AI Based Image Steganography

[1]Jahnavi S, [2]Nayana S, [2]Pruthivika V, [2]Chandini S, [2]Pushpamala S

[2] UG Students, Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India

[1] Associate. Professor, Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India

Abstract – Steganography is the technique of hiding private or sensitive information within something that appears to be nothing be a usual image. Steganography involves hiding Text Messages, so it appears that to be a normal image or other file. If a person views that image which has hidden information inside, he or she will have no idea that there is any secret information. The project provides a very simple application which simplifies the manual work done by hiding communication. We printed out the enhancement of the image steganography system using RSA approach, ANN and LSB method to provide a means of secure communication. Efforts to improve the robustness and embedding capacity are necessary to ensure that embedded information can securely defend against attacks This application is very time efficient and convenient for the user.

I. INTRODUCTION

The big losses and digital signal transmission due to unwanted access of data with the high demand in both; the security of data becomes an imperative and critical concept. For data securing and preventing them from unauthorized access, encryption and steganography processes is used. The most important concept in any communication process between sender and receiver via the transmission channel is security. The using of advance technology inside the World Wide Web (WWW) to exchange information leads to increase the challenges and risks. However, the management of challenges and risks is possible with using an advanced technology of secure networks but these technologies are not enough for information security over communication between sender and receiver. Therefore, additional mechanisms of security are needed to secure information. An origin of steganography word is Greek, steganography means "covered writing" or "concealed writing".

The technique of hiding secret information or data in an image is called image steganography. Generally, pixel intensities are the methods used in hiding data in image steganography. According to, images are the most popular and widely use cover objects used in steganography. The degree of redundancy in images has made it the most sought for, in terms of steganography. Two categories of classification namely spatial –domain and transform domain based have been proposed in image steganography. Explained that spatial domain embeds the message directly into the pixels intensity whereas the transform domain also called the frequency domain transform the image before the message is embedded. Various file formats exist in image steganography. TIFF, JPEG, PNG, GIF and BMP can all be implementing in image steganography. However, each of the file formats poses its own unique advantages and disadvantages. Because pixel intensities are used in image steganography, there is sometimes variation in the intensity of the original image and the stego image or the embedded image. The variation in intensity is so trivial or subtle in that it is not detectable or perceptible to the human eye.

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described it in 1978. RSA algorithm is an asymmetric cryptographic system that utilizes two set of keys to encrypt and decrypt messages to ensure the security of quality information. In its performance, the keys are generated through a process of complex mathematical computation. The two keys generated are called public key and private key. The public key is distributed to the sender of a message to encrypt the message whiles the receiver of a message keeps the private key secretly to decrypt the public key encrypted message.

LSB stands for Least Significant Bit. There are basically two methods of concealing messages in an image: Least Significant Bits and Discrete Cosine Transform. LSB belongs to the spatial domain whereas the DCT falls in the category of a frequency domain. The simplest and easiest method to implement in image steganography is LSB. In LSB, there is the encoding of the data to be hidden since the individual pixels of the least significant bits of the image are modified. Using an image of 8bit, the Least Significant Bit, thus the last bit is the 8th number bit of each byte of the carrier image becomes the bit which is considered as the secreted message. For 24 bit image, the colors of the each component such as the Red, Green, and Blue (RGB) are changed. For example: Assuming cover images has two- pixel values as (1010 0000 0010 0011 0100 0111) and (0101 1111 0011 1100 0111 1100).Let‘s also assume the secret bits are 1101112, immediately the secret bits are embedded, the pixel values also change. That pixel values are: (1010 0001 0010 0011 0100 0110) and (0101 1111 0011 1101 0111 1100). The underlined bits indicate the bits changed from the original value and only three bits in the carrier image get changed. Now days, Artificial neural network becomes very popular and useful model in various cases such as clustering, prediction, classification and pattern recognition. It is top most model of machine learning. It becomes adequately aggressive to ordinary regression and the statistical model concerning usefulness.

