International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 02 | Feb - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

An Efficient System for Secret Information Sharing Through Machine Learning Based Key Generation and Steganography

Tattukolla Rajesh

Abstract:
Currently several cryptography methods are currently being developed, including chaos encryption, advanced encryption standard, two-fish, and others. Two major issues plague these cryptography algorithms: computational capabilities and sluggish learning. In order to address these concerns, this research article proposes a new cryptographic scheme. Steganography is a popular and dynamic technique for hiding important information or data within an image, video, or audio so that it cannot be accessed by unauthorized people. In this technique, it is planned to include number of methodologies to propose a new technique for gray and color images to produce better results with respect to efficiency and payload capacity. In this proposed technique first we have to obtain codeword with sensitive secret data with the help of its checksum, then the produced codeword is compressed with the suitable compression algorithm before encrypting, then it is added to the header and then inserted into the original image. To embed each byte of data combination of different LSB and MSB of the selected pixels is identified. The use of the Artificial Neural Network (ANN) algorithm in a cryptosystem has been found to improve cryptographic performance in terms of security and attack resistance. For one hidden layer NN, we describe a sub-key generation technique based on an Extreme Learning Machine (ELM) for producing a good cryptosystem. To initialize the input-hidden layer weights and data in each cycle, the initial key was built using the ANN topology, activation function, and seeds for the Pseudo Random Number Generator (PRNG).The output layer weights are used to construct the sub-key in each round. The proposed method is evaluated and compared to existing algorithms on a variety of images of varying sizes. The proposed algorithm produces better PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Average difference(AD), Maximum difference(MD), Normalized absolute error(NAE), Cross – correlation(CC) values, as well as better PSNR and MSE values, than the sequential algorithms for different embedding rates of 10%, 30%, and 50%.

Keywords: Cryptography, Image Steganography, Encryption, Compression, Artificial Neural Network, Extreme Learning Machine

I.Introduction:

It is no longer advisable to save secret sensitive material on a personal PC or on a company's central server. Nowadays, everyone saves their personal information in the cloud. The term "cloud computing" is well-known and widely used. It provides a diverse set of services to a variety of sectors. Because data comes from a variety of sources and from different people or clients, providing security for client data is a prevalent and focused term in this setting. Many unique data protection solutions have been presented, with cloud providers providing some of the core security algorithms initially. Steganography is also a significant method of protecting sensitive or secret information from prying eyes.Data security is one of the most critical parts of any sector, and secure communication with other parties is one of the most crucial aspects of data transmission as well. Steganography is a well-known technique for protecting confidential information from unauthorised parties or third-party vendors.This is available in different formats like image steganography, video steganography and audio steganography also it is applicable in different domains like spatial domain, frequency domain and temporal domain.To safeguard the secret data in an original carrier image or in a carrier file, two separate domains are present. The spatial domain is used by the majority of existing algorithms. The data was static in the spatial domain environment, and it is still static in nature. The data in a frequency domain environment is dynamic in nature. This research is focused on the spatial domain, specifically the LSB and MSB bits of the carrier picture, as well as the secret data. Capacity, robustness, PSNR, and MSE are some of the goals of image steganography. The capacity is determined by the size of the secret data that will be contained in the carrier image. The various types of steganography techniques available in the spatial and frequency domains are depicted in Figure 1.

