

Secret Data Hiding using Artificial Neural Networks and Discrete Wavelet Transform

Shivank Tiwari, Nipun Mittal, Nupur Garg, Tribhuwan Kumar Tewari, Manish K Thakur

Abstract: Sensitive information requires safe and secure transmission. To hide such information, cryptographic models are used which require a set of keys in their working. Maintaining such keys itself is costly and securing them adds to the task of security. Also, such models are specific to a particular type of information that can be hidden i.e. not dynamic in working. The proposed interface omits the use of these complex mathematical models instead uses Neural Networks for data hiding. In this technique during the training phase of the network, it is subjected to a variety of data and once trained can be utilized to encrypt or decrypt the information of any size irrespective of what was used in training set. Once encrypted, it is concealed in a cover image using steganography and Discrete Wavelet Transform. This all being done at senders end, it is now transmitted over any channel to the designated receiver. After receiving the stegano image, a similar process is operated and thus we receive our secret message. For better results and analysis we incorporated our focus on the type of network, number of neurons, number of layers, simplicity and on parameters such as Peak Signal to Noise Ratio (PSNR). The proposed method shows greater flexibility in operation and low maintenance in regard to other crypto methods. The suggested technique would be suitable to incorporate in scenarios requiring least suspicion during an exchange of information and hence less prone to attackers. It would be easy to utilize on public modes of communication as sensitive information would be hidden in any media file which will appear just like some other normal media file.

Index Terms: Cryptography, Discrete Wavelet transform (DWT), Neural Networks, Steganography

I. INTRODUCTION

In today's connected world, distribution and access to information in digital form are unavoidable and now an important part of everyone's life. With this piracy, stealing sensitive information, etc through the medium of the internet has also become a grave issue. Finding preventive measures and deterring such type of activities has been a great field of research. One of the foremost challenges is to keep anyone not authorized to access information out while it is stored or

during sending data. Cryptography is one method that has been developed in this direction. The purpose of cryptography is to amend some valuable information also named to as a secret so that it can be accessed only by the destined authority. This covers the part that secret is not accessible to unauthorized people but the question is how to transmit it to designated ones. For this particular reason, we hide this secret information with any other file called host or cover. This file can be a snapshot, video clip or audio so that while transmissions, the suspicion is not aroused. Presenting the rough idea about our work, now comes the glimpse of challenges. What becomes the foremost challenge is that original quality is not significantly degraded while hiding the secret message. Also, to be applicable, this track should make message detection and extraction easier for designated people. It should be almost farfetched and not feasible for attackers, even when it is subjected to different manipulations. Also if somehow attackers manipulate the information, sender and receiver should be aware of it. In its extreme, if the attacker really ends up near the secret, the message should immediately self-destruct itself. With these things in mind, we worked on some aspects and present them here over criteria of imperceptibility, robustness, security, and payload. The imperceptibility can be defined as matching between the original file and file created after putting data in the original file. Hence, it is important to make the quality of embedded file less deviated from the original carrier so that no suspicion can be aroused [1]. How much a method can withstand many different types of attacks having a goal of erasing important information can be termed as Robustness [1]. The total amount of information that can be put into a host signal refers to payload [2]. One of the motives is to find a strategy of delivering higher payload keeping signal robust and imperceptible [3]. Also, the trade-off between robustness and imperceptibility is an issue of grave concern. More robustness means more data strength and hence degradation in transparency [4]. Till now a method to reach the optimization is under due consideration among the community. This paper describes a framework for sturdy hiding of data into image given that pictures represent a significant part of digital files. This method will go through three stages: concealing, transmission and retrieving. Contemporary hiding schemes are supported by mathematical models of Cryptography. These ways are simple to utilize but have a downside in terms of achieving good robustness, Maintenance of different keys which in turn itself require security, etc. Also, these methods are not versatile in nature i.e. if trained for small sized imaged cannot encapsulate large sized images or the other way.

Manuscript published on 30 June 2019.

* Correspondence Author (s)

Shivank Tiwari, Dept. of CSE and IT, Jaypee Institute of Information Technology, Noida, India.

Nipun Mittal, Dept. of CSE and IT, Jaypee Institute of Information Technology, Noida, India.

Nupur Garg, Dept. of CSE and IT, Jaypee Institute of Information Technology, Noida, India.

Dr. Tribhuwan Kumar Tewari, Dept. of CSE and IT, Jaypee Institute of Information Technology, Noida, India.

