As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology, 8(05):583-589, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0805089
Available online at: http://www.ijmtst.com/vol8issue05.html

Artificial Neural Network Based Technique for Hiding Image into Video using DWT- LSB, MSB for Cloud Environment

P.Venkata Hari Prasad[1] | Dr.K.Gangadhara Rao[2]

[1]Research Scholar, Department of CSE,Acharya Nagarjuna University
[2]Professor, Department of CSE,Acharya Nagarjuna University
Corresponding Author Email ID: p.venkatahariprasad@gmail.com

To Cite this Article
P.Venkata Hari Prasad and Dr.K.Gangadhara Rao. Artificial Neural Network Based Technique for Hiding Image into Video using DWT- LSB, MSB for Cloud Environment. International Journal for Modern Trends in Science and Technology 2022, 8(06), pp. 583-589. https://doi.org/10.46501/IJMTST0805089

Article Info
Received: 22 April 2022; Accepted: 12 May 2022; Published: 26 May 2022.

ABSTRACT

Cloud computing is a popular and widespread way to quickly access shared and enthusiastically adjustable possessions through a computer system. It provides strong rewards in the form of quantifiability, availability, and completely unique facilities. However, as this new technology advances, new risks and liabilities are also identified. A major problem with CSIT is Data Sanctuary. It is more difficult to set apart a safe haven for employer's records in the cloud computing environment because information is dispersed across several sites and facts are kept by a third party. There is an urgent need for a safe haven for hazy information in this situation, thus we developed an approach that produces better results than earlier ones.Steganography is a method of concealing the information in a picture.In this concept, most of themethods are depended on the LSB bit, but the hackers simply perceive as it inserts data consecutively in all pixels. Instead of inserting data consecutively few of the methods choose arbitrarily. So, in this paper we recommend novel method to provide the security for data. In this artificial neural network is used to select the cover video and train the best video for hiding the image. The selected video is converted into frames. The threshold is calculated to determine the size of redundancy and select the original cover video. In this for decomposition of video, hybridization of DWT , LSB and MSB is being used to identify the best position for inserting a secrete image into the cover image. For embedding process the artificial neural networks are used and those are used a s a classifier. The proposed algorithm provides better results it increases the PSNR and decreases the error ratio.

Index Terms: Artificial Neural Network, Classifier, Bit Slicing, IWT, PSNR, MSE, Standard Deviation, Entropy, Video Steganography

1. INTRODUCTION

Through the provision of computing resources on demand, the cloud is a popular way for users to share and move resources over the Internet. It provides a variety of conveniences to the many industries, including computer science, business, health, etc. Since information

is spread across various sites and is used by many different people, data security is a thoughtful and important topic in the computing haze. The preservation of a safe haven for employer records is more difficult when there is a haze because third-person atmosphere facts are retained. Sanctuary is typically concerned at three different places when there is a haze in the air. In order to provide informational safety in the hazy environment, numerous techniques are proposed. As a trendy method of providing safety for our statistics, steganography is used.

Steganography is a procedure whereby information is scrambled that is concealed, perceptibility of the subsequent records might not be noticeable to the usual humanoid sense. In a comparable manner, cryptanalysis practices are recycled wherever the facts are scrambled by engendering a protected key. However steganography procedure is the stimulating one since the consequential archive is not perceptible by usual humanoid sense, but in cryptanalysis practices, if you distinguish the pivotal then the unlawful individual is informal to interpret the facts. There are 3 distinct categories of approaches in steganography, i.e. steganography in the terms of pictures, steganography in the terms of auditory and audio-visual archives. Due to increasing necessity of sanctuary steganography inthe terms of depictions are equal standard today [2, 3]. In this procedure, information is entrenching in the picture that subsequent picture is stowed in haze atmosphere in its place of stowage unique figures into them. Sanctuary of any steganography practices is depended on the assortment of pels for interleaving privacy communication. Consequently, brink pels is an improved knowledge to dwelling the privacy data. In its place of captivating the entire picture as input division, the picture is divided into many segments so we can conceal a large quantity of records [1].