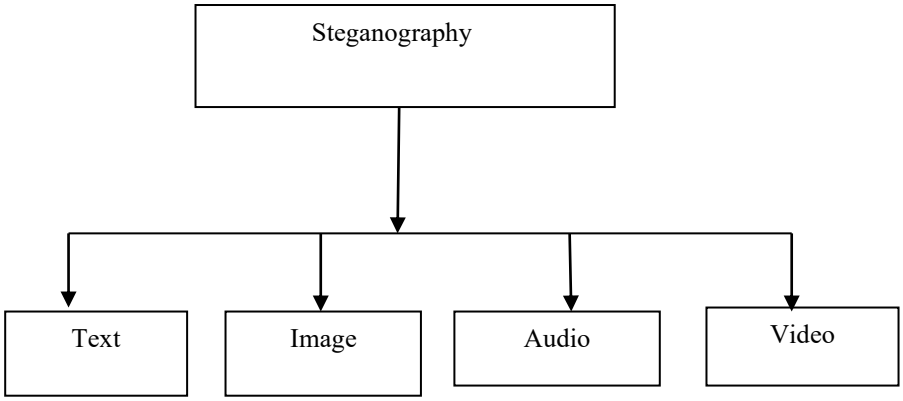


Figure 1: Types of steganography techniques

The remainder of the paper is structured as follows. The second section contains a review of the literature on the spatial domain. Basic principles relevant to the suggested methods are presented in section 3. Algorithms relating to the proposed method are presented in section 4. Section 5 compares the performance of the proposed algorithm to that of various existing algorithms. The chapter concludes with a discussion of the conclusion.

II.Literature Review:

In this presented brief information about various existing techniques in image steganography domain belongs to spatial domain environment [22]. Therefore the proposed technique is related to spatial domain and using LSB, MSB bits for embedding sensitive secret data.

In chanhey ci-ki and chengalu c-ms[1] the sensitive original data is inserted in LSB pixel of the cover image directly. In this technique first identify the LSB of the original carrier image. In those selected pixel directly inert secure data[13][14]. This algorithm produced a better PSNR and MSE values with respect to capacity and efficiency of the image.

One of the image steganography techniquesoffers [16][17]three bit replacement technique. Among those three bits we select a better pixel one is called as a optimal pixel.Based on the optimal pixel we select neighboring pixel and that one is used for hiding secret data.

In Akhtarfd Ng 2016 [5][18] proposed a variation in LSB substitution technique. It uses inverting concept. In those methods the hiding of secret data is embedded in the PSNR and MSE values. Especially in this inversion technique some of the LSB's pixels of the source image are modified with the obtained pattern of the image[19].

Another technique to hide the secret data in pixel based dereferencing method. In this the original method [6][20] was partitioned into block of non overlapping. The difference was calculated from two consecutive pixels of an image. For payload selection the calculated pixels are used.

The randomization is one of the improved techniques in steganography. It works on the basis of reaction of human eyes.In kukapalli[2] have proposed an enhancement in image steganography method. This technique is called pixel Indicator method. In this technique three MSB bits three LSB bits are considered and also use Blowfish algorithm for encrypting the data.

Dighle[3] proposed another improvement in data hiding in an image. In this the secret data embedded by using data parity. In Bash etal presented an improved version in inserting a data in an image under spatial domain environment. This method using four algorithm, Blowish algorithm for encryption and LZW compression. This algorithm produces a better payload capacity and improvement in the quality of the stego image.

In Dadgostar[4]using edge detection algorithm is interval valued edge detection algorithm to insert the sensitive information or data in edge pixels of the original image. This algorithm produces better quality of the stego image.

Some steganography algorithms embed data in the original image's Fibonacci pixels, improving PSNR and MSE values[7][8]. In his research, Dr.Kiran Kumar used steganography and secret key embedding techniques to provide a novel methodology for injecting data into the carrier picture[9][10].

Rajarathnam [11][12] introduced a new approach based on LSB image segmentation techniques, as well as DES and Triple DES for encrypting raw data into cipher text in Chandramouli. Horspool [15] proposed a better outcome employing hide and seek technology for embedding data into an image using image steganogrphyapproach..

Kiran[23] introduced a new image segmentation algorithm for embedding secret data into a picture in his paper. Before embedding the data, the image is separated into 9 equal portions and masking is used. The original image is translated into the differential image after the masking process. After dividing the original image into 9 equal halves, use the clever edge detection technique to find the Fibonacci edge pixels and insert them.
Suneetha[24] suggested a unique approach for inserting data into a picture in a spatial domain context. A new neural network technique based on the cascade feed forward network has been introduced in this algorithm. In terms of PSNR and Mean Square Error value, it improves performance.
Nasir Memon inserted hidden data into an image using an LSB-based image stegonagraphytechnique[25]. Patil, Priyadarshini, and colleagues[26] introduced a new approach to secure hidden sensitive data in an image by combining it with three existing algorithms: DES, AES, and triple DES. With different current methods, Mohammad Shkoukani [27] produced improved PSNR and MSE values utilising a new technique in combination with genetic and blowfish algorithms.