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.

The project provides a very simple application which simplifies the manual work. This application is very time efficient and convenient for the user. AI implementations have tweaked even steganographic techniques to make attacks harder to detect.

II. PROBLEM DESCRIPTION

As we know that steganography is a message hiding technique so that a user can send or communicate to the other user about their secret message securely. LSB is one of the technique which is used for hiding the secret message. LSB hiding technique works as it hides the secret message directly in the least two significant bits in image pixels, which affects the image resolution, due to this it reduces the image quality and make the image easy to attack. The amount of information that can be hidden is generally less. Hiding an image of the same size will probably lose a fair bit of information. In the case of Images, the algorithms do not exploit the structure of images. They don’t use the patterns found in natural images.

III. RELATED WORKS

Previously many researchers performed implements on image steganography.

[1]Omid Torki, Maede Ashouri-Talouki, Mojtaba Mahdavi have proposed two algorithms for steganography in blockchain, the first one is a high-capacity algorithm for the key and the steganography algorithm exchange and switching, and the second one is a medium-capacity algorithm for embedding hidden data. [2] A. H. Mohsin , A. A. Zaidan1 , B. B. Zaidan , K. I. Mohammed , O. S. Albahri , A. S.Albahri & M. A. Alsalem proposes and discusses a novel steganography based blockchain method in the spatial domain as a solution. The novelty of the proposed method is the removal and addition of new particles in the particle swarm optimization (PSO) algorithm. In addition, hash function can hide secret medical COVID-19 data in hospital databases whilst providing confidentiality with high embedding capacity and high image quality. [3] S. Pramothini, Y.V.V.S. Sai Pavan, N. focuses on exploring the suitability of Blockchain. ensuring integrity in the mobile

storage medium. A scheme that uses steganography to ensure confidentiality and blockchains to ensure non-repudiation is presented in this paper [3]. [4]Wenying Wen, Yunpeng Jian, Yuming Fang, Yushu Zhang and Baolin Qiu, the field of medical image content protection and security sharing, the introduction of blockchain technology has a problem in that the secret key may be lost and cannot be recovered. Therefore, this paper proposes an authenticable medical image-sharing scheme based on an embedded small shadow QR code and a blockchain framework. First, a small shadow image is obtained by employing a secret image-sharing method based on the Chinese remainder theorem[4]. [5] Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, Pulung Nurtantio Andono proposes an adaptive method that can select the most optimal pattern to minimize the error ratio due to message embedding. This adaptive pattern can optimize the performance of the inverted LSB substitution method, based on the two-bit + least-significant-bit (LSB) pattern in the container image. [6] Ardiansyah, G., Sari, C.A., Setiadi, D.R.I.M., Rachmawanto, E.H. proposed a combination of two Steganography domains coupled with Cryptography which aimed to make confidential information more secure and inaccessible to unauthorized persons. Messages are encrypted using the 3-DES method. On the other side of the cover image is decomposed into four subbands by using DWT. LH, HL, and HH subbands are chosen to embed encrypted message using LSB method. The last step, done Inverse DWT (IDWT) to get the stego image reconstruction. [7] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran, B. Front. Comput. Neurosci. This research article provides a thorough review of existing types of image steganography and the recent contributions in each category in multiple modalities. The article also provides a complete overview of image steganography including general operation, requirements, different aspects, different types and their performance evaluations. [8] Karakus, S., Avci, E, in the study, a new optimization-based method has been proposed by making use of the similarities of the pixels. In order to test the performance of the proposed method has been used visual quality analysis metrics such as MSE, RMSE, PSNR, SSIM and UQI. [9] Elavarasi Gunasekaran & Vanitha Muthuraman, proposed Double Layered Secure Secret Images Sharing Scheme is the first of its kind technique in this era, which enables double protection for sensitive data by incorporating two layers of secret sharing. In first layer, threshold-based secret sharing is performed and the second layer RIIIV+Ue3IIsKaUV IIIYIISeUIRUP RIIZI3KII6KIP ~U~~ II secret sharing approach. [10] Nipanikar, S.I., Hima Deepthi, V., Kulkarni, N. proposes a method for image steganography using sparse representation, and an algorithm named Particle Swarm Optimization (PSO) algorithm for effective selection of the pixels for the purpose of embedding the secret audio signal in the image.

