iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44967

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

An Approach of Deep Learning Neural Network Model for Image Security

Dr. Madhu B.[1], Manish Thapa[2], Bishal Rauniyar[3], Nitish Chaudhary[4], Kishan Kandu[5]
[1]*Assitant Professor, Department of Computer Science and Engineering, Dr. AIT, Bangalore, India*
[2, 3, 4, 5]*Student, Department of Computer Science and Engineering, Dr. AIT, Bangalore, India*

Abstract: ***Securing the Image and video data have applications in various fields like internet communication, multimedia systems, medical imaging, Telemedicine, and military communication. Watermarking protects digital intellectual property. It helps to prove the origin of an image and discourages unaccredited copies or distribution. The proposed method uses the concept of binding a secret message within another, ordinary, message. Our algorithm is used to unobtrusively hide a small message within the noisy regions of a larger image. Deep neural networks are simultaneously trained to create the hiding and revealing processes and are designed to specifically work as a pair. Different models are implemented to check the performance of the algorithm. The results are evaluated using 40,000 different types of images. With the state of art techniques like hiding the image in the least significant bits of the carrier image, our approach compresses and distributes the secret image's representation across all of the available bits.***

Keywords: Image Hiding Techniques, Digital Image, Steganography, Encoder and Decoder, CNN.

I. INTRODUCTION

Nowadays, the network plays an important role in people's life where we can share text, images, and many more. While sharing images or data, we find security issues and these issues cause problems to the people like unauthorized people can misuse the images or data. So, to deal with these problems what we do is hide the images, or data and that hidden images or data will be transferred to the receiver end. The main goal of this paper is to hide the image while transferring it from sender to receiver. Many techniques provide security to the images or data like copyright protection, secret transmission, and watermarks. In this paper, the sender uses this algorithm to hide the secret images in the cover images. At the receiver end, the receiver receives the hidden images and uses a decoding algorithm to view the secret images or to remove the cover images. This paper helps to minimize the noises in the cover images. Figure.1 indicates the architecture of the proposed system. The input image is a dog image and the secret image is a flower image. The proposed method hides the secret image in the original image to give watermarked image as output.

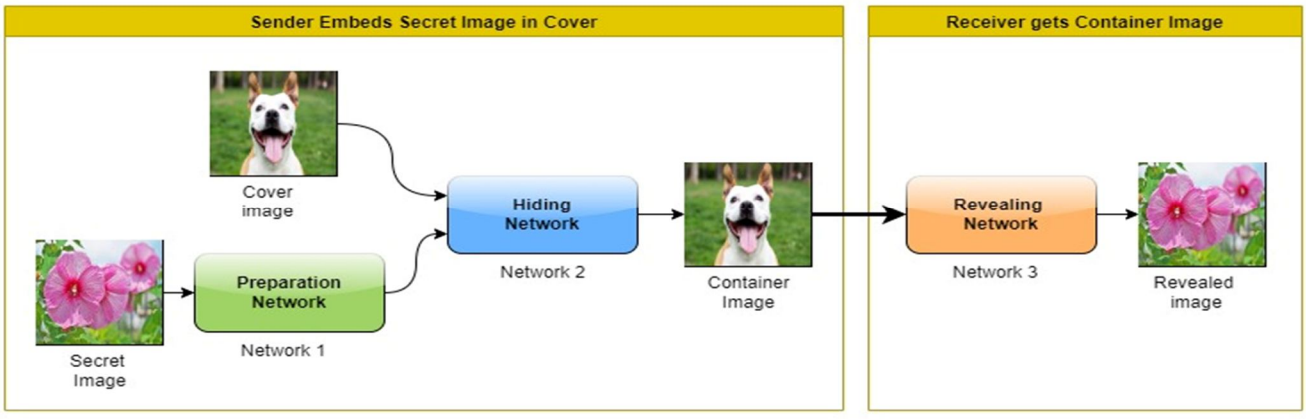


Figure 1: The three components of the full system.

The left one is secret-image preparation. Center one is hiding the image in the cover image. The right one is uncovering the hidden image with the revealed network. This is trained simultaneously but is used by the receiver The challenge of this project is that while decoding the image, it might be lost some data. The amount of lost data is depending upon two factors. One is the amount of data that is to be hidden. The second one is that the amount of lost data depends on the carrier image itself.

II. EXISTING SYSTEM

There are numerous ways that help to give security to the images, and data in which some of them are Images Encryption, Digital Watermarks, Copyright Protection, Secret Transmission, and numerous further. Image encryption substantially focuses on the creative idea of taking successive or arbitrary pixel bits of an image, acting inclusively and modified with sense creating a complete set of new pixels, distinct from the original bits. In this system, a new and more optimized way of image encryption is introduced. During the first step, the secret gray image is combined using the run of high figures and pseudorandom generator, therefore, increasing the difficulty of the algorithm. To make it more complex to obtain. To increase security, intensity values are suited. This provides better robustness in this system.

Disadvantages are

1) Time-consuming and threat.
2) Image losing and lower correlation.
3) Perplexed and lengthy process because there is a lot of analysis done in a single fashion.