III.Proposed method design:
This method consists of two different phases

1. Embedding phase
2. Extraction phase

On the server, the embedding is done. The new technique compresses and encodes the original data, and the resulting image is then inserted in the original cover image. On the receiving end, there is an extraction step. It's used to get the original secret info from a stego image. This section includes all of the components, vocabulary, and concepts needed to develop our suggested technique.

Integrity of data:
Image Steganography have different objectives one of the main objective of steganography is the robustness or strangeness of the algorithm. When an authorized person wants to manipulate the original image there was a loss of secret data. In this proposed algorithm payload is embedded with the receiver side to identify the data manipulation or to provide the concept of data integrity.

To implement data integrity in this proposed algorithm uses a famous well know technique Cyclic Redundancy check algorithm is used. The CRC technique is a very fast light weight algorithm and can provide a better assurance for integrity of the data. In this process the sender calculate checksum with 32 bit size for original secret data and append this checksum to the original codeword. In general the checksum length is equal to the codeword length 32 bits at the receiver side after receiving the codeword the last four bytes are separated after that the new checksum is calculated for the remaining bits. Finally compare those two modifications was done original image was rejected by the receiver.
Compression:
The aim of image steganography is to enhance the capacity of payload and also reduce the probability for chances of identifying the original message from an image.The data is hidden within the image, which is then compressed before

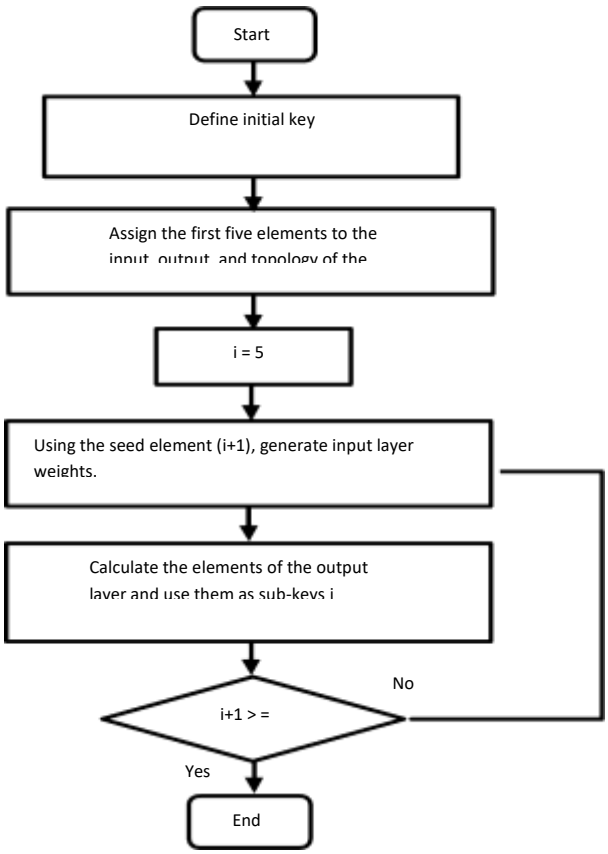
being stored in the required environment or transferred to the receiver side. In this the sender compresses the sender side codeword and decrypt at the receiver side.