IV.MATERIALS AND METHOD

1. HIDING USING LSB

LSB steganography is a popular method for hiding information in digital images. It is easy to implement and the changes made to the image are usually imperceptible to the human eye. However, it is vulnerable to steganalysis techniques that can detect the presence of a hidden message by analyzing the statistical properties of the image. Therefore, LSB steganography should be used with caution, and additional security measures should be employed to prevent detection by steganalysis techniques.

Based on Figure 1 it can be seen that from 9 pixels cover image only 4 pixels change value, and change value with a maximum difference is 1. It might happen if message bit equal to last bit cover then pixel value cover completely unchanged. This is what makes the imperceptibility aspect of the LSB technique so good and the human eye can not detect changes in pixel values directly. But this method is so simple and very easy to guess, this method also has a maximum payload of 1 bit per pixel when the maximum embedding per pixel is only 1 bit. Then this method still needs to be developed further to increase message payload and security.

Fig.1. WORKING OF LSB ALGORITHM

2. Secret Encryption using RSA

The RSA encryption algorithm is an asymmetric encryption algorithm that is broadly used in some products and services. A private and public key are generated, with the public key being available to anyone and the private key being a private known only by the key set creator. With RSA, the private or public key can encrypt the information, while the different key decrypts it. This is one of the reasons RSA is the second-hand asymmetric encryption algorithm. A prime number is the one that is divisible only by one and itself. For example, 3 is a prime number, because it can be divided only by 1 or 3. But 4 is not a prime number, because other than by 1 and 4, it can also be divided by 2. Likewise, 5, 7, 11, 13, 17....are prime numbers whereas 6, 8, 9, 10, 12 are non-prime numbers. RSA uses two exponents including e and d, where e is made public and d is private. Let P is the plaintext and C is the ciphertext. There are two algebraic structure including ring and a group. Figure 2 shows RSA Algorithm.

Encryption/decryption ring I− RSA need a ring R =< Zn, +, x > for encryption and decryption with two arithmetic operations i.e., addition and multiplication. In RSA, this ring is public because the modulus n is public. Someone can send a message to someone utilizing this ring to do encryption.

Key generation group i− RSA need a multiplicative group G =< Zϕn,*, X > for key generation. This group provides only multiplication and divisions, which are required for generation of public and private keys. This group is secret from the public because its modulus, ϕ(n) is secret from the public.

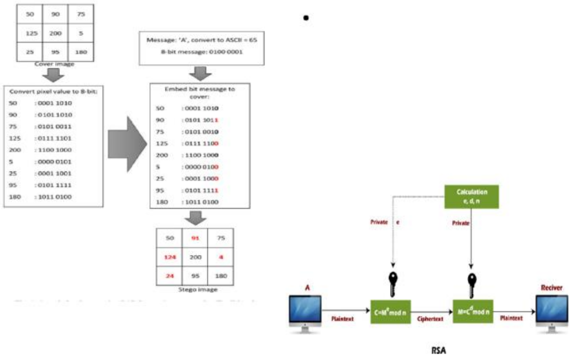


Fig.2. RSA ALGORITHM

To use RSA for secret encryption, the following steps are typically involved:

1.Randomly generates two primes P and Q of length K / 2 bit ;

2.To use RSA for secret encryption, the following steps are typically involved:

3.Randomly generates two primes P and Q of length K / 2 bit ;

This is the necessary and sufficient conditions for solvability of the decryption key keyE * keyD modΦ(n)=1

4.Calculate the decryption key, keyD=keyE-l mod(n), keyE-l is inverse for the decryption key keyD. The formula of the original equation is keyE * keyD modD(n)=1, cD(n) is known as the Euler function of n, the value is Φ(n) =(P1)*(Q-l)

Now, the public key, encryption key and decryption key are all created. Then, the process of encryption of the plaintext and decryption of ciphertext is as follows:

1.Encryption: C = MkeyE mod publicKey; where M is plaintext, C is ciphertext.