The hidden message bits are fixed into each color pixel sequentially by the pixel-value differencing (PVD) technique. This technique implements two consecutive non-overlapping factors; as a result, to embed the hidden message bits into a color pixel(i.e. consists of red, green, and blue) the straightforward conventional PVD is not applicable. Hence, in this scheme, at first, the three-color factors are represented in two overlapping blocks like the mixture of red and green color factors in which another one is the mixture of green and blue color factors respectively. After the first step, the PVD method is deployed on each block independently to embed the hidden data. And the two overlapping blocks are reconciled to gain the optimized three-color factors. The concept of overlapping blocks has improved the embedding capacity of the cover image. These sets of color images have been examined based on the above scheme and decent results have been achieved in
terms of embedding capacity and upholding the acceptable visual quality of the output image.

III. LITERATURE SURVEY

Jadhav and Shashikala Channalli, [1] presented a novel method of steganography called online information concealment on the instrument's output screens. This technique can be used to broadcast a secret message in a public setting. It can be expanded to include other channels like electronic billboards outside sporting venues, train stations, and airports. This steganographic technique is quite similar to video and image steganography. Here, the secret information is hidden using a private marking scheme that combines the LSB and symmetric key steganography techniques.

Po-Yueh Chen and Wei-En, [2] Wu proposed an image steganography strategy to improve on the side match method proposed by Chang et al. in 2004. The quality of the image is increased while keeping the embedding capacity the same by hiding additional information in the edge regions. This benefit arises from the fact that the human eye rarely detects insignificant variations in the edge regions. The embedding capacity can be altered to meet the needs of different users. In addition to enhancing image quality, the suggested method also offers decent security.

A. Nag, S. Biswas, D. Sarkar, and P.P. Sarkar, [3] introduced a unique method for picture steganography based on Block-DCT, in which DCT is utilized to convert original image (cover image) blocks from the spatial to the frequency domain. Before performing a two-dimensional discrete cosine transform on each of the P = MN / 64 blocks, a grey level image of size M x N is first divided into no joint 8 x 8 blocks. Then, prior to embedding, Huffman encoding is also applied to the secret messages/images, and each bit of the encoded secret message/image is placed in the frequency domain by modifying the least significant bit of each DCT coefficient of the blocks of the cover picture. The experimental findings demonstrate the algorithm's high capacity.

S. S. Askar, A. A. Karawia, and A. Alshamrani, [4] introduced a new algorithm for image encryption and decryption based on a chaotic economic map. This work represents the first attempt to incorporate a chaotic economic map into the development of chaotic cryptography. The proposed image encryption and decryption technique has a very wide keyspace of 1084, strong sensitivity to all secret keys, close to-ideal information entropy of 8, low correlation coefficients that are close to the ideal value of 0, and all of these characteristics have been demonstrated by simulations and experimental findings. In light of these findings, the suggested image algorithm is effective and reliable. Additionally, the outcomes support the application.

K.Brindha, R. Sharma, and S. Saini, [5] demonstrated picture encryption using the DES algorithm, which increases security during transmission. The suggested solution replicates the original image without sacrificing any information. They employed three different techniques: The image is first transformed into a byte array, and then the byte array is transformed into a string and sent for

DES encryption. The input image remains unchanged in the final encrypted version. The comparison study of DES and AES has been discussed. The encryption of text data included in photographs is a future project for them.

A. Jain, and N. Rajpal, [6] proposed employing DNA (Deoxyribonucleic acid) operations and chaotic maps to encrypt images. First, the input image is DNA encoded, and then a mask is created using the 1D chaotic map. Second, this mask is combined with the DNA-encoded image using DNA addition. A complement matrix created by two 1D chaotic maps serves as the intermediate product, which is DNA that has been complementary. In order to obtain the cypher image, the resultant matrix is then permuted using 2D chaotic maps and DNA decoding. The suggested method can withstand well-known statistical, differential, and plain text attacks and is invertible.

Q. A. Keste, [7] describes a method for transposing and reshuffling the RGB values of an image in phases that has been shown to be effective in terms of security analysis. After RGB component shifting, additional RGB value swapping in the image file strengthened the security of the image against all currently feasible assaults.

W. Zhu, [8] suggested an interesting method for picture discretization that makes use of Cat mapping. To achieve image encryption, the suggested method makes periodic adjustments. The encryption process for images of various sizes may employ various cycles. The trials demonstrate that the encryption approach may successfully encrypt images by selecting the ideal settings to get the best picture encryption result. According to the sensitivity analysis, this approach should work well for replacing and scrambling image pixels. This method's significant sensitivity to plaintext for encrypted security may be a factor in how well it handles varied plaintext attack scenarios.

S. Kaur, [9] presented a safe encryption method for digital pictures; it works with any digital file (e.g. text, image, audio, etc.). A block of secret bytes was ciphered using bit-wise XORing and shifting, and after that, the ciphered bytes were shuffled N times (N is the size of the secret key). Utilizing dynamic SBOX and TBOX, this methodology combines substitution and transposition methods. It offers superior protection against brute-force assaults because the key for the proposed cryptosystem is quite large. Additionally, the suggested algorithm's high acceptability is demonstrated by critical sensitivity analysis, statistical analysis, and differential attack analysis.

Y.-Q. Zhang, and X.-Y. Wang, [10] suggested a new image encryption technique based on spatiotemporal nonadjacent linked map lattices. In terms of dynamics, the system of non-adjacent coupled map lattices exhibits more remarkable cryptographic properties than either the logistic map or coupled map lattices. They used a bit-level pixel permutation technique for the proposed image encryption, which allows bit planes of pixels to permute one another without requiring additional storage space. The results of simulations show that the suggested algorithm is more efficient and secure than other techniques.