Data Encryption:

The proposed method consists oftwo level securities. In first level to protect the original secret message from unauthorized persons first we encrypt the original message using key generation algorithm .This algorithm works with either 128/256 length.The proposed ANN-based ELM algorithm consists of a single hidden layer with 100 neurons that generates a key with 10 sub-keys. The user must first specify an initial key K = (k,, k, k,,., @), where n (15) is the number of key elements. The first five elements are used to determine the ELM, which includes the number of inputs, outputs, activation function type, number of hidden layer neurons, and data size. K k,, k,, k,, k, k (3, 1, 1, 100, 100) denotes an ELM with three inputs, one output, the first type of activation function (four types are considered: Sin, Radial Basis Function, Sigmoid, and Hardlim), 100 neurons in the hidden layer, and 100 data.The initial stage in ELM training is to set up weights and biases in the input-hidden layer. In addition, the remaining ten key elements, namely K, ,, (8, 1, 7, 8, 5, 3, 2, 8, 2, 1), are utilized as ten seeds for the sub-keys' internal ten rounds. The number 10 was chosen because the sophisticated encryption standard AES has a certain number of rounds. By producing different weights and biases, each member of the seeds set is used to construct one sub-key. In each round of a single iteration of ELM, this is generated at random. Each sub-key is created independently and without regard to the other sub-keys.All rounds are run in parallel, and the ten sub-keys are created at the same time based on the ANN's and the proposed algorithm's independent attributes. It's worth noting that this method of creating Calculate the elements of the output layer and use them as sub-keys is unaffected by attacks,
even when using seedsare recognized by an attacker.This is due to the fact that determining the topology of the ANN and the ELM need additional information. Users can alsochange the content of the key and, as a result, the entire machine learning-based key generation approach by knowing this information.Figure 2 shows various Flow chart for generating the sub key using the proposed system.

Figure 2 :Flow chart for generating the sub key using the proposed system.

Header:



In this proposed method the new header information system is introduced. This header is used to guarantee that the secret is properly included.The sender is responsible for generating 4-bit header information. In this the first 2 bits are

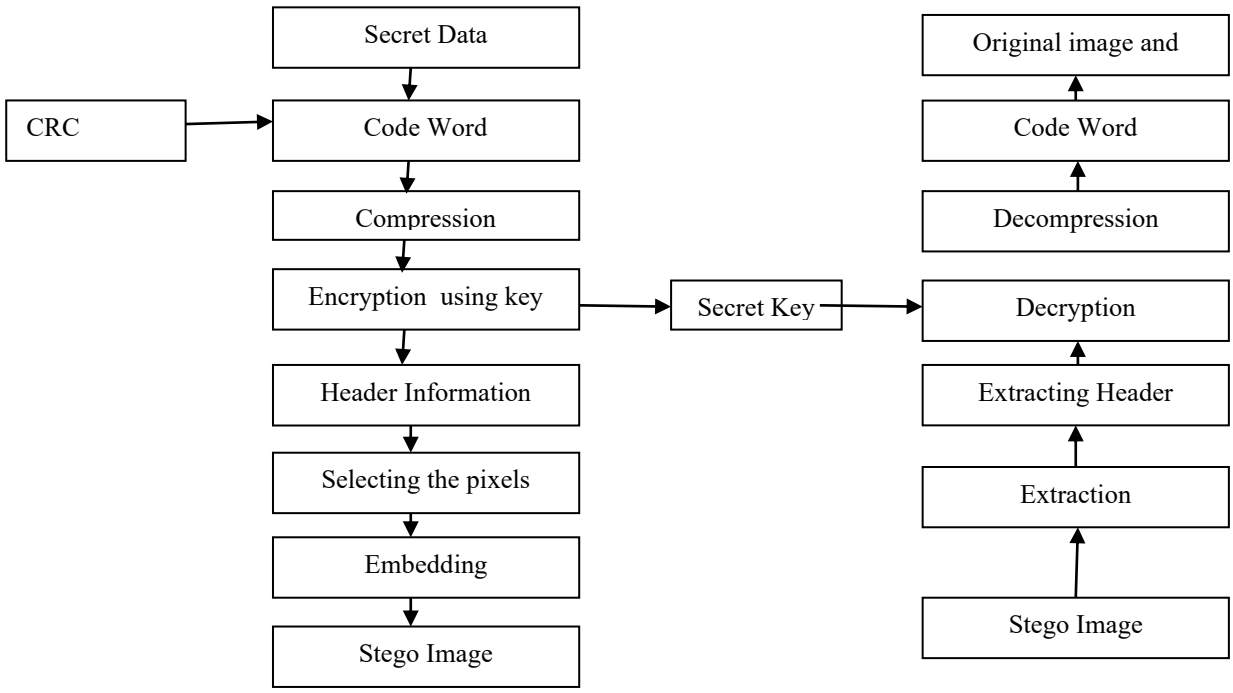
used to identify the type of data and the remaining two bits are used to identify the length of the data. The Header format is shown in Figure 3

