but robustness against image manipulation and resistance to statistical attacks is low and increases the amount of data distortion also increases.

Compared to two digital image file formats using different compression techniques is done by Bharat Sinha [8]. Images are two types of file format one is lossless compression technique data will not lose after transmission and lossy compressed technique data will lose after transmission comparison study is done between the PNG and JPEG where PNG image will more suitable for LSB steganography both BMP and PNG images have similar characteristics.

A survey is done on a stenographic tool for the BMP image format by Prof. SumedhaSirsikar et al. [9]. Various tools performances are evaluated by PSNR for stego and cover images values are very less and tools are provided by GUI and command line which is very complicated to use.

Image steganography based on the RSA algorithm is implemented by Rituparna Halder et al. [10]. Steganography is combined with RSA cryptography algorithm to provide more security to data along with encryption and decryption add authentication module for extra security from all above prevision studies in this study would be used steganography with more efficient and easy cryptography method i.e. Base64 and LSB steganography used for PNG image format which is distortionless, maintain data integrity and store more data. An android application is built which user friendly and also used for private communication.

- JPEG images are not well suitable for LSB steganography because data loss occurs.
- The compression algorithm which is used to maintain data integrity is complicated to implement.
- Steganography alone has less security.

3. Proposed Encryption and Decryption

The purpose of the proposed system is to provide an efficient and easy way to transfer secret data over the communication channel by using the combination of steganography and cryptography methods where the encryption method gives extra security level to get the original data.

The proposed system has the following objective.

- Stego image is PNG image format which maintains data integrity.
- More security on data.
- Provides user-friendly application.
- Maintains good image quality.

A. Overall Design Ideas.

As shown in fig.1 is the overall design idea of the proposed system where steganography is combined with cryptography to add more security for the system. Steganography using Least Significant Bit (LSB) method to hide secret data in the image cryptography using the Base64 encryption method to encrypt the secret data.

The proposed system has two phases encryption phase and decryption phase. In the encryption phase, secret data will hide in the image before embedding data in.

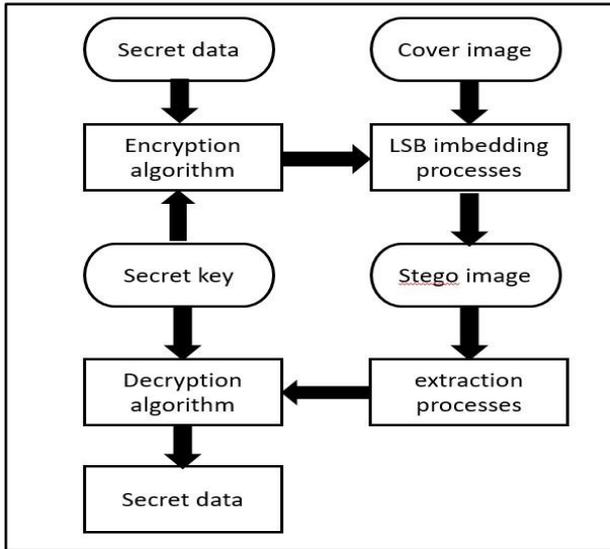


Figure 1: Architecture of steganography processes.

Image data will get encrypted into cipher text. In the decrypted phase, first data is extracted from the image then ciphertext is converted into plain text. An image that is used to hide the data is called a cover object. An image which embedded with data is called stego object.

B. Encryption and Embedding method.

As shown in fig.2, it is an encryption and embedding phase in this phase secret data which is in the form of plain text get encrypted by the Base64 method first, secret information is converted into ASCII code then ASCII code is again converted into binary data and binary data converted into ciphertext. Now ciphertext is embedded into the cover object. Cover object can be any type of image (e.g. JPEG, PNG, BMP) using LSB steganography processes to form a stego object where stego image is.png image format so when attackers are trying to compress the stego object image will not get compressed and it maintains the data integrity.