2.Decryption: M = CkeyD mod publicKey; in which M plaintext, C is ciphertext.

To implement RSA cryptosystem is a rather complex process, which involves the generation of prime numbers, large integer modular arithmetic and other mathematical calculations. In RSA cryptosystem, p and q are large prime numbers. To achieve it, the most important factor is the efficiency in generate large prime numbers. Normally, probabilistic algorithms are adopted in generate large prime numbers. This should be: p, q are large prime numbers, when seeking primes p and q with the method of factorization, then the difficulty is actually the same as to attack to RSA (the decomposition of large composite number) , it's feasible as to the computer . In general, probabilistic algorithms do not focus on generating prime numbers, but first randomly generate a large odd number, then determine whether this odd integer is a prime number with probabilistic algorithms (this process is commonly referred to as Primality Test).

RSA uses two keys, a public key for encryption and a private key for decryption. The security of RSA is based on the fact that it is difficult to factor large numbers into their prime factors.

To encrypt a message using RSA, the sender first obtains the public key of the recipient. The public key consists of two numbers, a modulus n and an encryption exponent e. The sender then converts the message into a numerical value m, using a pre-defined method. The numerical value of the message must be less than the modulus n.

The sender then applies the encryption function to the numerical value of the message and the encryption exponent e, using the following formula:

c = m^e mod n

The resulting value c is the encrypted message, which can be sent to the recipient using any communication channel.

To decrypt the message, the recipient uses their private key, which consists of two numbers, a decryption exponent d and the same modulus n. The decryption exponent d is calculated using the following formula:

d = e^(-1) mod (p-1)(q-1)

where p and q are the prime factors of the modulus n. The private key must be kept secret and must not be shared with anyone.

The recipient then applies the decryption function to the encrypted message c and the decryption exponent d, using the following formula:

m = c^d mod n

The resulting value m is the original numerical value of the message, which can be converted back into the original message using a pre-defined method.

3. Pixel Selection using ANN

Now days, Artificial neural network becomes very popular and useful model in various cases such as clustering, prediction, classification and pattern recognition. It is top most model of machine learning. It becomes adequately aggressive to ordinary regression and the statistical model concerning usefulness. Artificial Intelligence includes the concept neural network, machine learning, and deep learning. Recently cloud computing, Artificial intelligence, information security, internet, forensic techniques (science) are hotspots inspiring scenario for information & communication technology.

An ANN is an arithmetical form based on the unctions of biological neural structure shown in figure 3. ANN is considered as a statistical data of nonlinear type, where the complex association among the inputs and outputs are determined. ANN is used as a random number generator. ANN takes data samples to reach at solutions that minimize time complexity. The ANN is combined with multiple nodes that are called neurons. The nodes are connected by links and each link has a specified weight. Each of the nodes is assigned some input value. These input values are multiplied by the weight of the links. Then these input values are exclusive-or (XOR) with other input values and produce the desired outputs.

