https://doi.org/10.31871/IJNTR.10.2.7 International Journal of New Technology and Research (IJNTR)
ISSN: 2454-4116, Volume-10, Issue-2, February 2024 Pages 01-03 Pages 11-14

Data Hide using Deep Neural Network in Encrypted Images

Ms. Nagma Shaikh, Ms. Pooja Waghamare, Ms. Bhavana Potrajwar, Mrs. Rupali Sarde

Abstract- **In recent day, images are shared on social media platform, for this image security is big problem. In order to conceal the message from the image and vice versa, we would like to employ steganography and coding techniques. We often use a lossless reversible technique for embedding and extracting information within the designed system. By gently altering the pixel values, we can insinuate secret data into the cowl image via a technique known as reversible information concealment. In this paper, in this paper we study alternative approach for combining models such as convolution neural networks and generative adversarial networks to obtain meaningful encrypted images for RDH. In this practical we designed using a four-stage specification t includes the hiding network, the encryption/decryption network, the extractor, and ultimately the recovery network. Through residual learning, the crucial information was incorporated into the image within the concealing network. The main image is encrypted using GAN into a meaningful image called as the embedded image inside the encryption/decryption network. The embedded image is restored to the decrypted image. In this to fully extract the secret message on the receiving end, the original image must be retrieved. The numerous uses, including social control, the medical field (where patient data confidentiality is an example), and the military, where the ability to conceal information is highly valued.**

Index Terms- **Data Hiding, GAN model, Deep Neural networks RDH.**

I.INTRODUCTION

In publishing the image in the media, the medical industry, the military, and other industries Digital image use. As such, the integrity and copyright of digital images must be preserved. To represent the image using the standard text encoding formula not possible because of image's vast amount of knowledge, high correlation, and high redundancy between pixels. Knowledge hiding, a subset of digital watermarking technology, may be a crucial tool for guaranteeing the security of advice.

Ms. Nagama Shaikh, Working Lecturer at Swami Vivekanand Institute of Technology (Poly), Solapur. , Pursuing MTech in CSE.
Ms. Pooja Waghamare, Working I/C HOD at Swami Vivekanand Institute of Technology (Poly), Solapur. , Pursuing MTech in CSE.
Ms. Bhavana Potrajwar, Working Lecturer at Swami Vivekanand Institute of Technology (Poly), Solapur. , Completed ME in CSE.
Mrs. Rupali Sarde, Working Lecturer at Swami Vivekanand Institute of Technology (Poly), Solapur. , Completed BE in CSE.

Knowledge concealment might be enforced in a variety of distinct methods. Information concealment can be categorized into two types: irreversible information concealment and reversible knowledge concealment, depending on the recipient will retrieve the quilt image. Data hiding in the video may provide a means of preventing access to the original contents after the embedded messaging unit of measurement—such as image data, labels, annotations, or authentication information—are recovered from the encrypted photographs.

RIT-based frameworks protect the privacy of the first picture by shifting its content to that of the canopy image. They are changeable; they may be reconditioned from the altered image without losing any information. Because of this, RIT is frequently thought of as a unique secret writing topic known as "Semantic Transfer secret writing (STE)". Since the camouflage image is a type of plaintext, outsiders cannot annotate it. outsiders will only employ antiquated RDH techniques for plaintext images to insert additional information into the camouflage image.

There is popular issue in this method, maximize reversible information concealing within the encrypted picture (RDHEI) these methods, are unable to provide a robust embedding capacity. Therefore, for this offer a lossless element conversion (LPC) supported RDHEI over them. LPC is motivated by the coplanar map coloring question and uses a dynamic image division technique to split the original image into irregular regions as opposed to regular blocks. The LPC approach performs element conversion by region, meaning that accessible area is reserved to hold additional information.

II.RELATED WORK

Using distributed supply coding, Zhenxing Qian et al.'s paper suggests a method of reversible record concealing in encrypted photos. The real photo segments of MSB planes are chosen and compressed after encryption to create space for the additional mystery records.