A. Devi, A. Sharma, and A. Rangra, [11] discussed and surveyed the image encryption and decryption algorithms DES, AES, and Blowfish. In today's environment, it is critical to use effective encryption and decryption when transmitting images from one network to another via the internet to avoid illegal access. The authors also reviewed associated studies, identified several issues, and offered recommendations that could be helpful for image encryption. This will speed up the image's performance, encryption, and decryption timings.

G.S. Chandel, and Pragna Patel, [12] examined various methods for encrypting and decrypting images. According to their research, the writers were able to identify the problem formulation and analyse it, which allowed them to offer recommendations for future improvement. The following future directions, which can aid in better identification, were offered based on the study: 1) Make use of strong encryption methods like DES and RSA. 2) To increase image security, increase the randomization of the RGB and security keys. 3) 3) Enhance the block size or bit encryption standard, such as 128 bit and 256 bit. 4) The use of hybridization is a superior option because chaos-based cyphers shouldn't be vulnerable to conventional differential and linear cryptanalysis techniques.

Pia Singh, and Prof. Karamjeet Singh, [13] suggested picture encryption and decryption using a secret-key block cypher dubbed 64-bits Blowfish, which was aimed to improve security and performance. This technique is used with keys up to 448 bits in size. It uses a 16-time Feistel network iteration of a straightforward function. The blowfish method runs quicker than the widely used current algorithms and is secure from unwanted assault. MATLAB is used to create and implement the suggested algorithm. As a result, the blowfish algorithm grows more powerful as the number of rounds increases. Blowfish can be regarded as a top-notch common encryption algorithm because it currently has no known security vulnerabilities.

K.K.R.Saraf, V.P.Jagtap, and, A.K.Mishra, [14] used AES to encode and decrypt text and images. characteristics of data according on its types. As a result, not all forms of data can be encrypted using the same method. A comparable strategy cannot be used to secure both text and photos against unwanted access if the images have a big data size and issues with real-time constraints. Images and text can both be protected using a few different variants of the AES protocol.

R. Pakshwar, V. K. Trivedi, and V. Richhariya, [15] conducted a review of over 25 research publications addressing picture encryption approaches that scramble the image's pixels and lessen the association between them, thereby producing the encrypted image. This article provided a survey of the various image encryption and decryption methods currently in use. The research also concentrated on how Image encryption and decryption algorithms work.
statistical attacks, and differential attacks.
In this proposed method the thing which sets us apart from so far known methods and techniques is that here the secret image is concealed inside the noises of a cover image with the help of three networks. The three networks are the Preparation network, the hiding network, and the Revealing network. Here various learning rates, a large number of epochs, and activation functions like relu, tanh, selu, etc are used for optimizing the results.

IV. PROPOSED SYSTEM

The system consists of three networks i.e., preparation network, hiding network, and reveal network which helps in both hiding and revealing images.

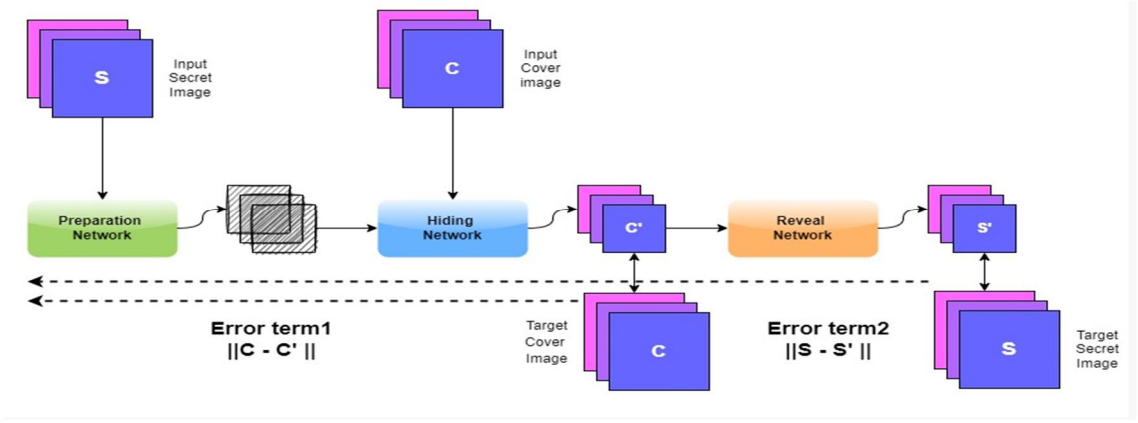


Figure 2: The architecture of the network

A. Preparation Network

This network develops the secret image to be hidden and serves two aims. First, when the hidden image (size M × M) is smaller than the cover image (N × N), the preparation network gradually increases the size of the hidden image to the size of the cover, by distributing the hidden image bit's across the entire N × N Pixels. (For space reasons, this network does not provide details of experiments with smaller images, and instead concentrates on full-size images). And the more crucial aim relevant to all sizes of hidden images is to convert the color-based pixels into more useful features (such as edges) for succinctly encrypting the image.

B. Hiding Network

It is close to the preparation network defined above but includes an extra Conv2D sequential layer for connecting Gaussian noise to the cover. Here, the hidden information is allowed to be encrypted in bits other than the LSB of the cover image. It takes the output from Preparation-Network as input and the cover image and creates the Container image. And the input taken in this network consists of N * N pixel field, with depth concatenated RGB channels of the cover image and the transformed channels of the hidden image. For a more detailed study of this network, over 30 architectures were attempted with a varying number of hidden layers and convolution sizes; the best suited contains 5 convolution layers that had 50 filters each of {3 × 3, 4 × 4, 5 × 5} patches.

