The Secure Steganography Hiding Images Using Neural Networks

Jane Karuniya J
janekaruniyads@gmail.com
5th Year Msc Data Science(Integrated)
Coimbatore Institute Of Technology,
Coimbatore.

Suruthi R
suruthir2001@gmail.com
5th Year Msc Data Science(Integrated)
Coimbatore Institute Of Technology,
Coimbatore.

Dr. D. Sudha Devi
MCA.,M.Phil.,Ph.D.
sudhadevi.cit@gmail.com
Associate professor
Department Of Computing
Coimbatore Institute Of Technology,
Coimbatore

Dr. M. Srividya
MCA.,M.Phil.,Ph.D.
srividya.cit@gmail.com
Assistant professor
Department Of Computing
Coimbatore Institute Of Technology,
Coimbatore.

Abstract

Steganography is a hidden communication technique. Steganographyconceals the mere presence of the data itself. Any slight shift in the photos' pixel count has a minimal chance of being seen by human eyes. Information as a result picture's pixels may conceal anything. In order to encode and decode many hidden pictures inside of a single cover image while maintaining the same resolution, we plan to use deep neural networks. A LSB DCT-based steganographic technique is provided for hiding several photos beneath a cover image. The data is embedded via modifying the cover image's quantizedDCT coefficients' least significant bits. It is feasible to hide several pictures by inserting just higher bits of data in the cover image.

Keywords : *Steganography, LSB, DCT,Cover Image*

1. INTRODUCTION:

Steganography is the method of concealing secret messages within non-secret Images. Steganography, in combination with encryption, can be used to conceal or secure data. Steganography is traditionally used to insert low-resolution pictures onto high-resolution photos using crude methods such as LSB modification. We aim to encode multiple images into the single cover image where we use the same resolution cover and secret images and aimto keep the changes to the encoded coverimage unnoticeable to human perception and statistical analysis, while at the same timekeeping the decoded images highlyintelligible.

2. METHODOLOGY :

With the help of a single cover picture,multi-image steganography and concealing three or more images is accomplished. The hidden photos must be retrievable with the least amount of loss possible. The original cover picture must be recognisable in the encoded cover image. We send a number of hidden pictures over the prep network, combine the resulting data with the carrier image, and then send the entire thing over the hiding network. In thisimplementation, we used conditional decoders instead of multiple decoders,which was an alternative option. Solely focused on putting into practice many prep/reveal networks. As a result, wechose to base our extension on this method. An overview of the encoder/decoder. The encoder Consists of many prep networks, each of which corresponds to a different input secretpicture. Concatenated outputs from theprep network are passed via the Hiding network together with the cover picture. Decoder consists of Multiple reveal networks, each of which is trainedindividually to decode its respectivemessage, make up the decoder network.