2 bits	2 bits
Type of Data	Data Length

Figure 3: Header Format

Pixel Selection:

One of the important or major aspects of embedding is the pixel selection or selecting pixels. In this proposed method a new algorithm with pseudo random approach is implementing to insert the sensitive secret data.For each image with various dimensions, the suggested technique identifies the dimensions of the cover image. Multiple dimensions have multiple pixel values. Among those multiple pixel values select random pixel values using proposed algorithm for hiding secret data.



Proposed Model: The Proposed Model shown in Figure 4

IV.Proposed Algorithm:

In this section presented proposed algorithm for embedding secret massage and extraction of secret message.

Embedding secret massage phase:

Process:

1 a) Convert the sensitive secret data into a byte array of 0s and 1s.
b) Calculate the checksum for secret data in byte array format.
c) To make the codeword, combine two bytes of the determined checksum with the sensitive secret data byte array.
2 Perform the compression operation with obtained or calculated codeword.

3 a) obtain randomly the symmetric key of 128-bit length using key generation algorithm.

b) Encrypt the compressed codeword by using key generation algorithm and obtain the cipher data.

4 a) Compute the header by using 4 bytes It consists of 2 bits of type of length and 2 bytes of codeword

b) Protect the 4-byte header using key generation 128-bit symmetric key.

5 a) The dimensions for the Original Image are calculated using the Width (w) and Height (h) of the original image.i.e w * h

b) Calculate or random secret key of 32-bit length using encryption algorithm.

6 a) for t= 0 to 4

Assume the following parameters

m=0

b) n=array [k]

c) Program mapping process j pixel coordinates by computing X and Y.

d) In the original cover image, find pixel n and access it

e) Embedded the encryption header information into the selected pixel of j.

f) Let n=n+1 and k=k+1

g) end for

7 for i=0 to l

a) Assume e= length of original secret data in the form of cipher text.

b) m=0;

c) k=array [t]

d) Perform mapping process j pixels coordinates by computing X and Y.

e) Access the selected pixel j in the original cover image.

f) Embedded the cipher data into selected pixel of i.

g) Let m=m+1 and k=k+1.

h) end for

8 obtain the stego image.

Extraction phase:

Input: OutputtedStego image.

Output: The original sensitive secret data and the original cover image.

Process**:**The reverse process of the embedding phase shown in Figure 3.

V.Experimental Results and Discussions:

Performance Metrics:

The proposed method is compared with the various existing algorithms of image steganography under spatial domain environment.

Image quality metrics:

These quality matrices are used to determine the stego image's quality in comparison to the original cover image. We calculated PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Average difference (AD), Maximum difference (MD), Normalized absolute error (NAE), and Cross – correlation using the proposed approach (CC).The regular measurement of outcomes and results that creates trustworthy information regarding the success of the proposed system is defined as a performance measure. Furthermore, performance measurement is the process of reporting, collecting, and analyzing data on a group's or individual's performance. Equations (1), and (2), respectively, provide the mathematical equations of an entropy value, PSNR, MSE,

Where, $p(m_i)$ is denoted as the probability of symbol occurrence m_i and m is represented as the total number of symbols $m_i \epsilon m$

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE}) \qquad (1)$$

$$MSE = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(x,y) - k(x,y)]^2 \qquad (2)$$

Where m and n represent the picture's width and height, $k(x,y)$ is represents the decrypted image, and $I(x,y)$ is denoted as the input image.

All of the images are from the http://sipi.usc.edu/database/ data set. For the purpose of explaining the suggested method and the process described in Figures 5 to 8, we used various color images of varying sizes with various lengths of secret data. Table 1 displays the varying image quality of the proposed technique with various embedding rates of various image sizes. Table 2 compares the PSNR and MSE values of the proposed and sequential LSB methods.