C. Revealing Network

This network is used by the receiver end and only takes the images from the container images neither from the cover images nor hidden images. It helps to decode the container images and to reveal the hidden images by removing the cover images from the container images. Loss Function is the function that examines how much data are lost while moving the
images. Reconstruction loss of cover image and hidden image are the two error terms that are contained by the loss function
L (c, c0, s, s0) = ||c − c0|| + β||s − s0|| Here, c and c0 represents original and reconstructed cover images and s and s0 represents original and reconstructed hidden images. And beta is a hyperparameter that controls how much of the hidden should be reconstructed.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

V. DEEP LEARNING ARCHITECTURE

Deep learning is part of machine learning and machine learning the part of artificial intelligence. Artificial intelligence is a technique that allows a machine to copy human actions. Machine learning is a technique that helps to achieve Artificial intelligence through algorithms trained with data and finally, deep learning is a type of machine learning caused by the structure of the human brain. Regarding deep learning, this system is called an artificial neural network. Let's understand deep learning better and how it's different from machine learning. Say, we create a machine that could differentiate between tomatoes and cherries if done using the machine we'd have to tell the machine the features based on which the two can be differentiated these features could be the size and the types of stems on them. Deep learning on the other hand the features are picked out by the neural network human intervention. Indeed, this kind of independence comes at the fetch of having a big volume of data to train our machines. Let's dive into the working of neural networks. Say there are three students and each of them down the digit nine on a piece of paper notably they don't all write it identically the human brain can easily understand the digits but what if a computer had to understand them that is where deep learning comes in. Here's a neural network trained to identify handwritten digits each number is present as an image of 28 times 28 pixels. Now that amount to a total of 784 pixels neurons the core entity of a neural network is where the information processing takes place each of the 784 pixels is fed to a neural in the first layer of our neural network. This forms an input layer on the other end we have the output layer with each neuron representing a digit with the hidden layer existing between them. The information is moved from one layer to another layer over connecting channels. Every one of them has a value attached to it and hence is called a weighted channel. All neurons have a special number linked with it called bias. This bias is added to the weighted sum of inputs reaching the neuron which is then applied to a function known as the activation function. The result of activation determines if the neuron gets activated. Every trigger neuron passes on information to the following layers this continues up till the second last layer the one neuron trigger in the output layer corresponds to the input digit the weights and bias are constantly balanced to produce a well-trained network. Deep learning is used in customer support, medical care, self-driving cars, and many more. Deep learning has a huge scope but also it has some limitations. The first we discussed earlier is data while deep learning is the most efficient way to deal with unstructured data a neural network requires a massive volume of data to train. Let's assume we always have access to the necessary amount of data processing this is not within the capability of every machine and that brings us to our second limitation. Computational power training and neural network requires graphical processing units which have thousands of course as compared to CPUs and GPUs are more expensive finally, we come down to training time deep neural networks take hours or even months to train the time increase with the amount of data and number of layers in the network.

A. Supervised Deep Learning

Supervised learning refers to a problem area where written references are labeled within the data used for training. In this section, we introduce a higher level of well-known deep learning structures - convolutional neural networks and duplicate neural networks, and more.

1) *Convolutional Neural Networks:* It is also known as CNN or comp net is also the artificial neural network that is so far been most popularly used for analyzing images although analysis had been the most widespread use of CNN. It can also be used for other data inquiries or to organize problems as well. Most generally we can think of CNN as an artificial neural network that has some type of specialization for being able to pick out or detect patterns and make sense of them. This pattern detection shows that CNN is an important technology and very useful for image analysis. So, if a CNN is just some form of an artificial neural network what differentiates it from just a standard multi-layer perceptron or MLP or CNN has hidden layers called convolutional layers. These layers are exactly what makes a CNN. Just like any other layer a convolutional layer receives input then transforms and then outputs the transform input to the next layer with a convolutional layer this transformation is a convolution operation.

Sample requests: Image recognition, video analysis, and natural language processing

2) *Recurrent Neural Networks***:** Recurrent Neural Networks are neural networks that are good at modeling sequence data. Let's say, you take a snapshot of a ball moving in time. Let's also say you want to predict the direction that which the ball moving. How would you do this well you can go ahead and take a guess but any answer you come up with would be a random guess without knowledge of where the ball has been you weren't having an update to predict where it's going. If you record many snapshots of the positions of the balls in succession you will have enough information to make better predictions so this is a sequence a particular in which one thing comes after another with this information. You can know that the ball is moving in the right sequence data comes in many forms' audio is the natural sequence, and text can also be sequence data.

Example request: Speech recognition and handwriting recognition

B. Unsupervised Deep Learning

In unsupervised learning each piece of data passed to our model during training is solely an unlabeled input object or sample there is no corresponding label that's paired with the sample but if the data isn't labeled then how is the model learning, how is it evaluating itself to understand how well it's performing well first let's go ahead and touch on the fact that with unsupervised. Since the model is unaware of the training data there's no way for it to measure its accuracy. So, accuracy is not a metric that we analyzed with unsupervised learning now essentially with unsupervised learning the model is going to be given the unlabeled data set and it's going to try to learn some type of structure from the data and will take out the helpful information or features from it. It is going to be learning how to create a mapping from given inputs to particular outputs based on what it's learning about the structure of this data without any labels let's make this idea solid with some examples of one of the most popular applications of unsupervised learning is through the use of clustering algorithms. Let's say we have height and weight data for a particular age group of males and females but we don't have the labels for this data so any given sample form of this data would just be a tuple consisting of one person's height and weight but there would be no associated label telling us whether this person was a male or females. Now clustering algorithms analyze this data and start to learn the structure of it even though it's not labeled through learning the structure it can start to cluster the data into groups.