In this part, we have projected a video-into image based steganography procedure that can shield and conceal the privacy information from unlawful individuals by introducing it simply in the separation based arbitrary brink pels. This procedure has been creation exceptional sanctuary for employer records in contradiction of steganalysis assaults. The enactment of this projected system is estimated with MSE, PSNR scruples and equated with many image steganography procedures.

2. RELATED WORK:

There are several many distinct advanced techniquesfor accumulating the data securely, using cloud computing such as point-to-point encrypted data broadcast, dynamic recommendation, steganography etc.There happen numerous picture built steganographic methods are extant to inset statistics steadily from unlawful employers [4, 5]. The picture-based methods can be divided into twofold classes of dominions: longitudinal, incidence dominions. In maximum of the latitudinal dominion, steganography methods are centred on LSB replacement method in which the LSB of pels is designated to insert the surreptitious communication. In this, we take twofold dissimilar classification LSB unused, LSB identical. In LSB standby method, LSB tad of every pel is re-placed with surreptitious documents. In LSB identical the LSB tad is substituted with subsequent tad of LSB if persons are not harmonized we can't inset the records. In both the methods we have multiple amalgamations of LSB tad lastly we have manifold behaviours of an entrenched surreptitious communication [6, 7].

Alternative entrenching method, called as pel significance modification procedure has remained projected. In this method the protection picture is separated into number of chunks that are assistant to every new and lastly choice arbitrary regulate pels to entrench the innovative documents. With concealing behind hand bends system, bend pels are recycled to insert the privacy communication. In this method recite the input picture, change the stealthy picture into twofold [8, 9]. Majorly, pick up the bend pels of a picture subsequently choosing straight entrench privacy information into the designated pels. HBC similarly indicate to low sanctuary since invaders effortlessly recognize the bend pels of a picture [10].

Some of the picture steganography methods are centred on LSB identical reconsidered method. In this, we compute the distinct inception scruples of creative picture and stego picture. If the inception scruples are harmonized or up to certain dimension enclosures privacy information into those pels straight. In this all is centred on the formularies that are recycled to estimate the inception standards. If an aggressor clutches the formularies, then effortlessly interpret the new records. In some of the procedure uses Markov evolution environment to calculate many topographies of a picture.

But it may have inconsequential debasing in presentation [11].

In order to effectively hide users' sensitive information, we have a variety of security algorithms based on image steganographic techniques. The proposed solution by Sharma V et al. uses image steganography and image cryptography to store user data in a cloud context. When obtaining a protected key, privacy information is first encrypted using the DES method, and then the protected key is once more encoded using the S-DES algorithm. The final one is created using the S-DES technique, which uses a key that is buried in a few pixels of the cover image [12, 13]. The outcomes are favourable, and it provides great security with suitable PSNR values.Yousef Bani et al. proposed in Awwad a genetic and blowfish-based technique for concealing sensitive information in images. For those cover images, the genetic population algorithm is used to compute the pixels, and the blowfish algorithm is used to encrypt the secret communication. Finally, a few pixels of the cover image are filled with the jumbled secret communication. Although it produces good results, compared to the several steganography algorithms, it produces more noise [14].

The improved blowfish algorithm, a method for concealing inputs in images, was proposed by Christina L et al. [15]. When employing the blowfish algorithm to encrypt data, a secret key can then be extracted and data is once more encrypted using se-ret keys. In a unique cover image, that encoded key is finally embedded.

An enhanced steganography technique, developed by Suneetha. D et. al., uses an efficient partition-based LSB algorithm to improve both picture quality and concealing capacity. The new cover picture is divided into several images for storing a large quantity of data in the projected process, and then an edge detection algorithm is applied to choose the edges of the picture [16]. Use LSB substitution for those edge pels after that to obfuscate private information in a photograph. The projected approach has been improved, and it increases the aspect of the stego picture while also improving the privacy communication duration [17].

A novel approach to the spatial context for a greyscale image was proposed by Kiran R et al. Using this technique, data is concealed in specific areas of the image so that anyone trying to pry it open cannot find it. When the projected algorithm is compared to the various current algorithms, the PSNR values are enhanced [18, 19].An innovative method for hiding secret communication in an image using a back propagation neural network was proposed by Sadeq AlHamouz et al. Two protection images—one a privacy image and the other a protection image—are recycled in his work and both are colour photographs [20]. For inserting privacy information, the technique uses two separate segments: one for information entrenching and the other for information mining. The chosen pixel locations are determined using a response transfer record that is Fibonacci lined. With increased processing time and an improvement in image quality, the results are associated with numerous thrilling processes that result in high PSNR and low MSE scruple [21].