Quantitative analysis on the color images:

This section demonstrates the experimental examination of a colour image. The colour images (pepper) used in the image embedding and extraction method is shown in Figure 5. Figure 5(a) depicts the cover picture (pepper), Figure 5(b) depicts the inserted cover picture and encrypted secret image . Figures 5(c) show the final decrypted secret images .

(a) (b) **(c)**

Figure 5. a) Color cover image 1024×1024, b) stego image c) decrypted secret image

Quantitative analysis on the grayscale images

This section demonstrates the experimental examination of a gray scale image. The gray scale image used in the image embedding and extraction method is shown in Figure 6. Figure 6(a) depicts the cover picture,Figure 6(b) depicts the inserted cover picture and encrypted secret image . Figures 6(c) show the final decrypted secret images.

(a)

(b)
(c)

Figure 6. a) gray scale cover image 1024 × 1024, b) stego image c) decrypted secret image

Table 1: Results of the Proposed Method

Embedding Rate	Original Image	Text Message Length(bits)	PSNR	MSE	AD	MD	NAE	CC
	Baoo.bmp	21524	60.45	0.0031	-0.0014	6	0.0001	1
	Leena.png	21524	66.32	0.0061	-0.0013	6	0.0002	1
	Elaanie.tiff	21524	61.55	0.0045	-0.0018	6	0.0002	1
10%	Minii.jpg	21524	68.09	0.0023	-0.0012	6	0.0001	1
	Babo.bmp	78353	57.39	0.0024	-0.0013	6	0.0001	1
	Leena.png	78353	58.47	0.0065	-0.0011	6	0.0002	1
	Elanaie.tiff	78353	51.36	0.0034	-0.0015	6	0.0003	1
30%	Minii.jpg	78353	54.85	0.0023	-0.0016	6	0.0002	1
	Baoo.bmp	132273	53.21	0.0067	-0.0013	6	0.0002	1
	Leena.png	132273	51.23	0.0043	-0.0012	6	0.0001	1
	Elaanie.tiff	132273	56.88	0.0022	-0.0012	6	0.0002	1
50%	Minii.jpg	132273	54.98	0.0056	-0.0013	6	0.0003	1

Table 2: Comparison results of existing and proposed algorithms

Payload Size(Kbytes)	Sequential LSB Method PSNR	Propose Method PSNR	Sequential LSB Method MSE	Propose Method MSE
1	62.34	63.86	0.022	0.023
2	62.45	61.76	0.0064	0.053
4	52.34	54.56	0.0056	0.1234
8	52.67	54.32	0.2456	0.2154
16	49.87	51.45	0.456	0.345
32	46.78	49.87	0.8	0.7568
64	45.34	44.67	1.456	1.234
128	43.45	42.34	3.46	2.893