1) *Self-Organizing Maps:* Dr. Teuvo Kohonen developed self-mapping (SOM) in 1982. It was widely known as the Kohonen map. It uses an unsupervised learning approach to produce low-dimensional, discretized, and helps to train its network through a competitive learning algorithm. It also helps to maintain the structural information from the training data. Reduction of dimensionality and grid clustering are the techniques that help to interpret and understand the data. *Application example: Size reduction, high-dimensional input to2-dimensional output, bright range effect, and group visibility*
2) *Autoencoders:* Autoencoders are simple learning networks that help to move inputs into outputs with less possible error. This means that we want the output to be close to the input as possible. An autoencoder neural network is basically an unsupervised machine learning algorithm that applies backpropagation setting the target values to be equal to the inputs. It is an unsupervised ML algorithm similar to the PCA. It reduces the same objective function as PCA.

Sample requests: Reduction, data consolidation, and data compression/decompression

C. Restricted Boltzmann Machines

It is a probabilistic graphical model for unsupervised learning that is used to discover hidden structures in data. Video recommendation system is the perfect application for this. Restricted Boltzmann Machines (RBM) is made up of two parts i.e., a visible layer that contains some nodes and a hidden layer that also contains some nodes. Now every node in the visible layer is connected to every node in the hidden layer. The restricted part here comes about because no node is connected to any other node in the same layer. Now all of these nodes are connected by edges that have something called weights associated with them and the weights represent the probability of being active. Now to train the network, we need to provide multiple inputs. The nodes in the visible layer, they'll receive the training data. This multiple by the weights and added to a bias value at the hidden layer. This is the first phase of an RBM and it's called the Feed Forward Pass and the second phase is the Feed Forward Pass.

Application Example: Reducing the size and shared filtering.

VI. ARCHITECTURAL DESIGN

The main purpose is to simplify the complete task of hiding as well as revealing the hidden image. This network design model contains three parts i.e., Preparation-Network, Hiding-Network, and Revealed-Network. Here, we will gather these three parts collectively to form an end-to-end system for hiding as well as revealing the secret image.

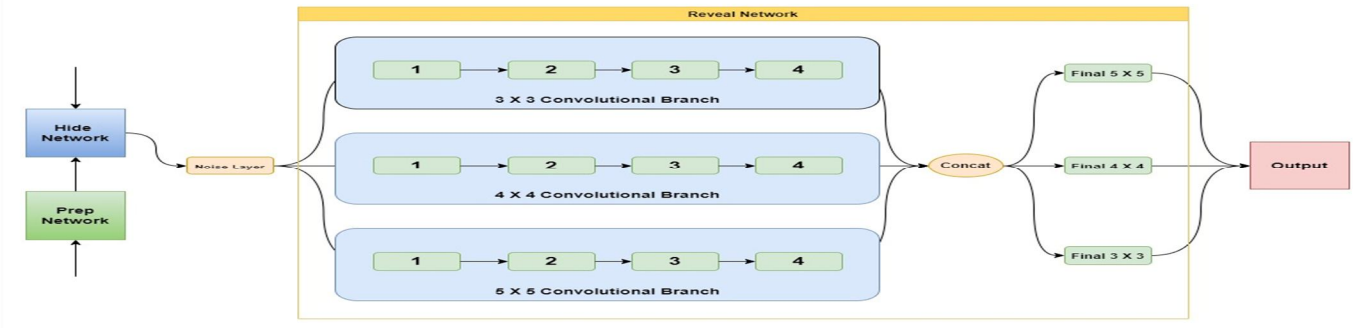


Figure 3: Architectural Design

1) *Noise Layer:* During the training of a neural network model, the addition of noise has a regularization effect and in turn, optimizes the robustness of the model. It has been shown to have an analogous impact on the loss function as the addition of a penalty term, as well as in the case of weight regularization methods. The size of training datasets can be increased by adding noise. A training sample is exposed to the model each time when arbitrary noise is added to the input variables making them different every time it gets exposed to the model. In this way, a simple form of data augmentation can be done by adding noise to input samples.
2) *Conv2D Layer*: Conv2D Layer is a library of Keras and implements a convolutional kernel that is wind with layers input which helps produce a tensor of outputs. A filter or a kernel present in a Conv2D layer "slides" over the 2D input data, performing an elementwise multiplication. Therefore, as a result, it will be adding up the results into a single output pixel. Similar layers are also represented within the Keras deep learning framework. Two-dimensional inputs, similar to images, are represented by *Keras.layers.Conv2D.*

VII. RESULTS

In this experiment, the top two models relu and tanh is compared to get a detailed analysis that which model will work efficiently for 20000 datasets. In other words, we are trying to find the model with the least final mean image reconstruction.