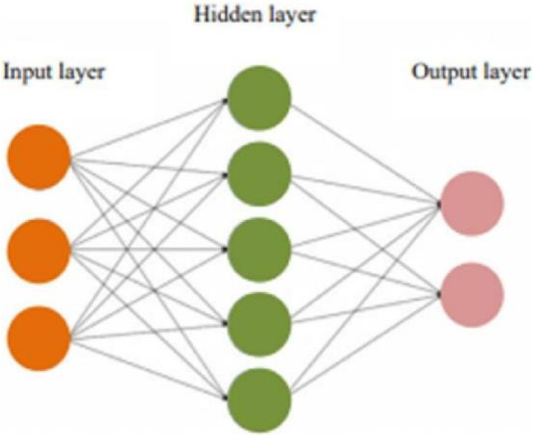


Fig. 3. Artificial Neural Network

Basically it is an interconnection of group of nodes which is inspired by simple structure of neuron in human brain. In above fig circular node stands for artificial neuron. Each arrow represents the connection between this neuron in the sense ones output is input for next stage neuron. Neurons, Connections with respective weights and Propagation function are the main components of the ANN.

An artificial neural network has many nodes i.e. processing unit analogs to neurons in the brain. Each node is provided with a node function. This, with a set of local parameters, determines the output of the node with a given input. Local parameters if modified may alter the node function. Therefore artificial neural network is an information processing system. The information is processed by the elements called the neurons. Connection links transmit the signals. The links have associated weights. That is, if x is the input to a neuron and the associated weight of the link is w then the net input given to the neuron is wx. Where wx stands for product of w and x. Output signal can be obtained from the activation function of the neuron i.e. if the activation function is f and the net input to the neuron is wx, then the net output from the neuron will be f(wx).The neural net can either be of single layered or multilayered.

At input side,

$$: \quad \sum_{=1}^{4} ,$$

At output side,

$$: \quad = \quad (\,)$$

ANN is computational model which is inspired by learning ability of a human intelligence nerve system. Basically it is structure processing method. Special characteristics of ANN make it is prominent. It has more number of weighted connections between those distributed elements. An ANN is highly utilized since it has enormous Parallelism nature, Distributed rendition with learning ability and fault tolerance. Main module of ANN are processing unit, topologies and learning algorithms. A digital image is represented in the form of matrix. Each value of matrix represents colour information of a pixel. This matrix is using as input for the neural network. Image is divided into many small parts. Hence small dimensions or values of image can quickly and easily help learning of network, set up the vector size and input vector numbers. Highly complex data is easily processed by ANN. Adaptive learning means the ability of learning how to complete task based on given initial conditions or training. Self-organization is more specific characteristics of ANN. An ANN generates its self or own organization (representation) of information which is received at time of learning time.

The process of pixel selection using ANNs typically involves the following steps:

1.Data preparation: The first step is to prepare a dataset of images with known pixel labels. These labels indicate which pixels are important for the task at hand. For example, in an image classification task, the labels might indicate which pixels correspond to the object of interest. In an object detection task, the labels might indicate which pixels correspond to the object's bounding box. In an image segmentation task, the labels might indicate which pixels belong to each object class.

2.Neural network architecture: The next step is to choose an appropriate neural network architecture for the task at hand. There are several different types of neural networks that can be used for pixel selection, including convolutional neural networks (CNNs) and fully connected neural networks (FCNs). CNNs are commonly used for image classification and object detection tasks, and can also be used for pixel selection by training the network to predict a binary mask indicating which pixels are important. FCNs, on the other hand, are specifically designed for image segmentation tasks, and can be used for pixel selection by training the network to output a pixel-wise classification map indicating the class label of each pixel.

3.Training the neural network: The next step is to train the neural network on the dataset of images with known pixel labels. This involves feeding the images into the network and adjusting the network's weights and biases to minimize the difference between the predicted pixel labels and the true pixel labels.

4.Evaluation: Once the neural network has been trained, it can be evaluated on a separate set of test images to assess its performance. This involves comparing the predicted pixel labels with the true pixel labels and calculating various performance metrics such as accuracy, precision, and recall.

V. RESULT

The experiments were conducted and results were acquired for the proposed AI based Image steganography. To accomplish the high secret image security, imperceptibility, confidentiality and robustness against different steganalysis attacks such as RS attack and noise, the proposed steganographic technique is implemented on MATLAB to evaluate the best visibility for secret image embedding algorithms based on RSA algorithm.