3. PROPOSED ALGORITHM:

The aim of this work is to analyzing the various existing steganography algorithm under different domains, various types steganography techniques and clearly understand the various limitation on those existing algorithms. To overcome those disadvantages, we have used artificial neural network for selecting cover video among multiple videos based on the threshold values. Later apply the concept of hybridization Of DWT along with the LSB, MSB techniques for identifying the pixels for embedding the secret image into the video, artificial neural network has been used as a classifier to classify the various regions to cover the secret image on the given selected video.

The main objective of the proposed algorithms is

(i) To enhance the embedding capacity (ii) To improve the PSNR and to reduce the MSE value

The methodology goes in the following manner:

START

1. Select the cover video using artificial neural network
2. Split the cover video into different frames
3. Apply the DWT technique to decompose the cover video into multiple frames and apply bit plain slicing technique
4. Split the secret image into multiple bit planes and apply bit slicing technique on each bit plain
5. Initialize the artificial neural network and identify the LSB and MSB from the video and embed the secret image into the cover video and obtain the stego video
6. Apply the reverse process to extract the secret image from the stego video

Fig 1: Steganography with Video

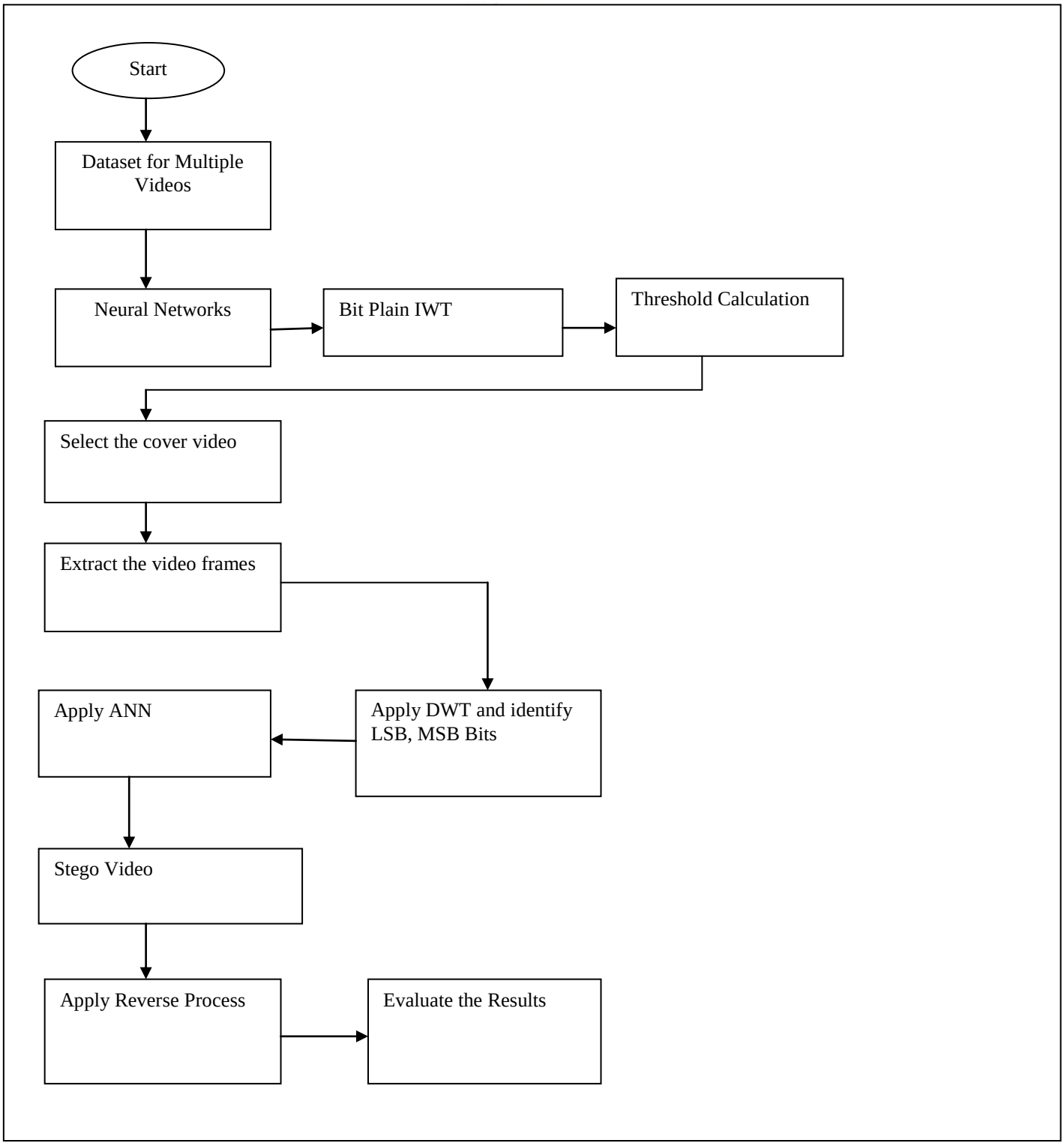

Fig 2: Process for Proposed Algorithm

4. RESULTS AND DISCUSSION:

The measurements like Malicious Square Fault Proportion and Highest- Gesture to Soundare two significant for shrewd picture eminence and boisterous proportion. PSNR is considered as an eminenceanalysisamongst novel and atreated picture.The larger PSNR, enhanced the eminence of therecreatedpicture. MSE is recycled as an accumulative sharpened faultamongst the creative and treated picture.

PSNR=10 log10 (MAXi)/MSE……. (1)

MSE=∑X, Y [J_1 (x, y)-J_2 (x, y)] ^{2}/X*J…….... (2)

Comparison of Table and Chart

This segment comprises assessment in amid the preceding effort through innumerable procedures and projected system designed scruples together PSNR and MSE. It is clear that designed standards illustrate certain substantial degrades recommend that projected system is faintly improved than the preceding methodologies. MATLAB apparatuses are recycled for assessing outcomes of the yielded picture.

Preceding MSE means that attained MSE scruples exhausting proposed approach procedures and both preceding and projected MSE are considered for identical dimension of pictures.

Preceding PSNR means that attained PSNR scruples exhausting Fibonacci brink based procedures and both preceding and projected PSNR are considered for identical dimension of pictures.

The following board tables from 1 to 4 displays comparison of Preceding and Projected Partitioning Method for different performance metrics.

Table 1: PSNR Comparison

S. No.	Previous PSNR	Proposed PSNR
1	68.45	75.67
2	64.53	76.89
3	78.67	83.99
4	75.46	84.02

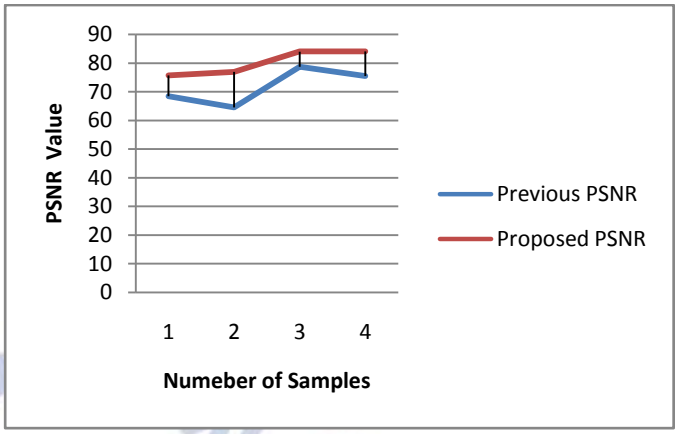

Fig 3: Comparison of PSNR

The above figure shows the comparison of PSNR values with previous existing works. Here the X-axis shows number if sample any Y-axis shows the PSNR values. It has been clearly observed the proposed work PSNR vales are comparatively greater than the existing work.

Table 2: MSEComparison

S. No.	Previous MSE	Proposed MSE
1	0.0076	0.0084
2	0.066	0.0067
3	0.084	0.0087
4	0.065	0.00789

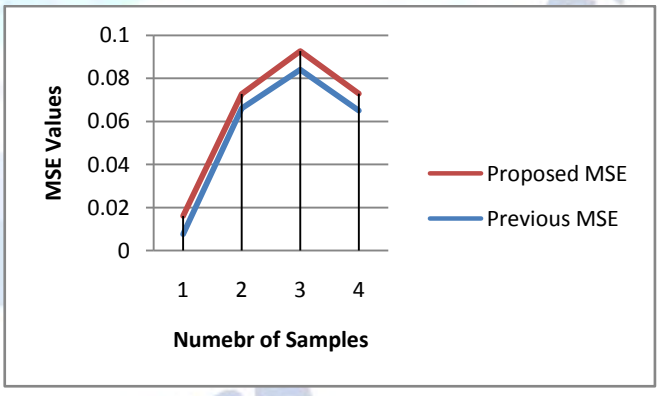

Fig 4: Comparison of MSE

The above figure shows the comparison of MSE values with previous existing works. Here the X-axis shows number if sample any Y-axis shows the MSE values. It has been clearly observed the proposed work PSNR vales are comparatively lesser than the existing work.

Table 3: Entropy Comparison

S. No.	Previous Entropy	Proposed Entropy
1	5.37	6.42
2	4.89	6.76
3	3.87	6.89
4	5.01	7.48

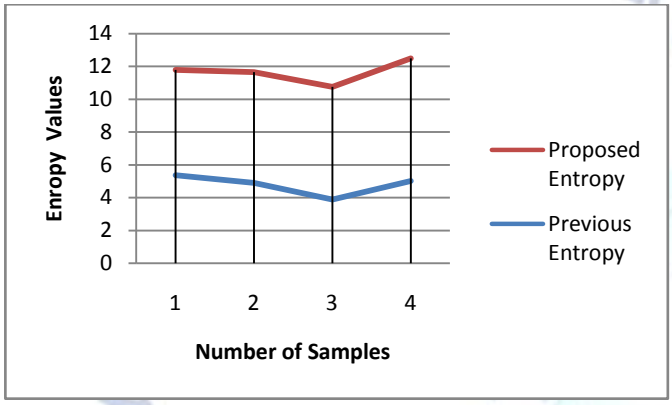

Fig 5: Comparison of Entropy

The above figure shows the comparison of Entorpy values with previous existing works. Here the X-axis shows number if sample any Y-axis shows the MSE values. It has been clearly observed the proposed work PSNR vales are comparatively greater than the existing work.

Table 4: Standard DeviationComparison

S. No.	Previous Standard Deviation	Proposed Standard Deviation
1	24.89	18.035
2	25.62	16.245
3	23.32	15.432
4	20.86	14.621

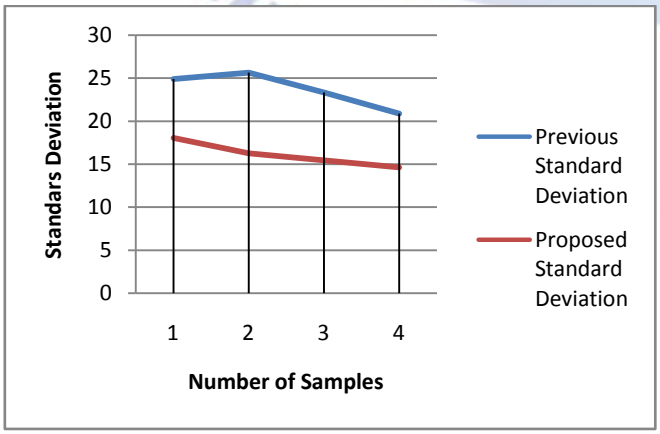

Fig 6: Comparison of Standard Deviation

The above figure shows the comparison of Standard Deviations values with previous existing works. Here the X-axis shows number if sample any Y-axis shows the MSE values. It has been clearly observed the proposed work PSNR vales are comparatively lesser than the existing work.

5. CONCLUSION:

Upon experimentation, it was found that the proposed alternatives of steganography techniques performed adequately and was able to embed message or image in an effective manner with minimum degradation to cover image quality. The investigational outcomes prove that the proposed algorithms increase security while maintaining the visual eminence of a video. The proposed steganography algorithms are resistant to several attacks, but the performance faintly decreased with the affine transformation. In the proposed work, the value of PSNR, MSE, Entropy and Standard Deviations are better than the existing techniques.In the future, Neural network could be hybrid with different available optimization technique and improve the quality of the stego image or stego video.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Singh, S., Singh, R., and Siddiqui, T. J. (2016). Singular Value Decomposition Based Image Steganography Using Integer Wavelet Transform. In Advances in Signal Processing and Intelligent Recognition Systems (pp. 593-601). Springer International Publishing.

[2] Rai, P., Gurung, S., and Ghose, M. K. (2015). Analysis of Image Steganography Techniques: A Survey. International Journal of Computer Applications, 114(1).

[3] Rasheed, Z. A. S. (2015). 'Steganography Technique for Binary Text Image. International Journal of Science and Research (IJSR) ISSN (Online), 2319-7064.

[4] Das, P., Kushwaha, S. C., and Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In Electronics and Communication Systems (ICECS), 2015 2nd International Conference on (pp. 845-849). IEEE.

[5] Deval, N. M. (2015) Secure Steganography Algorithm Based on Cellular Automata using Fibonacci Representation and Reverse Circle Cipher Application for Steganography.

[6] Ghebleh, M., and Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898-1907.

[7] Holub, V., and Fridrich, J. (2013, June). Digital image steganography using universal distortion. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 59-68). ACM.

[8] Jain, N., Meshram, S., and Dubey, S. (2012). Image Steganography Using LSB and Edge–Detection Technique. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 223.

[9] Jero, S. E., and Ramu, P. (2016). Curvelets-based ECG steganography for data security. Electronics Letters.

[10] Kanan, H. R., and Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications, 41(14), 6123-6130.

[11] Laha, S., and Roy, R. (2015, December). An improved image steganography scheme with high visual image quality. In Computing, Communication and Security (ICCCS), 2015 International Conference on (pp. 1-6). IEEE.

[12] Li, B., He, J., Huang, J., and Shi, Y. Q. (2011). A survey on image steganography and steganalysis.Journal of Information Hiding and Multimedia Signal Processing, 2(2), 142-172.

[13] Meligy, A. M., Nasef, M. M., and Eid, F. T. (2016). A Hybrid Technique for Enhancing the Efficiency of Audio Steganography.

[14] Mohamed, M. H., and Mohamed, L. M. (2016). High Capacity Image Steganography Technique based on LSB Substitution Method. Applied Mathematics and Information Sciences, 10(1), 259.

[15] Muhammad, K., Ahmad, J., Farman, H., and Jan, Z. (2016). A New Image Steganographic Technique using Pattern based Bits Shuffling and Magic LSB for Grayscale Images. arXiv preprint arXiv:1601.01386.

[16] Mungmode, S., Sedamkar, R. R., and Kulkarni, N. (2016). An Enhanced Edge Adaptive Steganography Approach Using Threshold Value for Region Selection. arXiv preprint arXiv:1601.02076.

[17] Nag, A., Singh, J. P., Biswas, S., Sarkar, D., and Sarkar, P. P. (2014). A Huffman Code Based Image Steganography Technique. In Applied Algorithms (pp. 257-265). Springer International Publishing.

[18] Rai, P., Gurung, S., and Ghose, M. K. (2015). Analysis of Image Steganography Techniques: A Survey. International Journal of Computer Applications, 114(1).

[19] Rasheed, Z. A. S. (2015). 'Steganography Technique for Binary Text Image. International Journal of Science and Research (IJSR) ISSN (Online), 2319-7064.

[20] Rayappan, J. B. B. (2013). Kubera kolam: A way for random image steganography. Research Journal of Information Technology, 5(3), 304-316.

[21] edighi, V., Cogranne, R., and Fridrich, J. (2016). Content-Adaptive Steganography by Minimizing Statistical Detectability. Information Forensics and Security, IEEE Transactions on, 11(2), 221-234.