256	36.45	40.67	5.67	5.456

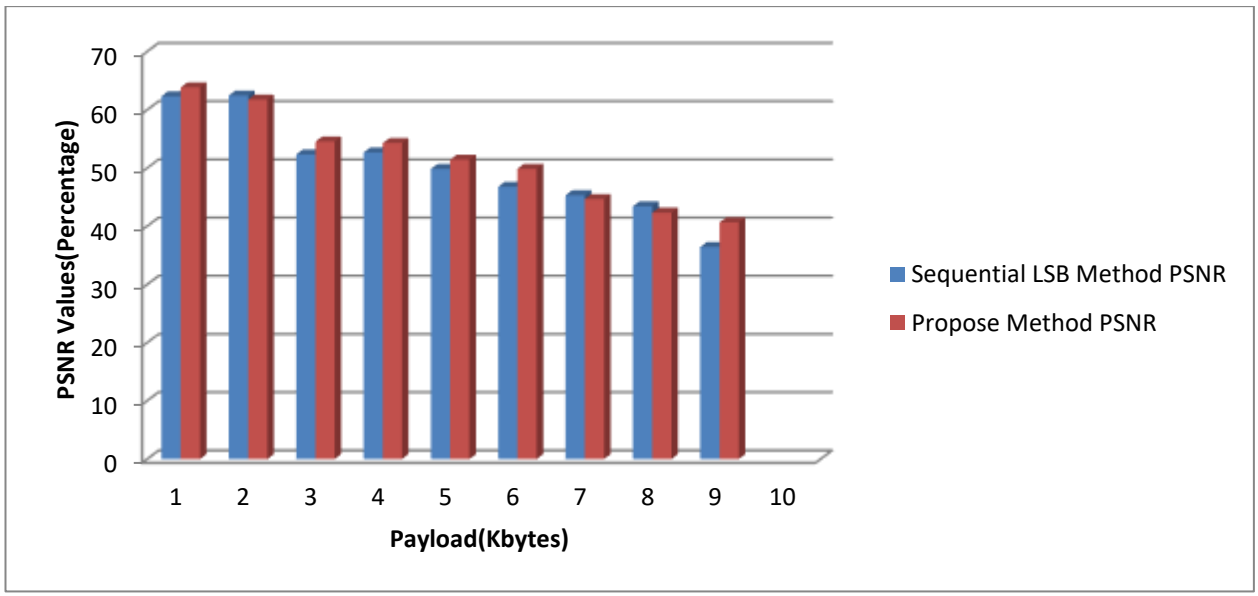


Figure 7: Comparison of Proposed Method PSNR value with Sequential LSB Technique

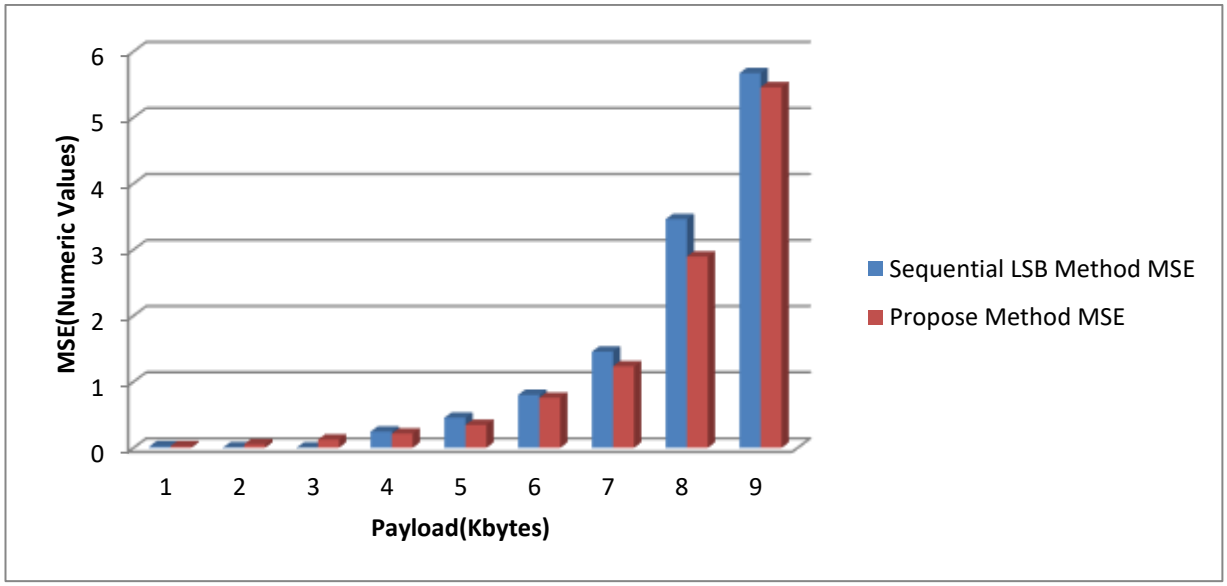


Figure 8: Comparison of Proposed Method MSE value with Sequential LSB Technique

VI. Conclusion and Future Scope:

We proposed of series of improvements and enhancements to the existing sequential LSB image steganography techniques. There are two levels of security in the proposed method. The first level encrypts the original secret message and generates a cypher key using a key generation technique. In the second level, the cypher key is embedded in the image based on the original image's selected pixel. This method proposes a number of enhancements to image quality measurements such as checksum, compression, header information, and random pixel selection. The proposed method was compared to several known sequential LSB steganography techniques and outperformed them. We may conclude that the proposed approach achieves many necessary objectives of picture steganography and also gives better results when compared to various current algorithms by comparing it to various existing algorithms.With