Below figure 4 shows the overview of AI based Image steganography of problems. Areas in which toolboxes are available include signal processing, control systems, neural networks, fuzzy logic, wavelets, simulation, and many others.

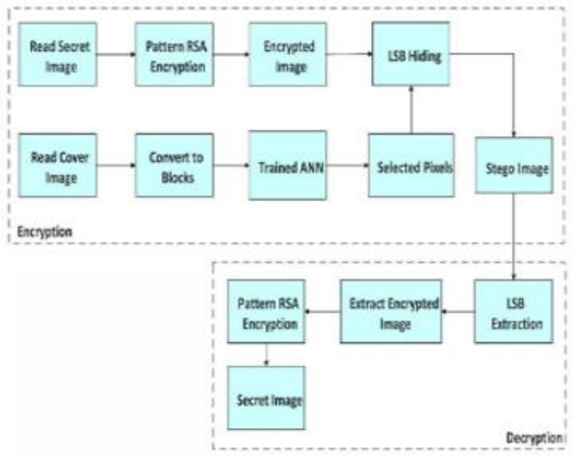
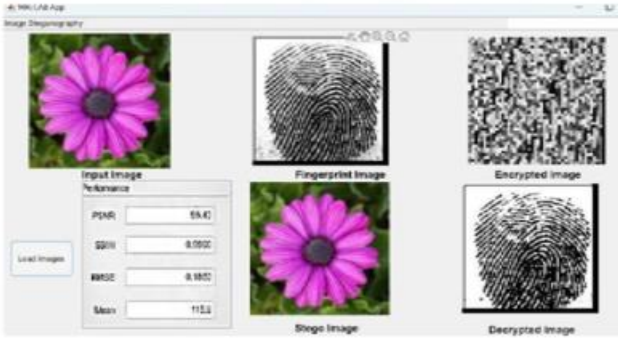


Fig. 4. Flow chart.



Performance

PSNR 55.43

SSIM 0.9900

RMSE 0.1852

Mean 115.8

Fig 5:AI based image steganography Performance Analysis:

4. MATLAB

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning.

In Academic environment, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In Industry, MATLAB is the tool of choice for high-productivity research, development, and analysis.

MATLAB features a family of add-on application-specific solutions called toolboxes Very important to most users of MATLAB, toolboxes allow us to learn and apply specialized technology.

Toolboxes are comprehensive collections of MATLAB functions (M-files) that extend the MATLAB environment to solve particular classes

The excellent visible quality of stego image is the most essential property of steganographic system because it is hard to be noticed by the detectors; the distortion between cover image and stego image is measured in terms of peak signal-to-noise ratio (PSNR). This is a traditional image quality measurement which indicates the ratio of a maximum possible power of a signal and power of corrupting noise which distresses the fidelity of its representation.

PSNR= 10 10(255)2
MSE dB (1)

where MSE stands for mean-square error, defined as

MSE= 1 ∑ ∑ (, − ,)^2 (2)
=1 =1

RMSE is the square root of the MSE.

Structured Similarity Index Measurement (SSIM): SSIM is a metric of comparison to check the similarity between the cover image and stego image. It measures the perceptual difference between the two images.

SSIM (2µ x µ y + c 1) (2σ xy +c 2)/ ((µ x) 2 + (µ y) 2 +c 1) ((σ x) 2 + (σ y) 2 + c 2) (3)

Comparison between proposed and the existing scheme:

In this section, the proposed scheme was compared with existing scheme and the results achieved in terms of PSNR metrics are tabulated in Table 1. The obtained values clearly show that the PSNR got heavily improved in the proposed strategy in comparison with existing technique. Moreover, the PSNR values of proposed scheme is 55.43 respectively. While, the existing scheme achieved only just 50.49, 48.64, 47.4113, 49.1347 and 53.3 respectively, which are lower than the proposed results. Thus the reconstructed image quality of the proposed scheme was found to be when compared to existing scheme as shown in figure 6 and 7.