On the receiving end, the encryption key is the sole tool used to retrieve the genuine photo, and the embedding key is the only tool used to extract concealed records. The real photo can be flawlessly recovered and the concealed records fully extracted when all of the encryption and embedding keys are difficult for the recipient to decipher. [2]

The goal of Weiming Zhang ET. Al's suggested strategy is to improve upon earlier approaches that converted a target image into a cowl image by encryption. It support reversible image

modification, which preserves the privacy of the first image of the same size while transferring the original image's linguistics to a subsequent image. By using a modified, incredibly safe, and lossless method of reversible image modification, the original image can be recovered from the encrypted image. Two RDH techniques were used, namely PEE-based RDH and UES, [1]

Xinpeng Zhang developed paintings with probabilistic and homomorphism qualities that suggest lossless, reversible, and mixed record concealment techniques for ciphertext images encrypted using public-key cryptography. In the lossless technique, new values for embedding the additional records into the LSB-planes of the cipher textual content pixels are applied to the cipher textual content pixel values. In this manner, the unique plaintext picture may be decrypted without any issues, and the contained records can be quickly recovered from the encrypted domain. In the reversible technique, half of the cipher textual content pixel values are altered for record embedding, and a histogram reduction preprocessing is done prior to encryption. Data can be extracted in plaintext on the receiving end. [4]

III.PROPOSED SYSTEM

Proposed Architecture:

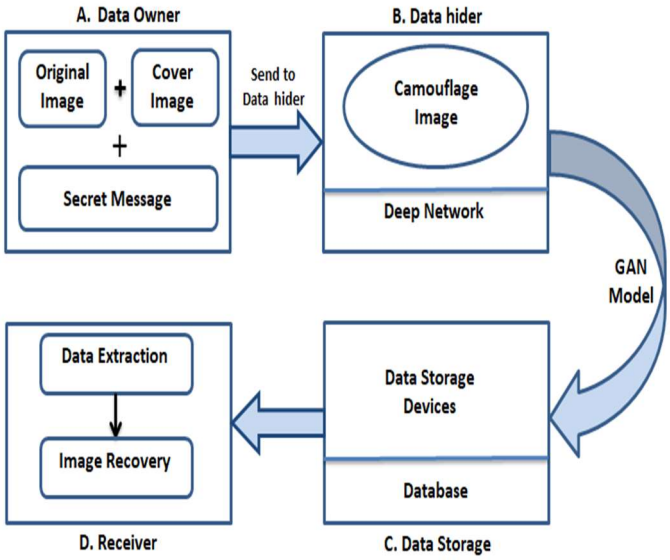

Fig.1. Proposed flow Architecture

Modules

A.Data Owner
B.Data Hider
C.Data Storage Devices
D.Receiver

Data Owner

Choosing image as Input: The color image is taken as the original cover image

Encrypt one image into another image: The original image is encrypted into another plaintext image with a key. Camouflage image generation is done and it is input to the data hider.

Data Hider

Encryption of Data: Secret data to be embedded is concealed using a data-hiding key into the camouflage image. A camouflage image with secret data so formed is passed as an input to the Data storage device. The next Module is the data storage device module.

Data Storage Device

Data Embedding: The storage devices (maybe outsiders) can embed additional data into Camouflage images by using any classical RDH method of plaintext images.
Data Removing: The Storage devices (maybe outsiders) can extract additional data from Camouflage images by using any classical RDH method of plaintext images. So formed Camouflage image with additional data is passed as an input to the receiver.

Receiver

A receiver can be either the content owner or any authorized person having the key, the receiver will have the key for decryption.

a. Image decryption: A camouflage image so formed from the data hider is received by the receiver. The image is decrypted using the decryption key.

IV. MATHEMATICAL FORMULATION

Encoding Formula

$$Yi = Ek(Xi),$$

where Ek() is the encryption function and Yi is the corresponding cipher-text to Xi.
Sizes of Xi and Yi are identical.

Decoding Formula.

$Xi = Dk(Y\ 0i)$ if $\sigma(Dk(Y\ 0i)) < \sigma(Dk(Y\ 1i)) = Dk(Y\ 1i)$ else.

Showing Quality of Image with PSNR

The Peak Signal Noise Ratio (PSNR) measures the relationship between an image's maximum possible power and the amount of noise that distorts the image's quality.

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

The common square difference between the genuine value and the calculable worth is measured by the Mean Square Deviation (MSD) or Mean Square Error (MSE) of an expert. Love the first instant of the square mistake loss, but it's a risky operation.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(Y_i - \hat{Y}_i)^2$$

Structure similarity (SSIM) index for a volume or grayscale picture a mistreated referee due to the volume or reference image. A value closer to one denotes a better-quality image.

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Pearson Correlation Index

The Pearson's methodology is widely used in image processing, pattern identification, and applied mathematics analysis. Utilizing the latter, applications include comparison Two images for the purpose of image registration

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

Embedding Capacity

$$\text{Relative Capacity} = \frac{\text{Absolute Capacity}}{\text{Size of the Image}}$$

V. RESULTS

1. Main Option for Users

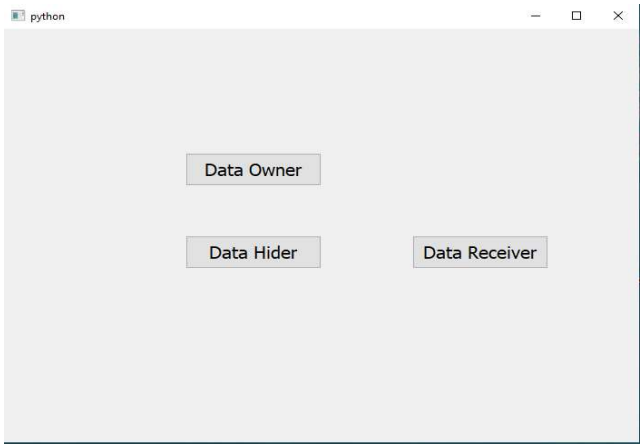

Figure2. Main Window of Project

Figure2 shows the Main Window of the Project where the Data owner, Data hider, and Data receiver can log in for further operation.

2. Calculation of Embedding Capacity

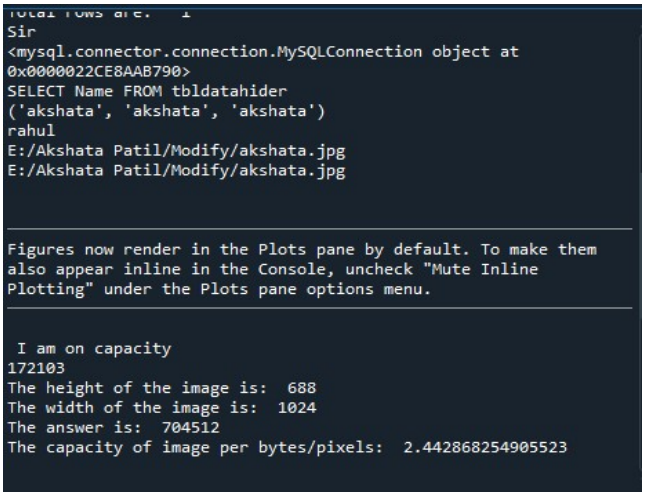

Figure 3 Calculation Embedd Capacity

Figure3 Shows embedding capacity of image per bytes/pixels.

3. Creation of Camouflage Image

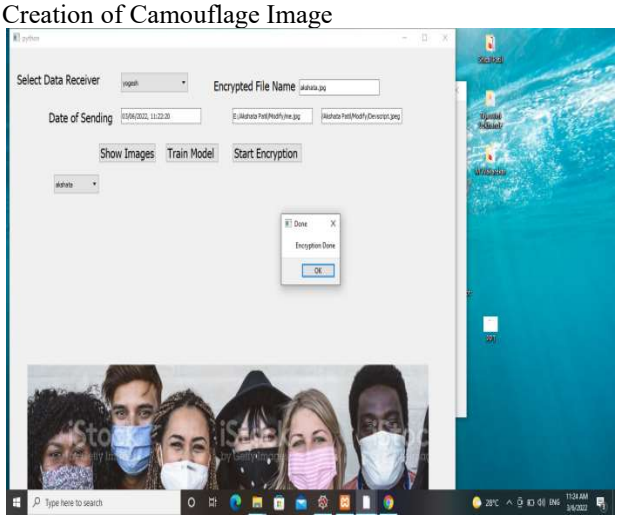

Figure4. Creation of Camouflage Image

Figure4 shows the creation of a camouflage image with secret and cover images and also data hider enters the encrypted file name. Since the technique is reversible, we combine the two images into one image.

4. Decryption of Information

Show that the receiver can decrypt the authorized File. Here we use an encoder and decoder network for decryption purposes.

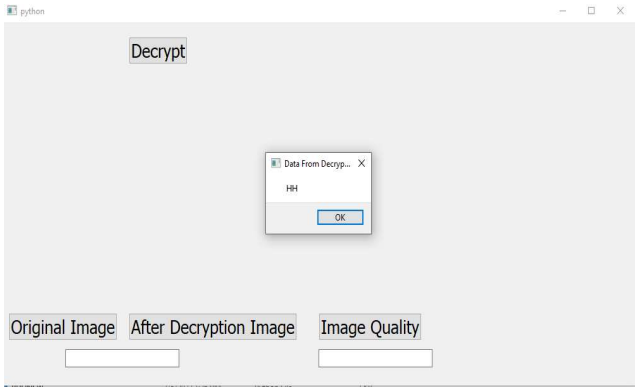

Figure5. Decryption of Information

5. GAN Model Evaluation

```
Anaconda Prompt (anaconda3) - python  untitled3.py
0
tensor(0.0958, grad_fn=<MseLossBackward0>)
6.757725603878498
tensor(0.0642, grad_fn=<MseLossBackward0>)
13.262911010533571
The Training Accuracy is : 0.06494920107111493
The Epoch is: 2
tensor(0.0577, grad_fn=<MseLossBackward0>)
0
tensor(0.0658, grad_fn=<MseLossBackward0>)
6.090288128703833
tensor(0.0764, grad_fn=<MseLossBackward0>)
12.259729091078043
The Training Accuracy is : 0.06027984894259237
The Epoch is: 3
tensor(0.0539, grad_fn=<MseLossBackward0>)
0
tensor(0.0517, grad_fn=<MseLossBackward0>)
5.87327191606164
tensor(0.0508, grad_fn=<MseLossBackward0>)
11.722299665212631
The Training Accuracy is : 0.058253395762755254
The Epoch is: 4
tensor(0.0323, grad_fn=<MseLossBackward0>)
0
tensor(0.0520, grad_fn=<MseLossBackward0>)
5.972410369664431
tensor(0.0531, grad_fn=<MseLossBackward0>)
11.539793536067009
The Training Accuracy is : 0.0573919155625067
```

Fig6 GAN Model Evaluation

The Fig6 Shows the GAN Model evaluation and iteration.

4. Metrics for evaluating image quality

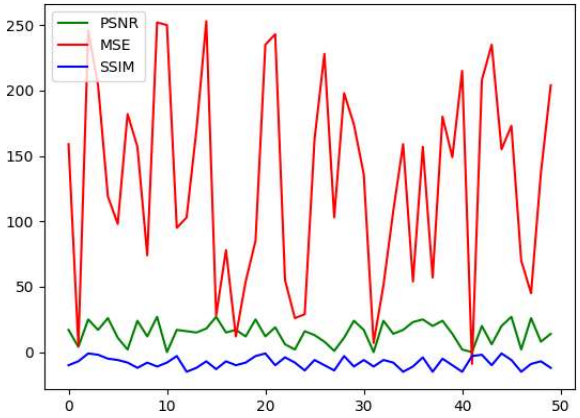

Fig.7This chart shows PSNR, MSE, and SSIM as Image Quality Evaluation Metrics.

CONCLUSION

In this paper, we have tested a novel architecture that supports reversible image transformation (RIT) and reversible data concealment in the encrypted image (RDC-EI). Unlike earlier frameworks, which converted a plaintext image into a cipher text type, this one is distinct. In order to protect a picture's privacy, it embeds one image within another. Consequently, some of the shapes of plain text images are present in encrypted images. Here, the data has been encrypted and decrypted using the CNN and GAN Model using RDH technique. The embedding capacity is initially calculated in this technique. The purpose of this GAN model is to increase accuracy while reducing the number of iterations.

REFERENCES

[1] W. Zhang, H. Wang, D. Hou, N. Yu "Reversible Data Hiding in Encrypted Images by Reversible Image Transformation" 2016 IEEE.

[2] Z. Qian, X. Zhang "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding" IEEE Transactions on Circuits and Systems for Video Technology 2016.

[3] X. Cao, L. Du, X. Wei, Dan Meng "High-Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation" IEEE TRANSACTIONS ON CYBERNETICS, 2015.

[4] X. Zhang, J. Long, Z. Wang, and H. Cheng "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" IEEE Transactions on Circuits and Systems for Video Technology, 2016.

[5] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography" IEEE Trans. on Circuits and Systems for Video Technology, 2015.

[6] J. Zhou, W. Sun, Li Dong, et al., "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, Mar. 2016.

[7] Z. Qian, and X. Zhang, "Reversible data hiding in an encrypted image with distributed source encoding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, Apr. 2016.

[8] Duan, X.; Jia, K.; Li, B.; Guo, D.; Zhang, E.; Qin, C. Reversible Image Steganography Scheme Based on a U-Net Structure. IEEE Access 2019, 7, 9314–93