an improvement in PSNR and a drop in MSE, our proposed algorithm offers improved outcomes in the spatial and frequency domain. If more parameters are used and the principles of cascade feed forward networks are used to train the selected pixels and DCT coefficients, the performance of the suggested algorithm is projected to increase.

References:

[1] Chan C-K and Cheng L-M 2004 Hiding data in images by simple LSB substitution. Pattern Recognit. 37: 469–474

[2] Kukapalli V R, Rao T B and Reddy B S 2014 Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare. International Journalof Computer Trends and Technology 15(3): 97-101

[3] Dighe D and Gand Kapale N D 2013 Random InsertionUsing Data Parity Steganography Technique. Int. J. Eng. Sci.Innov Technol (IJESIT) 2(2): 364–36

[4] Dadgostar H A and Fsari F 2016 Image steganography basedon interval-valued intuitionistic fuzzy edge detection and modified LSB. Journal of Information Security and Applications(JISA). 30: 94–104

[5] Akhtar N 2016 An LSB substitution with bit inversion steganography method. In: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics 43: 515–521

[6] Wu D-A and Tsai W-H 2003 A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett.24(9–10):1613–1626.

[7] D.Suneetha 2017 Data Hiding Using Fibonacci EDGE Based Steganography for Cloud Data International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5565-5569

[8] Kiran 2018 A Secure Steganography Approach For Cloud Data Using Ann Along WithPrivate Key Embedding International Journal of Computer Science and Information Security (IJCSIS),Vol. 16, No. 6, June 2018

[9] D.Suneetha , 2018 Enhancement of Security for Cloud DataUsing Partition-Based Steganography,springer AISC Series

[10] Dr.R.Kian Kumar ,2019 A Novel Approach For Data Security In Cloud Environment Using Image Segmentation And Image Steganography, springer AISC Series

[11] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2015. Proceedings. 2001 International Conference on. Vol. 3. IEEE, 2001.

[12] Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.

[13] Awwad, Yousef Bani, and Mohammad Shkoukani. "STC The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.

[14] Akimov, Kolesnikov. "Security implications of virtualization: A literature study." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 3. IEEE, 2017.

[15] Horspool. "Hide and seek: An introduction to steganography." IEEE security & privacy 99.3 (2018): 32-44.

[16] R. Chandramouli and N. Memon,"Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2016.

[17] R.J. Anderson, F.A.P. Petitcolas, “On The Limits of Steganography”, IEEE Journal of Selected Area in Communications, pp. 474-481, May 2017.

[18] N.F. Johnson, S. Jajodia, “Stag analysis: The Investigation of Hiding Information”, IEEE, pp. 113-116, 2016.

[19] H.Hastur,Mandelsteg,ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/

[20] K. Rabah, "Steganography- the Art of Hiding Data", Information Technology of Journal, 3(3), pp.245-269, 2014.

[21] N.F.Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer 31, pp.26-34, 1998.

[22] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, “Information Hiding - A Survey", IEEE Proc., Special Issue on Protection of Multimedia Content, 87(7),pp.1062-1078, July 2015.

[23] Dr.R.Kirankumar, 2nd International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systemsand Computing 828

[24] suneetha,4 th International Conference on Information Systems Design and Intelligent Applications” held during 19th-21st July, 2018

[25] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." Image Processing, 2001. Proceedings. 2001 International Conference on. Vol. 3. IEEE, 2017.

[26] Patil, Priyadarshini, et al. "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science 78 (2016): 617-624.

[27] Awwad, Yousef Bani, and Mohammad Shkoukani. "STC The Affect of Genetic Algorithms on Blowfish Symmetric Algorithm." IJCSNS 17.3 (2017): 65.