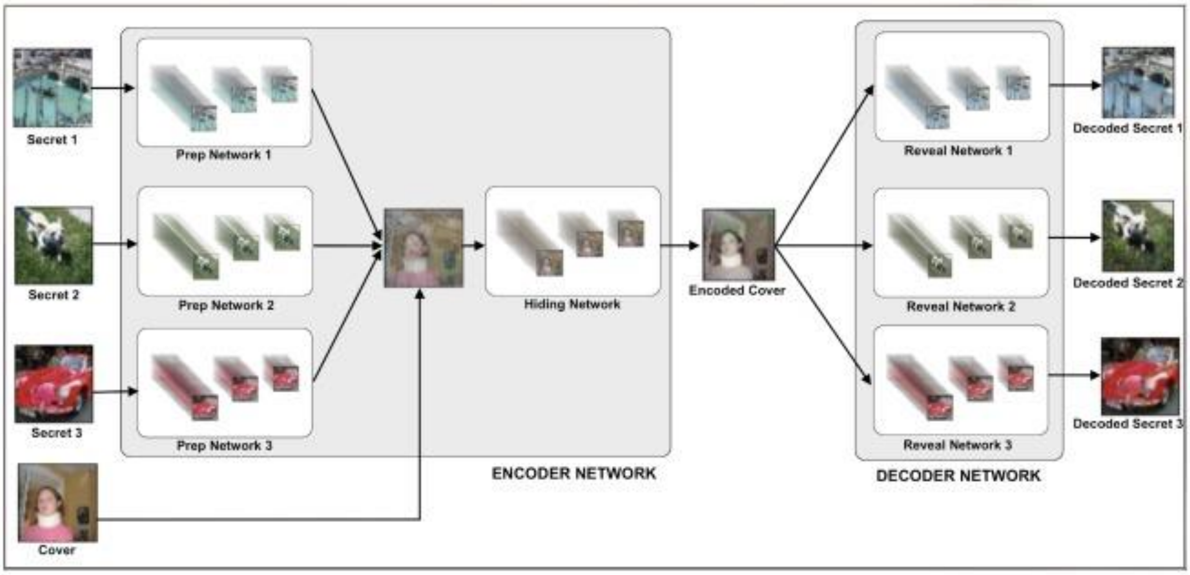

Fig 3.1– Model Architecture of MultipleImage Steganography using Deep Neural Network

The underlying architecture of each ofthe sub-networks is as follows:

- Each prep network is constructed from two layers. Each layer ismade up of three different Conv2D layers. There are 50, 10 and 5 Conv2D layers in total. It has kernel sizes of 3, 4, and 5, respectively within each layer. The stride length is always one alongboth axes . The required padding is applied to such that the outputpicture is kept in each Conv2D layer with the same dimensions. Each Conv2d layer is followed bya RELU activation.
- The hidden network is divided into five levels. These layers are composed of three separate Conv2D layers. The Conv2D layers in the hidden network have the same fundamental structure asthe Conv2D layers in the PrepNetwork.
- The core design of each of the reveal networks is similar to that of the concealment network, with 5 layers of similarly generated Conv2D layers.

3. IMPLEMENTATION DETAILS:

The Adam optimizer was used in conjunction with a custom LR scheduler. The learning rate remains constant at 0.001 for the first 250 epochs, then reduces to0.00045 between 250 and 450 epochs, and then drops to 0.00006 for the remainingiterations. The model was trained for

750 epochs with 254 batches and 470 epochs with 32 batches. Tiny Image Dataset was utilised, with pictures of 64x64 pixels. The dataset is created by taking 10 photos each class for training and a total of 2500 images for training and testing. Tiny Image Dataset was utilised, with pictures of 64x64 pixels. The dataset was created by taking ten shots each class for train and a total of 2500 photographs for train and test. The preparation and concealment networks share the stacking Keras model and loss. The revelation network has it own layered model as well as its own loss given the following outcomes -function. The current rate of learning is 0.0013. Reveal network weights are frozenbefore being introduced to the whole model to guarantee that weights are only adjusted once. Gaussian noise with a standard deviation of 0.01 is introduced before passing the encoder output via the decoder. The loss of the decoder was calculated using the mean sum of squared errors. While training the reveal network, we just analyse the loss's concealed image component. The loss for both the cover and concealed picture is evaluated throughout the model training process. Both s and c are currently treated as 1.00.

1. Total lost- 167083.26
2. Loss1 - 49834.5
3. Sec2 - 38674.76
4. Loss 3 - 38758.09
5. Loss Insurance - 46283.08

The results two and three are now being taken. The secret image is then added to the cover image and retrieved. The loss for all values grows as the number of frames increases because more visual elements are accessible and buried in a single image.

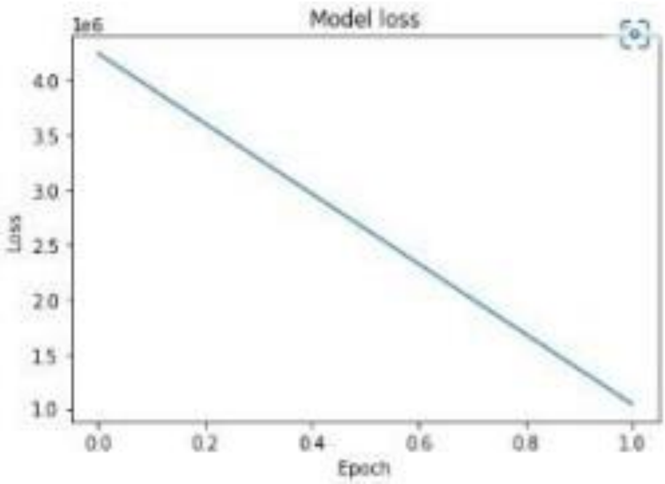

Fig 3.2 – Total Loss per epoch forthe whole model

A. PURPOSE:

Steganography is a way of hiding information within an item while making the object containing the hidden information indistinguishable from the original. Steganography's principal purpose is to limit access to secret information to authorised clients while concealing its content and existence from the rest of the world. Various carriers, such as physical items, texts, noises, and network packets, have been employed to discreetly disguise and transport private data. In modern digital steganographic techniques, one of the most widely used carriers is a digital picture.

B . MAJOR RESEARCH FINDINGS :

The encrypted cover image closely matches the original cover, and it does not disclose important image information. Encrypted shells lose more than shells when only two secret images are used. Secret artworks were successfully restored in both situations. Losses after 750 epochs

4. CONCLUSION:

In the image domain, we learned about the covert printing strategy. Reading other papers may help us understand more about the problem statement, which is crucial in data security. Our approach has increased the single sample steganography picture of the deployment of some network of revelations corresponding to each secret image. We were able to encrypt and decode up to three distinct secret pictures on a single comparable-sized cover photo while minimising private we haven't met the kind of hypothetical losses that are better suited to our model.

Fig 4.1 – Final outputs after applying Deep Neural Network

5. FUTURE ENHANCEMENTS:

Increase the number of concealed images while reducing loss. We're looking into s and c to see how they affect our results. Use conditional decoders instead of multiple decoders. We used eye inspection as our major evaluation criterion; however, we might enhance this by putting the encoded cover image via security technologies to validate pixel details. This project provides an opportunity to experiment with steganography and, more broadly, the inclusion of supplementary information in photographs. Several previous strategies used neural networks to complement or replace a minor component of an image-hiding system. We are seeking to demonstrate an approach for constructing a totally trainable system capable of producing visually pleasing outcomes when inserting multiple full-size, colour pictures into a carrier image in an unobtrusive manner. Extensions can lead to a comprehensive steganographic system that hides the message's existence from statistical analyzers. This will very definitely necessitate a new aim in terms of training and embedding smaller images within larger cover designs.

6. REFERENCES :

i. Channalli, S.; Jadhav, A. Steganographyan art of hiding data. arXiv 2009, arXiv:0912.2319.

ii. Zhang, X.; Wang, S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Lett. 2004, 25, 331–339. [CrossRef]

iii. Goljan, M.; Fridrich, J.; Holotyak, T. New blind steganalysis and its implications. In Security, Steganography,and Watermarking of Multimedia Contents (VIII); International Society for Optics and Photonics: Washington, DC, USA, 2006; Volume 6072, p. 607201.

iv. Pevny, T.; Bas, P.; Fridrich, J. Forensics Secur. (TIFS) 2010, 5, 215–224.[CrossRef]

v. Ronneberger, O.; Fischer, P.; Brox, T. U-net: Convolutional networks for biomedical image segmentation. In International

vi. Conference on Medical Image Computing and Computer-Assisted Intervention;Springer: Cham, Switzerland, 2015; pp. 234–241

vii. Springenberg, J.; Dosovitskiy, A.; Brox,T.; Riedmiller, M. Striving for Simplicity: The All Convolutional Net. In Proceedings of the International Conference on Learning Representation Workshops (ICLRW), San Diego, CA, USA, 7–9 May 2015.

viii. Ioffe, S.; Szegedy, C. Batch normalization: Accelerating deep network training by reducing internal covariateshift. In Proceedings of the Int'l Conference on Machine Learning (ICML), Lille, France, 6–11 July 2015; pp. 448– 456.

ix. Noh, H.; Hong, S.; Han, B. Learning deconvolution network for semantic segmentation. In Proceedings of the Int'l Conference on Computer Vision (ICCV), Santiago, Chile, 7–13 December 2015; pp. 1520–1528.

x. Agarap, A.F. Deep learning using rectified linear units (relu). arXiv 2018, arXiv:1803.08375.

xi. Hore, A.; Ziou, D. Image quality metrics: PSNR vs. SSIM. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, Steganalysis by subtractive pixel adjacency matrix. IEEE Trans. Inf. 23–26 August 2010; pp. 2366–2369.