Dr. Manish K Thakur, Dept. of CSE and IT, Jaypee Institute of Information Technology, Noida, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>



Even if encryption is done, hiding poses many challenges towards fulfilling the objective as, in [5], alterations like compression, noise, etc. produced drastic effects as they modified hidden information. This all can be attributed to the fact that data was stored in the least significant bits of the carrier signal. Next in line comes transmission issues related to suspicion and channel of transmission, data loss, etc. Having a rough idea about challenges, coming to the reforms. If the data to be hidden is spread all over the carrier file, there are chances of increasing imperceptibility and robustness against different attacks [4]. In this regard, algorithms based on different transform domains such as Discrete Fourier Transform (DFT) [6], Discrete Cosine Transform (DCT) [7], Discrete Wavelet Transform (DWT) [8], Contourlet Transform [9] and others have been proposed [10]. Ruanaidh et al. [11] initially proposed to use Discrete Fourier Transform phase. The projected methodology, the info is kept inside vital frequency elements of a picture wherever solely the DFT section is employed for embedding. Extraction is disbursed employing an applied mathematics model. A combination of DFT and Hough Transform results in a stringent system capable to tackle severe attacks of scaling, rotation, etc. as supported by Zou et al. [12]. But DFT based schemes brings disadvantages regarding cropping attacks and also chances of survival of information drastically reduces if the ratios are manipulated. This can be attributed to the severe changes that occur to the frequency domain of the image. Koch and Zhao were the first to apply DCT [4]. In the process of putting data in host images, many areas in such images were selected randomly which were then with the help of DCT, transformed further modifying some medium frequency coefficients. The problem with DCT based schemes is that it cannot withstand robustness criteria against high compression attacks, geometric distortions, etc. The downside in DCT and DFT based methods, to an extent, were taken care of with DWT based strategies by utilizing multi-resolution techniques. A CT based methodology which incorporates features of the human visual system was put forth by Zaboli and Moin [13]. They proposed breaking down of cover signal into four regions. For the purpose of security, the PN sequence was utilized to disorganize thoroughly to give the random distribution of the file. This technique has shown improved strength against numerous forms of attacks like scaling, compression, and filtering. This strategy proved to be more imperceptible over other methods. In this paper, we propose an interface based on cryptography using Artificial Neural Networks and steganography using DWT. This setup shows promising results in image encryption and hiding amidst other applications with decent Peak Signal-to-Noise Ratio (PSNR). The contributions of this work can be summarized towards developing a framework which can encrypt secret messages and simultaneously hide them in multimedia. One of the greatest advantages of this framework would be that once trained with a set of images it can be extended to any image size that is because of the use of neural networks. With steganography, it was made sure to deter any suspicions during the transmission of the secret message over public means of communication. The remaining paper proceeds as Section II gives background details of cryptography neural nets etc. Section III covers the suggested methodology.

Section IV covers the implementation details of the proposed method, where results and comparative evaluations against different attacks are given. Finally, Section V concludes the paper.

II. BACKGROUND

A. Cryptography

Cryptography is the method used to prevent unauthorized access of valuable information to third parties. It is divided into two components: Encryption and Decryption. Encryption is the process of encoding a message into a secret packet which cannot be understood by anybody but the one who has its key. Decryption is the process of decoding the secret packet into the original message by the authorized person with the key. Therefore, Cryptography is the science covering the domain of information security and its related mathematical strategies applied in, for instance, data integrity, authentication, etc. There are many stages in the development of Cryptography. Classic Cryptography, which includes Transposition Ciphers and Substitution Ciphers. Modern Cryptography, which in itself is divided into two categories: Symmetric-key Cryptography, which means both sender and receiver have the same key to encrypt and decrypt data. Public-key Cryptography, which means both sender and receiver have distinct keys (a key-pair) to encrypt and decrypt data. We have proposed to implement Cryptography using Neural Networks(ANNs).

B. Neural Networks and Back Propagation

A Neural Network is an interconnection of densely connected layers where each layer contains a different number of neurons. Each neuron represents a single data variable in the network which has its own property i.e, weight and bias. Neural networks are used to produce near human-level intelligence by machines by mimicking are the structure of the human brain which in itself is a humongous neural network containing billions of neurons and trillions of connections between them. A positive weight of the neuron reflects an excitatory connection, while negative values mean inhibitory connections. The neural network has many attributes which include a number of layers, number of neurons in each layer, activation function between each layer. The determination of these attributes depends on the nature and complexity of the task performed by the neural network. The model is trained by adjusting the weights and biases of each and every neuron by iterating epochs on a given training dataset. The task performed by the neural networks is broadly classified into two categories: Supervised learning and unsupervised learning. In this paper, we will focus mainly on the supervised learning aspect of the neural networks. Supervised learning can further be divided into two categories: Regression and Classification. In Regression, we have to train our model to produce an output value for an input value. Here the value could be numeric, image or any form of readable content.

In Classification, we have to map the input to the finite set of predefined outputs i.e. for a given input we have to find the probability distribution of the given set of outputs and choose whichever has the highest probability. So, based on the above applications we train the neural network accordingly. This paper applies the neural network for Cryptography and shows the demonstration of encryption and decryption models using the network. In Artificial Neural Networks Backpropagation is a methodology employed to find a gradient which is further utilized to determine weights to be used in neural nets. Backpropagation stands for "the backward propagation of errors," as a slip-up is calculated at the output and propagated to all the preceding layers. Backpropagation can also be said to be an exploitation of chain rule as it iteratively figures gradients for every layer thus being a generalization of delta rule to multi-layered feedforward networks.

C. Discrete Wavelet Transform

The wave transform is prominently accustomed to decompose a logo into a bunch of basis functions. These basis functions are mentioned as wavelets. One example wave, noted as mother wave, is used to induce all the wavelets by dilations and shifting [8]. The DWT has been familiar with as a very capable and extensible methodology for sub-band breakdown of signals. They have a key advantage over Fourier transforms of temporal resolution i.e., it'll capture every time and frequency information. The shape of five normally used basis operate throughout one scale of the various scales (mother wavelets) is illustrated pictorially in a very quantitative manner:

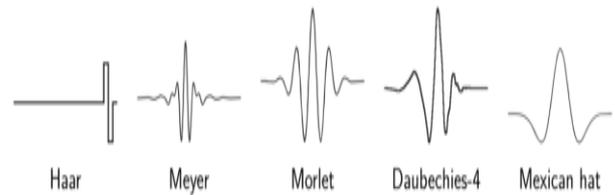


Fig 1: Basis functions in a single scale of many scales (mother wavelets) is illustrated pictorially in a qualitative manner [14]

In DWT, the signal energy concentrates to specific riffle coefficients. This characteristic is useful for compression images[9]. Wavelets convert the image into a series of wavelets that will see on lots more efficiently than pixel blocks.

In our project, DWT is used for steganography purposes. Image is broken into different components and in those very components, only secret message is hidden to minimize suspicion.

III. METHODOLOGY

The proposed scheme is an amalgamation of the work in the fields of cryptography, neural networks, and steganography. In the scheme presented here, the first the encryption of secret message is done before putting it in the cover image thus making the process of hiding a two-phase setup. In the first phase, the secret message is encrypted with the help of artificial neural networks. This encrypted image is then hidden in a cover signal using discrete wavelet transform and

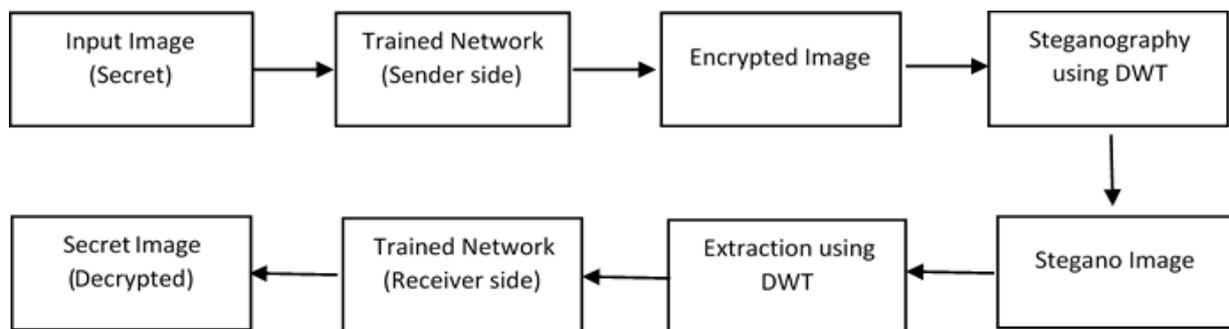


Fig 2: Flowchart of Proposed Methodology

hence completing the steganography phase. All this being done at sender's side, now the message is ready to be delivered over any channel. The reverse process is repeated at the receiver end. Firstly the signal received is separated into cover and an encrypted secret message. Then this encrypted message is decrypted using neural networks and hence we receive our secret message securely. The proposed scheme has the advantage as once the network is trained need to

maintain different keys is dropped etc. Also, no separate medium of communication and hence reduction in suspicion while transmission of the message. Next, the different steps in the scheme are presented.

A. Training

- a. Initialize a neural network with 3 layers: an Input layer, Hidden layer, and Output layer. There are 2 neurons in the input layer, 8 in the hidden layer and 2 in the output layer.
- b. Load the image for training, normalize the data between (0.0 to 1.0) and divide it into a set of 2 pixels so that we can feed each row of our training dataset to the neural network.
- c. Forward-backward propagation is utilized during training the network.

- d. The expected output of each input is the input itself. So, accordingly, we backpropagate the error produced after each input to the network.
- e. We have used the sigmoid function as an activation function between the input layer and hidden layer and linear function between the hidden layer and the output layer.

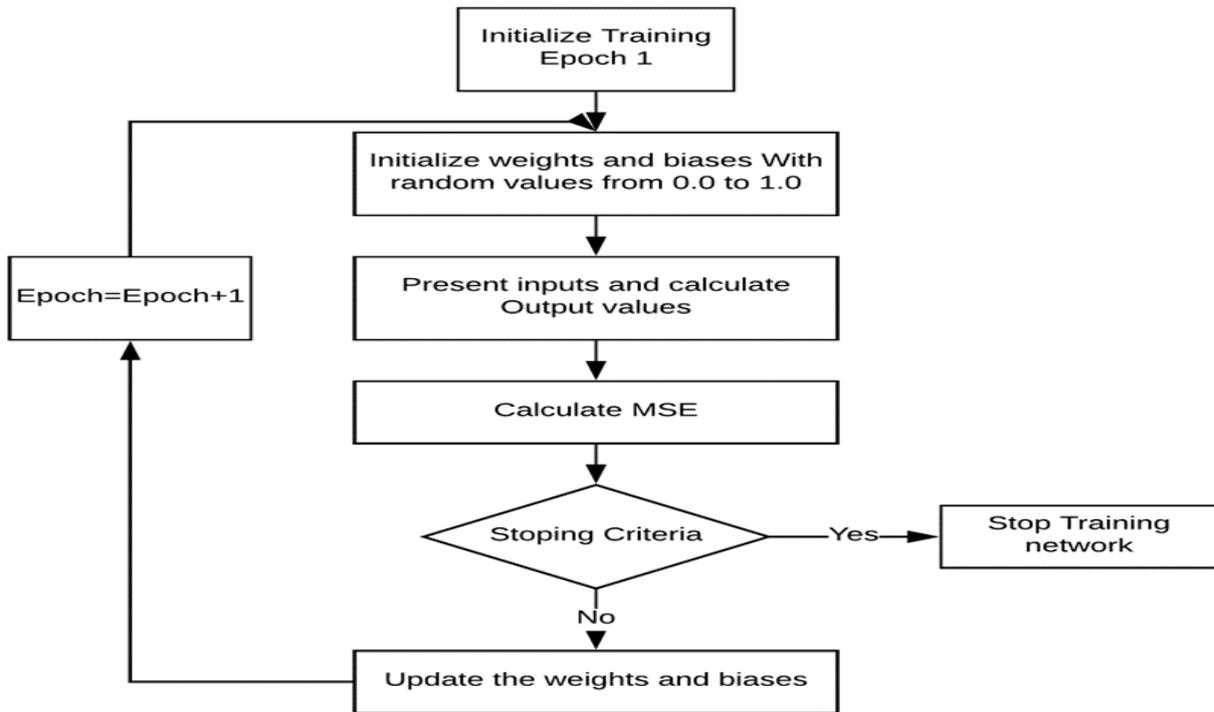


Fig 3: Flowchart of Training Neural Network

- f. After training data for 100 epochs the error graph is:

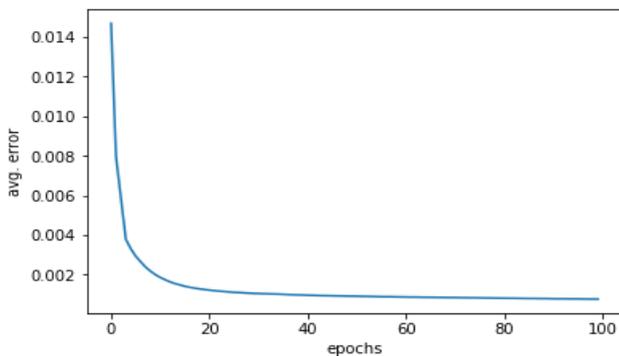


Fig 4: Plot of average errors against epochs during the training of neural network with the 2-8-2 model (2 input neurons - 8 hidden neurons - 2 output neurons)

B. Encryption

- a. Load the secret image, normalize the data between (0.0 to 1.0) and divide it into a set of 2 pixels so that we can feed each row to the network.
- b. Now for encryption, we take the output from the hidden layer instead of the output layer and treat it as the encrypted image.
- c. Since the hidden layer has 8 neurons while input has 2 neurons, the size of the encrypted image is 2 times the size of the original image which can be adjusted by doubling the height and width.

C. Hiding

- a. Steganography is the strategy of concealing a file, message, image, or video within another file, message, image, or video. The advantage of steganography over cryptography alone is that the meant secret message doesn't attract attention to itself as an associate object of scrutiny. Plainly visible encrypted messages, no matter but unbreakable they're, arouse interest and should in themselves be criminatory in countries within which encoding is unlawful.

b. First, we have loaded the cover image in which the encrypted image needs to be hidden. Divide it into three 8-bit images of Red, Green and Blue pixels.
c. We have applied Haar DWT (Discrete Wavelet Transform) in the red component of the cover image. The data is put into the diagonal component of the transformed image by using the first 4 LSBs of each pixel value. Then, the image is transformed back to its red component and all three components are combined back to form the cover image (embedded with encrypted image known as the stegano image).

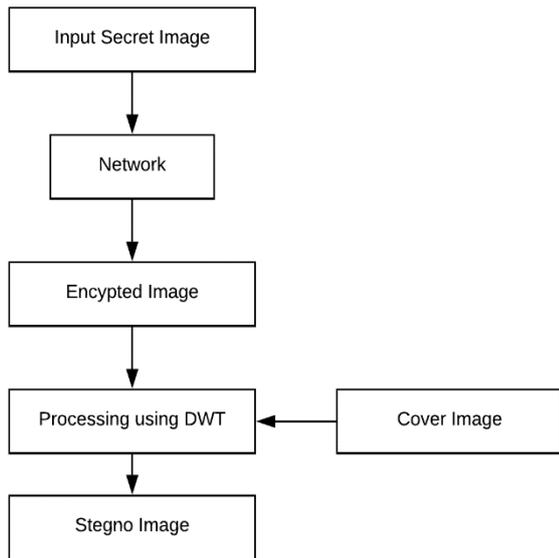


Fig 5: Flowchart of Hiding encrypted image into Cover media

D. Sending

After the secret message is hidden inside cover media, it is then transmitted over any communication channel towards the intended receiver.

E. Separation

The process of embedding of the encrypted image into the cover image is exactly reversed to extract back the encrypted image at the receiver side. Once we get the encrypted image, the process of decryption starts.

F. Decryption

- a. Now, the extracted image is loaded, normalized between (0 to 1) and divided into a set of 8 pixels so that we can feed each row to the hidden layer of the network.
- b. Now for decryption, we take the output from the output layer and recover the encrypted image
- c. Since the hidden layer has 8 neurons while the output layer has 2 neurons, the size of the decrypted image is 1/4 times the size of the encrypted image but is equal to the original image.

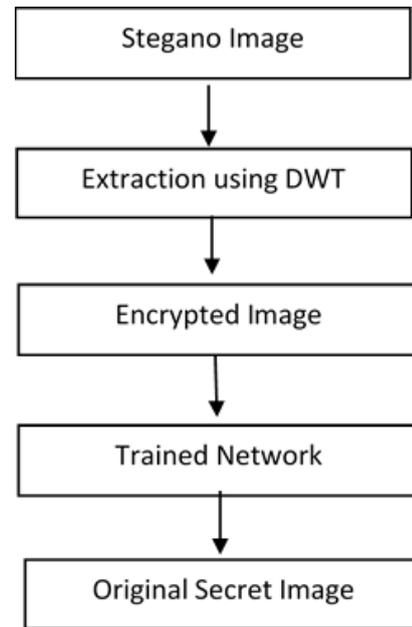


Fig 6: Flowchart of Decrypting message obtained after separating cover media and encrypted message.

IV. EXPERIMENTAL RESULTS

During our experimental work, we reached the following results regarding the different configuration of neural networks and which neural network to seems fit to utilize. Also, there are complete sets of data used throughout the process.

The various error graphs on creating ANNs with different number of input, hidden and output layers as (input-hidden-output) are as follows –

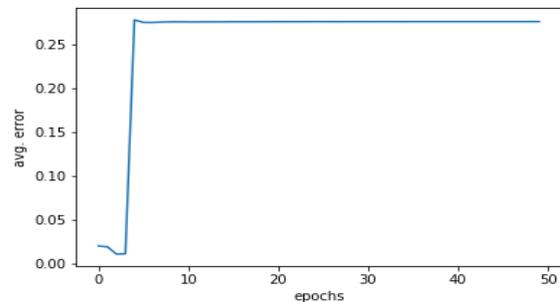


Fig 7:Plot of average errors against epochs during the training of neural network with 2-2-2 architecture. (2 input neurons - 2 hidden neurons - 2 output neurons)

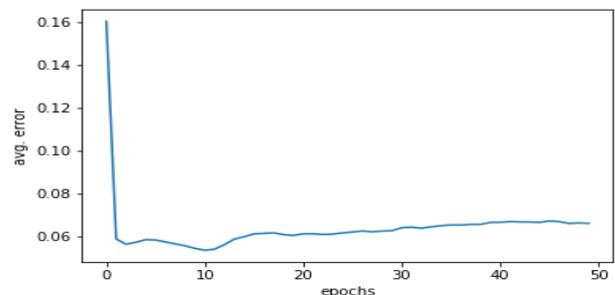


Fig 8:Plot of average errors against epochs during the training of neural network with 4-4-4 architecture (4 input neurons - 4 hidden neurons - 4 output neurons)



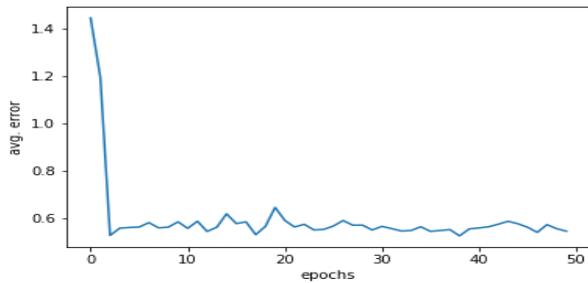


Fig 9: Plot of average errors against epochs during the training of neural network with 8-8-8 architecture (8 input neurons - 8 hidden neurons - 8 output neurons)

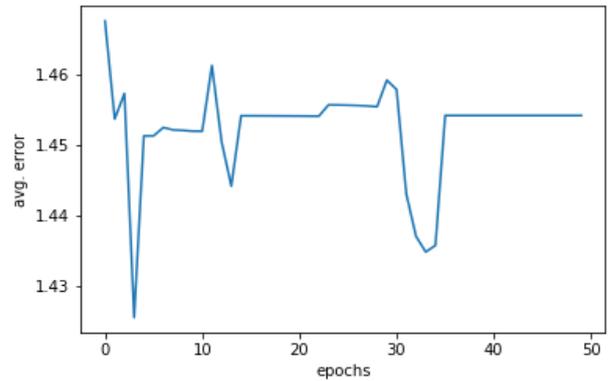


Fig 13: Plot of average errors against epochs during the training of neural network with 16-4-16 architecture (16 input neurons - 4 hidden neurons - 16 output neurons)

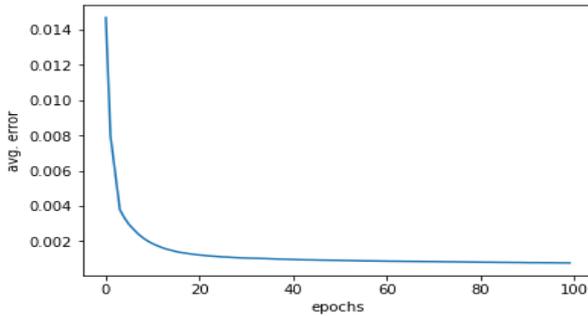


Fig 10: Plot of average errors against epochs during the training of neural network with 2-8-2 architecture (2 input neurons - 8 hidden neurons - 2 output neurons)

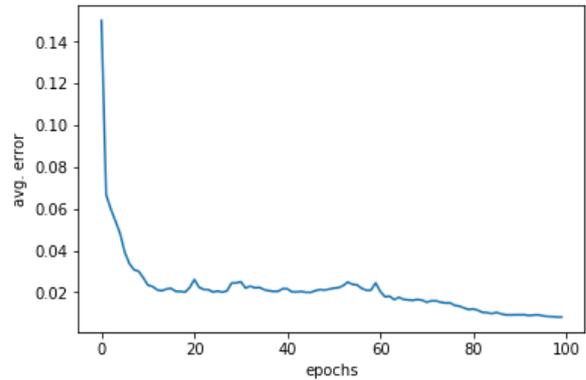


Fig 14: Plot of average errors against epochs during the training of neural network with 4-16-4 architecture (4 input neurons - 16 hidden neurons - 4 output neurons)

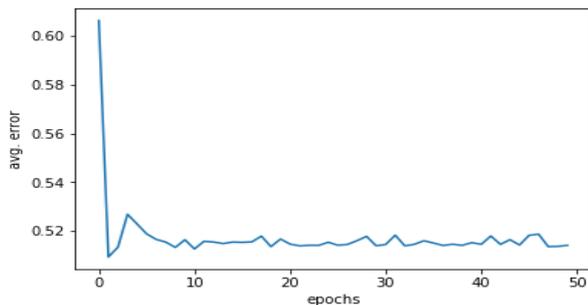


Fig 11: Plot of average errors against epochs during the training of neural network with 8-2-8 architecture (8 input neurons - 2 hidden neurons - 8 output neurons)

After analyzing all the models, the model with 2-8-2 Architecture shows the lowest error rate and hence been chosen as our model to encrypt and decrypt the secret image.

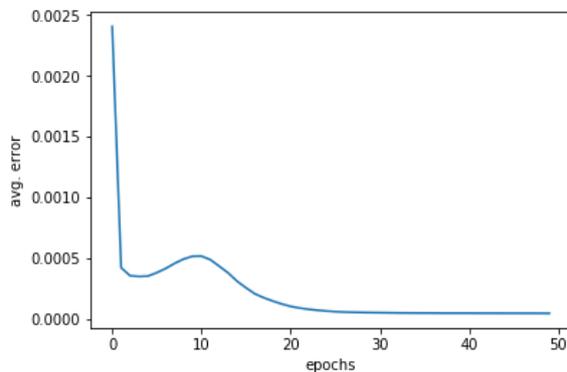


Fig 12: Plot of average errors against epochs during the training of neural network with 1-4-1 architecture (1 input neurons - 4 hidden neurons - 1 output neurons)



Encryption-Decryption of some test images is given by figure 15:

The following figure provides pictures at different stages of the project. Input image, here a secret message which when passed through network produces an encrypted image. This encrypted image is then hidden into cover media to form

stegano image which is transmitted over any communication network. Once received, encrypted image is separated from the cover image and then processed through the network to get the original input secret image.

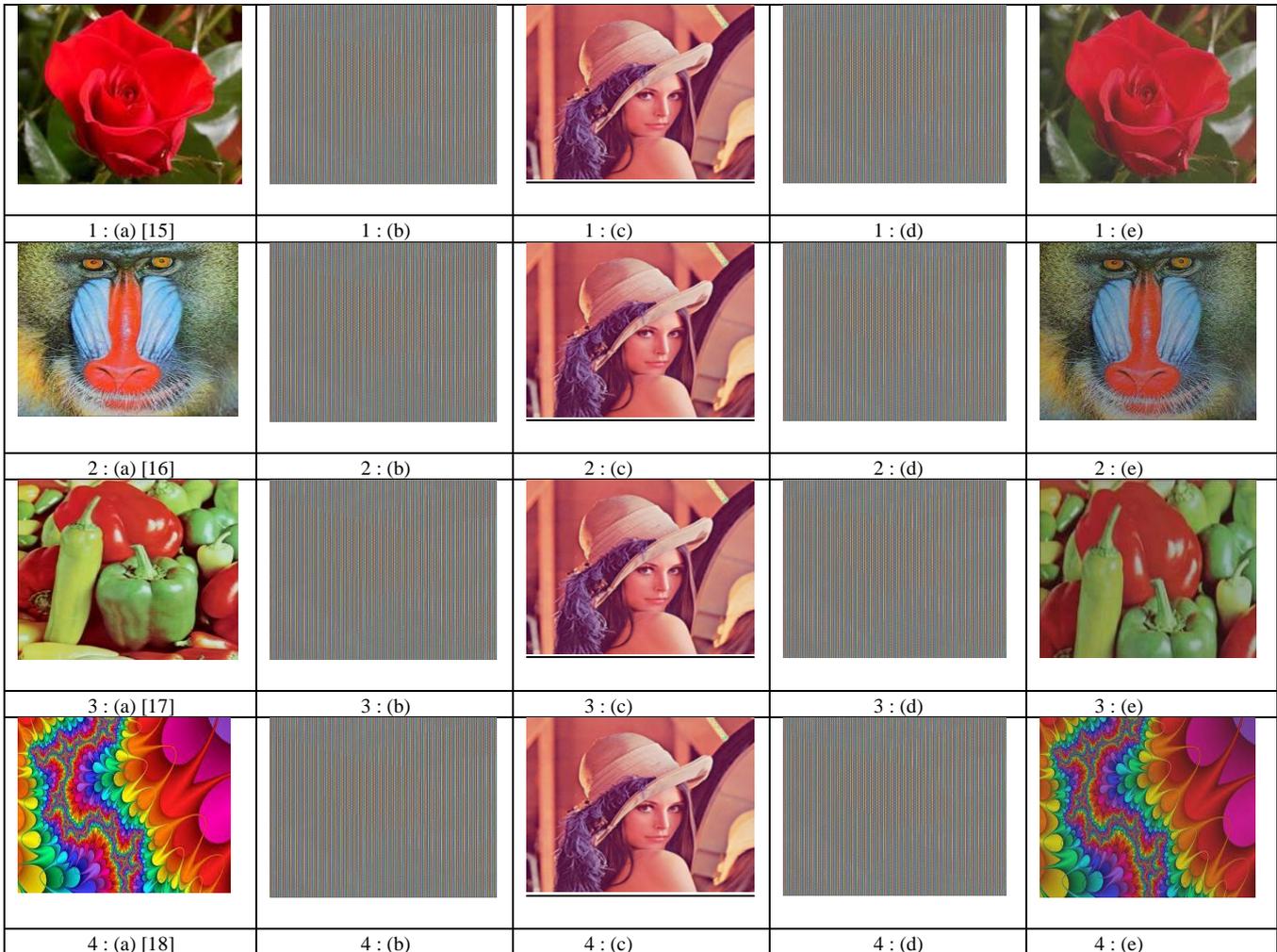


Fig 15:Results for test images (1-4) where (a) is the original secret image; (b) is the encrypted image obtained from neural network; (c) is the stegano image resulting from cover image [19] and encrypted image ; (d) is the encrypted image received after separating it from cover image; (e) is the decrypted image obtained using neural network.

V. CONCLUSION

This paper projects an interface utilizing the Discrete Wavelet Transform for hiding and Neural Networks for Encryption. We contemplated distinctive methodologies of coordinating cryptography and neural systems towards the normal target of a quicker and productive method for encryption and decryption. Information concealing utilizing steganography models radically drops odds of doubt. Joining these two modules results in an interface which can be utilized to uphold secret information exchange on a computerized medium. For example, this can be utilized to conceal data in a music/sound file or in a video record. An only approved individual has proficient system interface to decode a secret message. One of the main advantages of the method is that it does not require the original carrier file i.e. unedited host signal is not needed during the retrieval stage. Research points out that DWT-based schemes serve good imperceptibility and an improved payload. Also, it can stand

against different alterations and attacks proving good on robustness scale. In nutshell, it's suitable for information transfer requiring less attention and suspicion from unauthorized entities by utilizing public means of communication rather than a private line. Also at the same secure enough so that no one from public means can retrieve sensitive information or even suspect about its presence. Its further augmentation, for an instance, can be, when an unapproved client plays the document or alters the record it records the movement. The future work which can be done but is not only limited to improve efficiency on these existing methods by introducing more efficient techniques regarding different types of images and network structure, analyzing different types of attacks like Compression attack, Pixel Tampering and apply them on our model to check its robustness and reliability, make a real-time application using this model on image and video encryption.



REFERENCES

1. A. Al-Gindy, A. M. Zorrilla, and B. Beyrouti, "DCT watermarking technique using image normalization," in Proc. 2015 Int. Conf. Develop. E- Syst. Eng., 2015, pp. 145–149.
2. C. Namratha and S. Kareemulla, "Multi-image watermarking using Lagrangian support vector regression," in Proc. IEEE Int. Conf. Recent Trends Electron., Inf., Commun. Technol., 2016, pp. 513–516.
3. H. Sadreazami, M. O. Ahmad, and M. Swamy, "Multiplicative watermark decoder in contourlet domain using the normal inverse Gaussian distribution," IEEE Trans. Multimedia, vol. 18, no. 2, pp. 196–207, Feb. 2016.
4. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. San Mateo, CA, USA: Morgan Kaufmann, 2007.
5. T. Chen and H. Lu, "Robust spatial LSB watermarking of color images against JPEG compression," in Proc. 2012 IEEE 5th Int. Conf. Adv. Comput. Intell., 2012, pp. 872–875.
6. C.-M. Pun, "A novel DFT-based digital watermarking system for images," in Proc. 2006 8th Int. Conf. Signal Process., vol. 2, pp. 16–20, 2006.
7. T. K. Das, S. Maitra, and J. Zhou, "Cryptanalysis of Chu's DCT based watermarking scheme," IEEE Trans. Multimedia, vol. 8, no. 3, pp. 629–632, Jun. 2006.
8. G. Tianming and W. Yanjie, "DWT-based digital image watermarking algorithm," in Proc. 2011 10th Int. Conf. Electron. Meas. Instrum., vol. 3, 2011, pp. 163–166.
9. S. R. Chalamala, K. R. Kakkirala, and R. G. B. Mallikarjuna, "Analysis of wavelet and contourlet transform based image watermarking techniques," in Proc. 2014 IEEE Int. Adv. Comput. Conf., 2014, pp. 1122–1126.
10. L. Ghouti, A. Bouridane, M. K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets," IEEE Trans. Signal Process., vol. 54, no. 4, pp. 1519–1536, Apr. 2006.
11. J. Ruanaidh, W. Dowling, and F. M. Boland, "Phase watermarking of digital images," in Proc. Int. Conf. Image Process., vol. 3, 1996, pp. 239–242.
12. J. Zou, X. Yang, and S. Niu, "A novel robust watermarking method for certificates based on DFT and Hough transforms," in Proc. 2010 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process., 2010, pp. 438–441.
13. S. Zaboli and M. S. Moin, "CEW: A non-blind adaptive image watermarking approach based on entropy in contourlet domain," in Proc. 2007 IEEE Int. Symp. Ind. Electron., 2007, pp. 1687–1692.
14. Czech Technical University, online at http://people.ciirc.cvut.cz/~hlavac/TeachPresEn/11ImageProc/14WayeletsEn.pdf?fbclid=IwAR11MI1f5xHSQBgnuGm6Tq3_azUu9pd76uzG4n5eTpcquAWBSsKjgO0vUzU. Accessed on April 20, 2019.
15. AForge.NET, online at http://www.aforgenet.com/framework/docs/html/img/imaging/sample_1.jpg. Accessed on April 20, 2019.
16. COMPUTER-AIDED ENGINEERING, online at <https://homepages.cae.wisc.edu/~ece533/images/baboon.png>. Accessed on April 20, 2019.
17. COMPUTER-AIDED ENGINEERING, online at <https://homepages.cae.wisc.edu/~ece533/images/peppers.png>. Accessed on April 20, 2019.
18. Genchi Wallpapers, online at http://genchi.info/image/abstract-color-wallpaper-28.jpg?fbclid=IwAR3tp3IzcdRm3GjltNAzCD_rYooQQPdjN0RaSXtUdqsbafXlO2WsMQs0ts. Accessed on April 20, 2019.
19. COMPUTER-AIDED ENGINEERING, online at <https://homepages.cae.wisc.edu/~ece533/images/lena.png>. Accessed on April 20, 2019.

AUTHORS PROFILE



Shivank Tiwari is a final year undergraduate in the Department of CSE&IT at Jaypee Institute of Information Technology (JIIT), Noida. He is National Talent Scholar (NTSE – conducted by Ministry of Human Resource Development, Government of India) and also won in other Olympiads, talent search examinations, etc. Chose to further his interest in research, he will be joining Arizona State University for Fall 2019 term in the United States. His current interests include cybersecurity, artificial intelligence, and finance.



Nipun Mittal is a final year undergraduate in the Department of CSE&IT at Jaypee Institute of Information Technology (JIIT), Noida. He is joining IIT Bombay for his master's degree. He has been qualified for the regionals of the Association for Computing Machinery - International Collegiate Programming Contest (ACM-ICPC). His current interests include neural cryptography and theoretical computer science.



Nupur Garg is a final year undergraduate in the Department of CSE&IT at Jaypee Institute of Information Technology (JIIT), Noida. She topped the International Mathematical Olympiad at a regional level. She started her professional career as Software engineer in PlaySimple Games. Her current work includes mobile game design and development.

Tribhuvan Kumar Tewari is currently working as an Assistant Professor



(Senior Grade) in the Department of CSE&IT at Jaypee Institute of Information Technology (JIIT), Noida. He has completed his Ph.D. in 2015 and his M.Tech. from Jaypee Institute of Information Technology, Noida, Uttar Pradesh (U.P), India. His research interest includes image processing, audio processing, graph algorithms, and machine learning.



Manish K Thakur is currently working as Associate Professor in the Department of CSE&IT at Jaypee Institute of Information Technology (JIIT) Noida. He completed his Ph.D. in 2014 from JIIT, Noida and his M.Tech in Computer Science from Birla Institute of Technology, Mesra, Ranchi India. His research interest includes evolutionary algorithms, graph algorithms, parallel and distributed computing, videoprocessing, and machine learning.