Method	Author	PSNR values in db
Convolutional Neural Networks (CNN), Auto- Encoder network and U-net architecture (2021 [18])	Ismail Kich, El Bachir Ameur, Youssef Taouil, Amine Benhfid	50.49 db
Image steganography technique using a Novel Puzzle (2020 [16])	M. Espina, C. Fajardo, D. Gerardo, and R. P. Medina	48.64 db
New optimization- based method (2022 [8])	Karakus, S., Avci	47.4113 db
Ant Lion Optimization algorithm (2021 [9])	Elavarasi Gunasekaran & Vanitha Muthuraman	49.1347 db
Modified cycle Generative Adversarial Networks (Mod Cycle GAN) algorithm (2020 [17])	Kuppusamy P.G., K C Ramya, S Sheebha Rani, M Sivaram	53.3 db
Proposed method		55.43 db

Table 1: Comparison between existing and proposed method

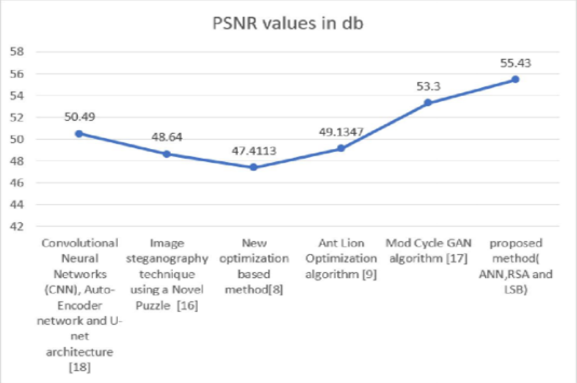


Fig 6: Comparing PSNR values with existing and proposed method in Graph

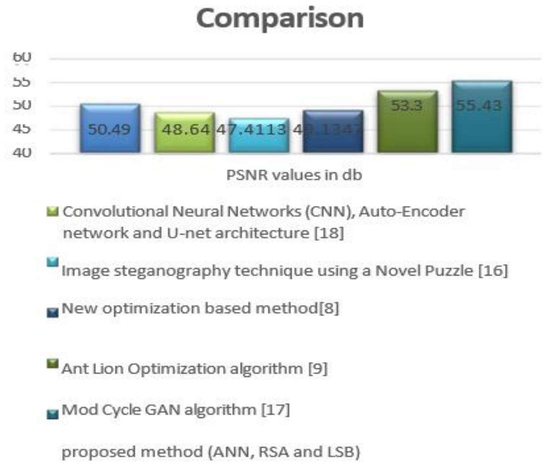


Fig 7: Comparison in Barchart

Thus, From above figure 6 and 7, it is clear that the proposed scheme is better in image reconstruction too in comparison with other existing methods.

VI. CONCLUSION

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using RSA, ANN for pixel selection and LSB for hiding approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image.

This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

The main goal of this projects it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data. The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message. Better results are obtained without any loss of information.

The project provides a very simple application which simplifies the manual work. This application is very time efficient and convenient for the user. AI implementations have tweaked even steganographic techniques to make attacks harder to detect.