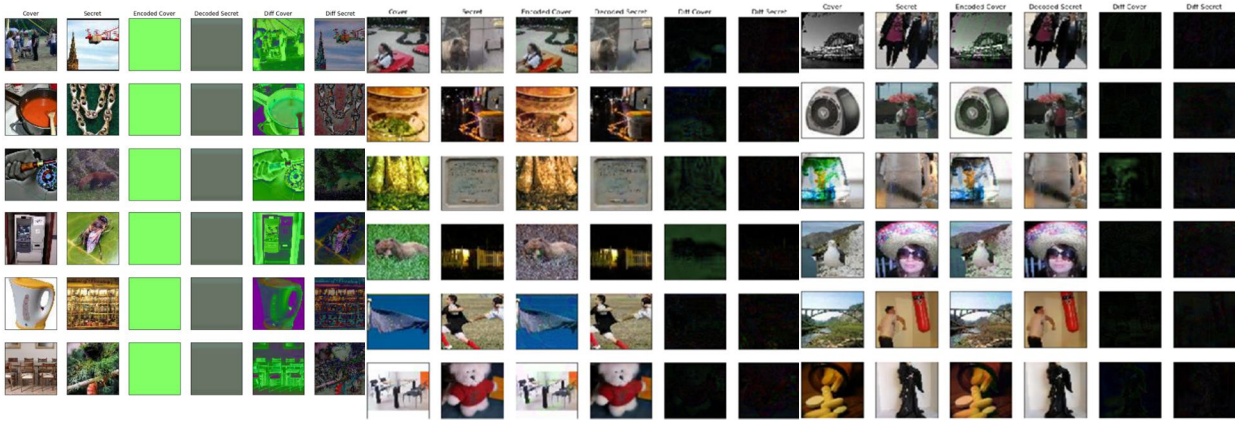


Figure 4: Results of Conducted Experiment, selu vs tanh vs relu

The output will be derived in the format as:

1) There are six objective examples as represented by six rows.
2) The six columns represent:

- cover image (Input)
- secret image (Input)
- encoded cover (Output of encoder Network)
- decoded secret (Output of reveal Network)
- the difference between encoded cover and original cover (Diff Cover).
- the difference between a decoded secret and an original secret image (Diff Secret).

The models are made to run for different epochs i.e 600 and 300 to get the optimized output.

- The first model, selu, leaves too many traces of the secret image while encoding it in the cover image. Due to the less efficiency of the model we have not considered it for the comparison.
- The second, tanh model leaves some traces (features) of the secret image while encoding it in the cover image. The tiny portion of the secret image can be observed in the encoded cover image in this model.
- The previous point is reaffirmed by the visible features in the diff Cover column. This illustrates the dissimilarity between the pixels of the generated cover image and the original cover image. Ideally, both the images should be the same, and the result should be a black picture as is the case of a secret image. But in the case of cover image difference, we can see some visible features which point to the fact that the obtained cover image is not identical by a little margin to the original cover image.

Comparing the results with the third model, we can see that it conceals the secret image much better as there is almost no trace of the secret image in the generated cover image. Also, the difference between the original cover and decoded cover is mostly a black picture which points to the fact that the generated cover image was very close to the original cover image. Hence, from the metric visualizations, it is confirmed, that the first model performs the best.

A. Effects of Activation Function

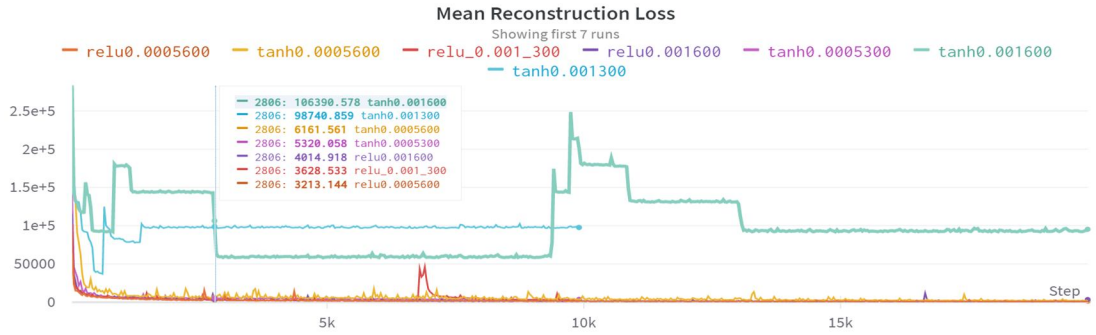


Figure 5: Effect of Activation Function

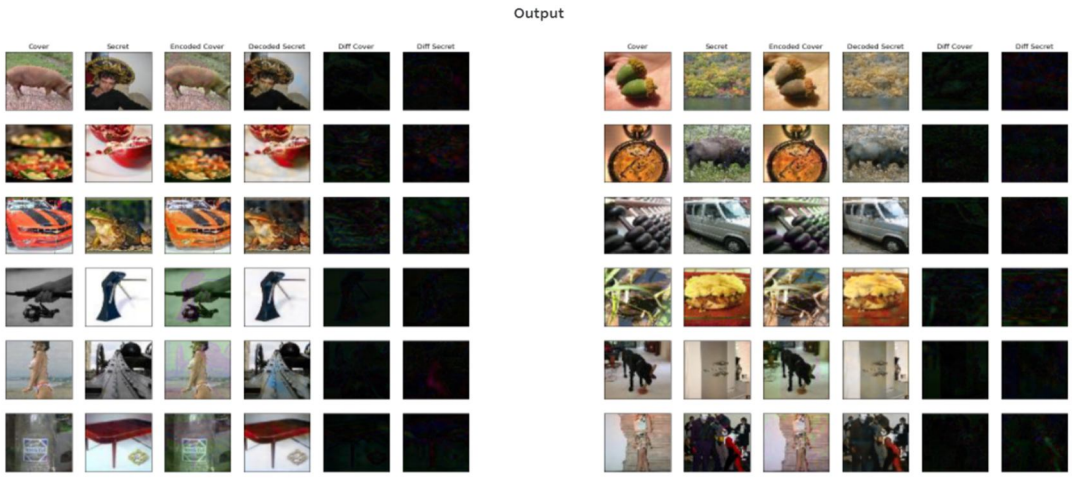


Figure 6: Results of Activation Function, relu vs tanh

Above shown figure, is the effect of activation functions on the performance of the model we have a side-by-side comparison of two models with all the same hyper-parameters that only differ in their activation functions. One uses relu activation and the different uses tanh.