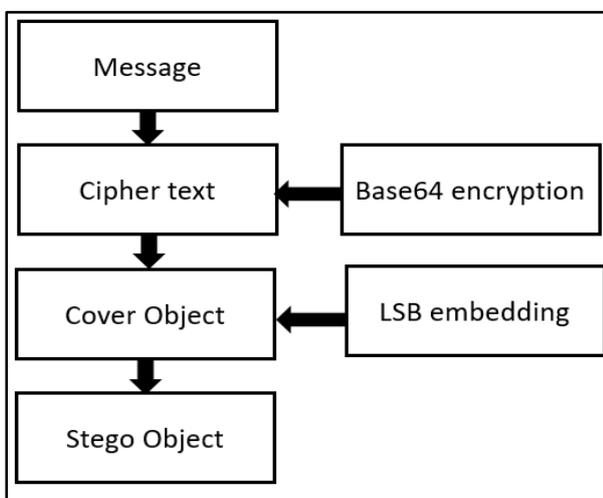


Figure 2: Encryption and Embedding phase.

C. Extraction and Decryption method

Fig.3 shows an extraction and decryption phase in this phase, the first information is extracted from the stego image extracted information is decrypted to get back the original image.

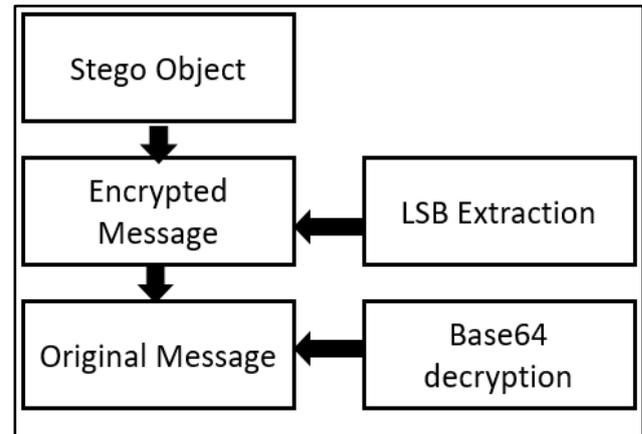


Figure 3: Extraction and Decryption phase.

4. Implementation of Proposed Method

Image compression is a technique that is widely used in steganography. It is mainly classified into two types lossless compression and lossy compression wherein lossy compressed image (e.g., JPEG image format) will not retain its original data when it undergoes some transmission. When attackers try to extract the information from the image it loses some important data whereas in lossless compression image it preserves its original data correctly hence lossless compression is chosen for LSB steganography (e.g., BMP, PNG, and GIF image format).

In the proposed method steganography is combined with cryptography to provide more security for secret information. This technique makes sure that a secret message is encrypted before hiding in the cover image so when hackers got the data from the cover image still they can't access the encrypted data this provides the extra layer of security and this is done by using an efficient encryption and decryption algorithm. The proposed system uses two main technologies for secure data transmission are steganography which embeds the sensitive data in an image by using most popular technique called Least Significate Bit(LSB) and cryptography which changes the meaning of message called cipher and method which is used to encrypt the data is the proposed system is a base64.

To transmit the secret data from the sender to receivers in such a way that intruder does not suspect the existence of the information an effective system is designed. System design is divided into two parts namely Embedding function and Extraction processes. In embedding function secret message encryption using base64 and then hides the encrypted data in the cover

image using the LSB technique is taking place. It makes sure that encrypted data is embedded in the cover image to form a stego object. In the second part of the system, Extraction is taking place where ciphertext is extracted from the stego object using the LSB technique and ciphertext is decrypted to get back the secret data in the reverse order of base64 method.

A. Least Significant Bit (LSB):

Steganography is a process of hiding the secret message with a cover image the method which is used for embedding the information within a cover image is the least significant bit (LSB) which is simple and popularly used approaches. In this method, the least significant bits of some or all of the bytes inside an image is replaced with a bit of the secret message. Every digital image is a finite set of pixels each pixel is the colour combination of RGB modal i.e. 24bit image file one can store 3 bits in each pixel by replacing it by secret message bits. Suppose for example if we want to hide a message “A” in a cover image convert message “A” to ASCII code i.e.1000001 here we are using 3 pixels that are about 9 bytes for insertion to replace all the least significant bits. Now replace the last bits of the pixel with ASCII code of “A” bits as shown below [14]. Fig.4 shows the status before insertion of pixel and Fig.5 shows the status after the insertion of pixel.

10000000	10100100	10110101
10110101	11110011	10110111
11100111	10110011	00110011

Figure 4: before insertion of pixel

10000001	10100100	10110100
10110100	11110010	10110110
11100110	11000011	00110011

Figure 5: After insertion of the pixel

As discussed in the related work section loss less compression image like.PNG image format is the best image steganography because when an image tried to compressed image will not lose its data.

B. Base64 Encoding method.

Base64 is one of the most popularly used encoding algorithm to transmit over the internet of 8-bit bytes code which belongs to binary-to-text encoding schemes. Text is converted into ASCII code of string format and translated into radix-64 represented. Its advantages are that the efficiency of the algorithm is high, the coded results are short, also unreadable[20].

C. Algorithm of the proposed system:

Algorithm to hide data into image:

Algorithm Hiding:

```

Input: CoverImage, SecreteMessage, SecreteKey
Output: StegoImage
Read the CoverImage, SecreteMessage, and SecreteKey
Ciphertext = Compress (SecreteKey, SecreteMessage)
    FindLSBs (CoverImage)
    While (CoverImage):
StegoImage = Embbed (Ciphertext into CoverImage)
Return StegoImage
    
```

Algorithm to Unhide data from image:

Algorithm Unhiding:

```

Input: StegoImage, SecreteKey
Output: CoverImage, SecreteMessage
Read the StegoImage, and SecreteKey
If (SecreteKey == StegoImage(SecreteKey))
    FindLSBs (StegoImage)
    While (StegoImage):
CoverImage, SecreteMessage = Uncompressing (StegoImage)
Return CoverImage, SecreteMessage
    
```

5. Result and Discussion

An android application is designed to perform image steganography processes. Select the cover image of any format, enter the secret data next give a secret key for authentication purposes. First secret data will be converted into ciphertext using the Base64 encoding method then encoded text embedded into the cover image. Encoded images will get saved in the device in.png format to overcome the problem of data loss. Now in the decode phase select the image and enter the same secret key to access the secret data if the secret key is the wrong application gives a message wrong key if key is correct secret data will be displayed.

The result of the proposing system is evaluated using three parameters Peak Signal to Noise Ratio, Mean Square Error (MSE) and Histogram.

Compression table of PNG (portable network graphics)and JPEG (joint photographic expert group) images are done in the table 1.

Table 1. Property Comparison of PNG and JPEG.

Property	LSB in PNG	LSB in JPEG
Visibility	Low	Low

Independent of File Format	Low	Low
Robustness Against Statistical Attack	Low	Medium
Stego analysis Detection	Low	Medium
Payload Capacity	High	Medium
Data Capacity	High	Low
Efficient When Amount of Data Reasonable	High	Medium
Robustness Against Image Manipulation	Low	Medium
Percentage Distortion Less Resultant Image	High	Medium

Comparison of LSB for lossless and lossy images is one in the above table which tells that PNG image format is well suitable for LSB steganography processes where it stores large amounts of data with high payload capacity, less distortion in the resulted image and low stego analysis detection when compared to JPEG image. Due to the loose less compassion nature of the JPEG image, it does not maintain data integrity. When it undergoes some compression data loss occurs to overcome this problem entropy encoding is used to produce stego image which is a very complicated compression method to maintain the data integrity. Table 2 shows the comparison of the results obtained by the proposed method with PSNR and MSE [6]

Table 2: Comparison of Results

Sr. No	Cover Image(.Jpeg)	Proposed system		Existing system	
		PSNR	MSE	PSNR	MSE
1	 nature	75.56	0.0018	59.85	0.0677
2	 animal	73.54	0.0028	60.25	0.0617
3	 flower	79.85	0.00067	60.63	0.0567
4	 smiley	91.62	4.47	63.34	0.0303
5	 peacock	86.2	0.0015	62.21	0.0394

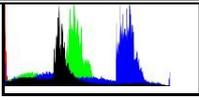
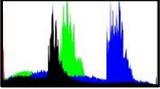
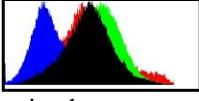
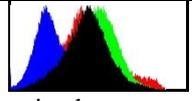
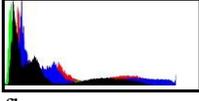
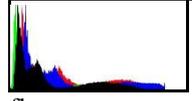
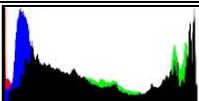
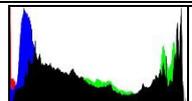
The image quality of an image is measured using peak signal to noise ratio (PSNR) and mean square error (MSR)[15] for stego image and cover image and also histogram is used to measure the distortion of stego image and cover image using the following equations.

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right)$$

$$MSR = \frac{1}{mn} \sum_0^{m-1} \sum_0^{n-1} ||f(i, j) - g(i, j)||^2$$

Mean square value is calculated for the original image and compressed image lesser the value less error in the image, which is an inverse relation between MSE and PSNR which means a higher value of PSNR is good because it means that the ratio of signal to noise is higher[16]. MSR and PSNR values of the stego image and cover image of an image and intensity of the images is shown in Table 3.

Table 3: Histograms of encoded and decode images

Sl. No	Cover image	Stego image
1	 nature	 nature
2	 animal	 animal
3	 flower	 flower
4	 smiley	 smiley
5	 peacock	 peacock

Five image samples of different size are taken for experiments and image quality measurement is done on those images PSNR and MSR is calculated and we got a result with higher PSNR value and low MSE value which proves that there is no much difference between the cover image and stego image and image is maintaining the actual quality. Histogram is used to measure the distortions less of the cover image and stego image [14].

PSNR and MSR values are compared to the existing system and the proposed system fig.6 shows that the proposed system has the highest PSNR value than the

existing system and fig. 7 shows that the proposed system has less error value than the existing system.

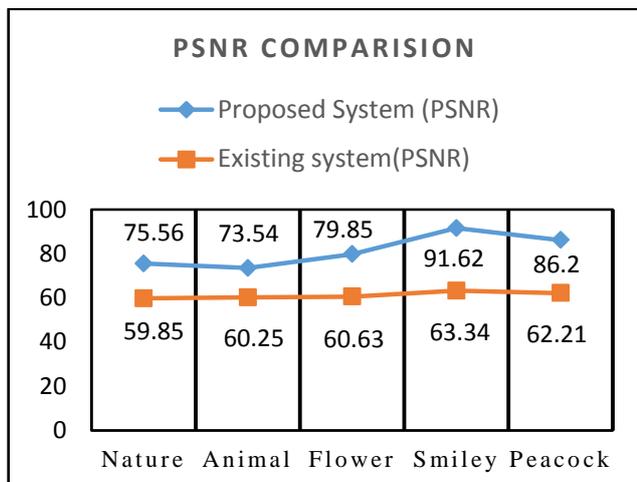


Figure 6: PSNR comparison.

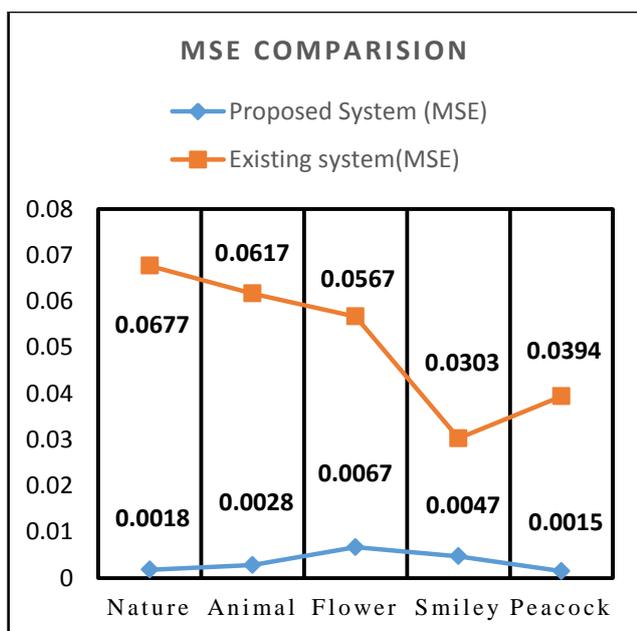


Figure 7: MSE comparison.

6. Conclusion

In this study, steganography is combined with the Base64 encoding and decoding method for data security purposes. An android application is built which is a fast, secure and user-friendly interface to encode and decode images. To evaluate the performances of the proposed system PSNR and MSR, parameters are calculated. The result shows that the proposed system can store more amount of secret data while a stego image is most similar to the cover image. Histogram graphs show that distortions less between the cover image and stego image. Comparison graphs are drawn to show a proposed system PSNR and MSE values are improved by 33% and 43%

respectively than the existing system. This proposed system is implemented to increase the security of the data when transmitted through a highly vulnerable and insecure network.

Acknowledgment

This is a matter of pleasure for me to acknowledge my gratitude to the School of Computing and Information Technology, Reva University for allowing me to explore my abilities via this paperwork. I would like to express my sincere gratitude to our project guide, Dr.MallikarjunShastry PM, for his valuable guidance and advice in completing this paperwork. Let me take this opportunity to thank the School Director, Dr.SunilKumar S. Manvi for the wholehearted support extended to me throughout the conduct of the study. Last but not the least, I would like to express my sincere thanks to my family members, friends for their immense support and best wishes throughout the curriculum duration and the preparation of this paper.

References

- [1] I GedeWiryawan, Sirias, and I GedeArisGunadi, "Steganography Based on Least Significant Bit Method was designed for Digital Image with Lossless Compression Technique", in International Conference on Signals and Systems (ICSigSys),2018.
- [2] Sheelul and Babita Ahuja, "An Overview of Steganography", in IOSR Journal of Computer Engineering, Volume 11, Issue 1 (May. - Jun. 2013), PP 15-19.
- [3] Abbas Darbani, Mohammad M. AlyanNezhadi and Majid Forghani, "A New Steganography Method for Embedding Message in JPEG Images ", in 5th International Conference on Knowledge-Based Engineering and Innovation (KBEI) 2019.
- [4] <https://www.keycdn.com/support/lossy-vs-lossless> Accessed on March 2020.
- [5] Neil R. Bennett, "JPEG Steganalysis & TCP/IP Steganography" in a thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in computer science & statistics 2009.
- [6] I Gede Arya Putra Dewangga, Tito WaluyoPurboyo, and RatnaAstutiNugrahaeni, "New Approach of Data Hiding in BMP Image Using LSB
- [7] Steganography and Caesar Vigenere Cipher Cryptography", in International Journal of Applied Engineering and Research,ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10626-10636".
- [8] Eltyeb E. Abed Elgabar, "Comparison of LSB Steganography in BMP and JPEG Images", in International Journal of Soft Computing and

- Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013.
- [9] B. Sinha, "Comparison of PNG and JPEG format for LSB Steganography," International Journal of Science and Research, vol. 4, no. 4, pp. 198-201, 2015.
- [10] Prof.SumedhaSirsikar and Prof.Asavari Deshpande," Steganographic Tools for BMP Image Format", in International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) Volume 2, Issue 1, February 2011.
- [11] Rituparna Halder, Susmit Sengupta, Sudipta Ghosh, DebashishKundu. "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 39-43.
- [12] T. Morkel, J.H.P. Eloff and M.S. Olivier, "An Overview of Image Steganography" in Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa, 2005.
- [13] K. F. Rafat and M. J. Hussain, "Secure Steganography for Digital Images," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, pp. 45-59, 2016.
- [14] V. Lokeswara Reddy, Dr. A. Subramanyam, andDr.P. Chenna Reddy," Implementation of LSB Steganography and its Evaluation for Various File Formats", in Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011).
- [15] Avcibas and B. Sankur, "Statistical analysis of image quality measures," Journal of Electronic Imaging, vol. 11, no. 2, pp. 206-224, 2002.
- [16] Nisha and Dr. Rajeev Yadav, "Image Description Notes with LSB Encoding in Steganography Technique", in IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 03, 2017 | ISSN (online): 2321-0613.
- [17] LEAST SIGNIFICANT BIT STEGANOGRAPHY TECHNIQUE FOR HIDING COMPRESSED ENCRYPTED DATA USING VARIOUS FILE FORMATS, student paper.
- [18] Dr.Asoke Nate, Sayudh Roy, ChahatGopalika and Dubaians Mitra, "Image Steganography using Encrypted Message", in International Journal of Advanced Research in Computer Science and Management Studies Volume 5, Issue 4, April 2017.
- [19] Yuhua Qin, "the Realization of Information Hiding in BMP Images" in 2009 Second International Workshop on Computer Science and Engineering.
- [20] Abdelkader Moumen and HocineSissaoui," Images Encryption Method using Steganographic LSB Method, AES, and RSA algorithm", Nonlinear Engineering 2017; 6(1): 53–59.
- [21] Somchai and Wen Dong," Research on Base64 Encoding Algorithm and PHP Implementation", in 26th International conferences on geoinformatics 2018.