REFERENCE

[1] Omid Torki, Maede Ashouri-Talouki, Mojtaba Mahdavi. ‘Blockchain for steganography: advantages, new algorithms and open challenges’ .arXiv:2101.03103v1 [cs.CR] 8 Jan 2021

[2] A.H. Mohsin, A. A. Zaidan1, B. B. Zaidan, K. I. Mohammed, O. S. Albahri, A. S.Albahri & M. A. Alsalem(2022).’PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in

decentralised hospitals intelligence architecture’. https://doi.org/ 10.1007/s11042-020-10284-y

[3] S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini. ‘Securing Images with Fingerprint Data using Steganography and Blockchain. International Journal of Recent Technology and Engineering’ (IJRTE)ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018

[4] Wenying Wen, Yunpeng Jian, Yuming Fang, Yushu Zhang and Baolin Qiu. 'Authenticable medical image-sharing scheme based on embedded small shadow QR code and blockchain framework’. https://doi.org/10. 21203/rs.3.rs-1806415/v1

[5] Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, Pulung Nurtantio Andono(2020).‘Inverted LSB Image Steganography using Adaptive Pattern to Improve Imperceptibility’. 10.1016/j.jksuci. 2020.12.017 *I*

[6] Ardiansyah, G., Sari, C.A., Setiadi, D.R.I.M., Rachmawanto, E.H.‘Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm’.2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE). IEEE, pp. 249– 254. https://doi.org/10.1109/ICITISEE. 2017.8285505

[7] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran.'Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research'.Front. Comput. Neurosci., 11 December 2019.

[8] Karakus, S., Avci, E.‘A new image steganography LI method with optimum pixel similarity for data hiding in medical images.’(March 2022) .https://doi.org/10.1016/j.mehy.2020.109691

[9] Elavarasi Gunasekaran & Vanitha Muthuraman.’Double layer secure secret images sharing scheme for biometrics’(August 2021).2022,liii Distributed and Parallel Databases

[10] Nipanikar, S.I., Hima Deepthi, V., Kulkarni, N.’ A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform’ (December 2018).https://doi.org/ 10.1016 /j.aej. 2019.09.005.

[11] S Jahnavi, C Nandini. ‘Novel multifold secured system by combining multimodal mask steganography and naive based random visual cryptography system for digital communication’. Journal of computational and theoretical nanoscience, American Scientific Publishers, 17 (12), 5279-5295, https://doi.org/10.1166/jctn.2020.9420

[12] S. Jahnavi and C. Nandini, "Smart Anti-Theft Door locking System," 2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), 2019, pp. 205-208, doi: 10.1109/ICATIECE45860.2019.9063836.

[13] Nandni, C., Jahnavi, S. (2021). Quantum Cryptography and Blockchain System: Fast and Secured Digital Communication System. In: Bhateja, V., Satapathy, S.C., Travieso-González, C.M., Aradhya, V.N.M. (eds) Data Engineering and Intelligent Computing. Advances in Intelligent Systems and Computing, vol 1407. Springer, Singapore. https://doi.org/10.1007/ 978-981-16-0171- 2_43

[14] Jahanvi Shankar, C Nandini. ‘Hybrid Hyper Chaotic Map with LSB for Image Encryption and Decryption’. Scalable Computing: Practice and Experience, universitatea de vest din Timisoara, Volume 23, Issues 4, pp. 181–191, DOI 10.12694/scpe.v23i4.2018181-192.

[15] Jahnavi S, Dr.C. Nandini. ‘Digital Data Security Using Visual Cryptography And Steganography Techniques: An Extensive Review’. Journal of Emerging Technologies and Innovative Research 5 (9), 212

[16] M. Espina, A. C. Fajardo, B. D. Gerardo, and R. P. Medina, “A novel puzzle-based image steganography technique,” in Eleventh International Conference on Graphics and Image Processing, 2020, vol. 1137317, no. 1.

[17] Kuppusamy P.G., K C Ramya, S Sheebha Rani, M Sivaram,"A Novel Approach Based on Modified Cycle Generative Adversarial Networks for Image Steganography" March 2020Scalable Computing 21(1):63-72 DOI:10.12694/ scpe.v21i1.1613

[18] Ismail Kich,El Bachir Ameur,Youssef Taouil,Amine Benhfid,"Image Steganography Scheme Using Dilated Convolutional Network"2021 12th

International Conference on Information and Communication Systems. (ICICS), 10.1109/ ICICS52457.2021.9464546