B. Effects of Learning Rate

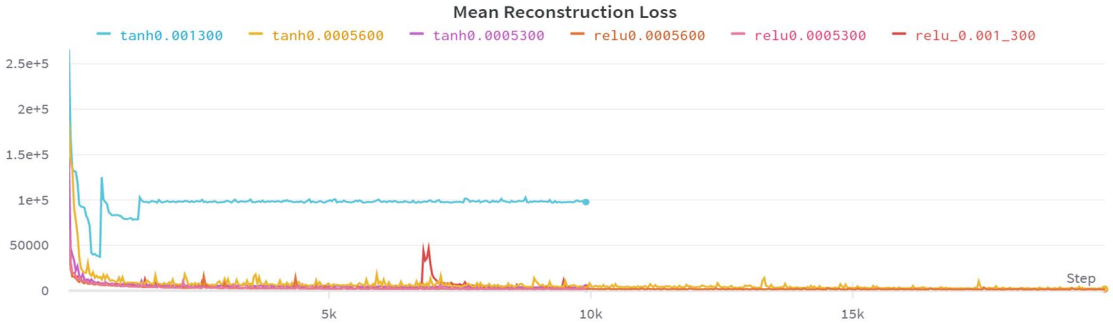


Figure 7: Effect of Learning Rate

Figure 8: Results of Learning Rate, relu vs tanh

Another fascinating outcome from the metric visualization is that the model with tanh activation, while optimized using a higher learning rate, got stuck in some local minima as pointed out by the flat mean reconstruction loss curve. Models with relu activation functions don't seem to face this problem. Let's see if we can confirm our deduction by visualizing the outputs of the models with tanh activations that got stuck in local minimas.

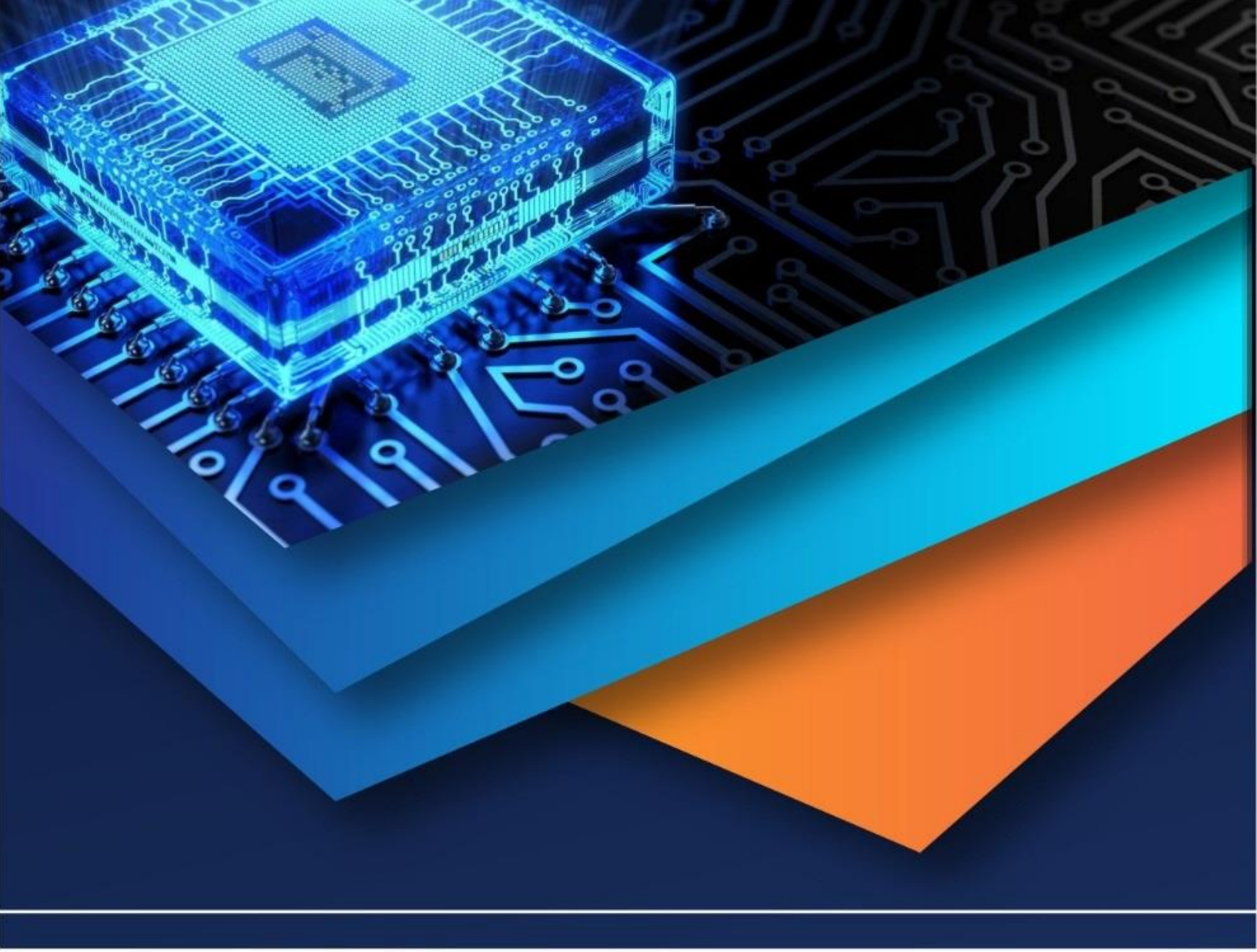
VIII. CONCLUSION AND FUTURE WORK

The proposed method concentrates on securing the image using DNN scenario in the beginning, we have started our work by surveying multiple papers and came to a conclusion that there is still scope for improving the image and thus increase in the accuracy of the retrieved image. We experimented our proposed work with 20,000 different pairs of datasets taken from Kaggle and other sources. We have experimented the proposed method using CNN, encoder, and decoder, model with different activation functions like selu, relu and tanh by varying learning rates, number of epochs and other parameters. After testing the accuracy achieved from the above test work is 96%. Thus, the objective of securing the image had been successfully implemented in our proposed work. We can extend our proposed work using GAN.

REFERENCES

[1] Shashikala Channalli and Ajay Jadhav, “Steganography An Art of Hiding Data” Shashikala Channalli et al /International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141
[2] Po-Yueh Chen, and Wei-En Wu, “A Modified Side Match Scheme for Image Steganography” International Journal of Applied Science and Engineering 2009. 7, 1: 53-60
[3] A. Nag, S. Biswas, D. Sarkar, and P.P. Sarkar, “A novel technique for image steganography based on Block-DCT and Huffman Encoding” International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010
[4] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image Encryption Algorithm Based on Chaotic Economic Model," Hindawi Publishing Corporation, Mathematical Problems in Engineering, vol. 2015, Article ID 341729, 10 pages, 2015.
[5] K.Brindha, R. Sharma, and S. Saini, "Use of Symmetric Algorithm for Image Encryption," International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, Issue 5, pp. 4401- 4407, May 2014.
[6] A. Jain, N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimedia Tools and Applications, An International Journal, Springer Science + Business Media Ne York, pp. 1-18, February 2015.
[7] Q. A. Keste, "Image Encryption based on the RGB PIXEL Transposition and Shuffling," I. J. Computer Network and Information Security, 7, in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijcnis.2013.07.05, pp.43-50, Published Online June 2013
[8] W. Zhu, "Image Encryption using CAT Mapping and Chaos Approach," International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pp.1-8, 2014.
[9] S. Kaur et al, "A Review of Image Encryption Schemes Based on the Chaotic Map," International Journal of Computer Technology & Applications, vol. 5, Issue. 1, PP. 144- 149, 2014.
[10] Y.-Q. Zhang, X.-Y. Wang,"A new image encryption algorithm based on nonadjacent coupled map lattices, "Applied Soft Computing, vol. 26, pp. 10–20, 2015.
[11] A. Devi, A. Sharma, and A. Rangra, "A Review on DES, AES, and Blowfish for Image Encryption & Decryption," Aarti Devi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, Issue. 3, pp. 3034-3036. http://www.ijcsit.com/, 2015.
[12] G. S. Chandel, P. Patel, "A Review: Image Encryption with RSA and RGB randomized Histograms," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 2, Issue 11, November 2013.

[13] Pia Singh, Prof. Karamjeet Singh, "Image Encryption And Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7, July 2013.
[14] K. K. R. Saraf, V. P. Jagtap, and A. K. Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 3, Issue 3, pp. 118-126, May – June 2014.
[15] R. Pakshwar, V. K. Trivedi, and V. Richhariya, "A Survey on Different Image encryption & Decryption Techniques," International Journal of Computer Science and Information Technology, vol. 4, no. 1, pp. 113-116, 2013.
[16] Madhu, Ganga Holl, "CNN approach for medical image authentication", Indian Journal of Science and Technology, Year: 2021, Volume: 14, Issue: 4, Pages: 351-360, Year: 2021, Volume: 14, Issue: 4, Pages: 351-360, https://doi.org/10.17485/UST/v1414.1963. Scopus, SIR Indexed, Q4 Level, SIR 0.11, H Index 41, WOS Indexed]
[17] Madhu B, Ganga Holi, "An Optimal and Secure Watermarking System using SWT SVD and PSO", Indonesian Journal of Electrical Engineering and Computer Science, Vol 18, No 2, May 2020, pp. 917926, DOI: http://doi.org/10.11591/jeecs.v18.12.gp917-926
[18] Madhu B, Ganga Holi, "Medical Image Authentication by SWT and SVD", International Journal of Recent Technology and Engineering (URTE), Volume-8 issue-3, September 2019, pp.953-958, ISSN:2277 3878, http://doi.org/10.35940/ijrte.C4111.098319.
[19] Madhu B., Holi G. (2019) An Imperceptible Secure Transfer of Medical Images for Telemedicine Applications. In: Santosh K., Hegadi R. (eds) Recent Trends in Image Processing and Pattern Recognition. RTIPZR 2018. Communications in Computer and Information Science, vol 1036. Springer, Singapore. https://doi.org/10.1007/978-981-13-9184-2_30



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY