IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

# Reversible Data Hide using in Encrypted Images using deep neural network and gan model

**Nagma Shaikh**
**Dr. S.P. Pawar**
SVERI Collage of Engineering, Pandharpur

***Abstract***- These days, images are shared on social media, which has led to photo security. In order to conceal the important 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, we propose an alternative approach for combining models such as convolution neural networks and generative adversarial networks to obtain meaningful encrypted images for RDH. The experiment is designed using a four-stage specification that 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 quilt image is encrypted using GAN into a meaningful image known as the embedded image inside the encryption/decryption network. Subsequently, the embedded image is restored to the decrypted image. In order 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. This application also aims to retrieve the original image without any loss. Another strategy is to determine the standard of image exploitation by calculating the image's embedding capabilities. SSIM.

.

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

## I. INTRODUCTION

Digital images are widely used in publishing, the media, the medical industry, the military, and other industries. As such, the integrity and copyright of digital images must be preserved. It is not possible to represent the image using the standard text encoding formula due to the image's vast amount of knowledge, high correlation, and high redundancy between pixels. In addition to features, many technologies, such as watermarking and image authentication, being created for images. Knowledge hiding, a subset of digital watermarking technology, may be a crucial tool for guaranteeing the security of advice.

In order to achieve the goal of useful embedding of hidden knowledge, 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 whether 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.

Our suggestion is a framework called Reversible Image Transformation (RIT). RIT-based frameworks protect the privacy of the first picture by shifting its content to that of the canopy image. Additionally, because 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 called "Semantic Transfer secret writing (STE)". Since the camouflage image is a type of plaintext, outsiders cannot annotate it. Consequently, outsiders will only employ antiquated RDH techniques for plaintext images to insert additional information into the camouflage image.

A lot of methods are anticipated to maximize reversible information concealing within the encrypted picture (RDHEI), which is becoming a popular issue. These methods, however, are unable to provide a robust embedding capacity. Therefore, in this research, we tend to offer a lossless element conversion (LPC) supported RDHEI theme. In contrast to the earlier RDHEI algorithms, 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. In other words, pixels within the same regions are reborn to an equivalent conversion value, which can occupy a lesser size. Since LPC may be a process, the original picture is retrieved on the receiver facet without any loss.

## II. Related Work

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. Supported by 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, to add more information to the encrypted image in order to meet various requirements for embedding capability and image quality. [1]

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]

Xiaochun Cao et al. proposed a novel method in this study called the HC_SRDHEI, which inherits the reparability property of RDH methods in encrypted images as well as the features of RRBE. Are vacated for knowing concealing by our technology is significantly larger used than advancing alternatives? The knowledge information hider only uses the element replacement technique to replace the provided room with additional secret information. The area unit that contains the information extraction and canopy picture recovery can be separated, and it is error-free. Based on three datasets of experiments, it is unquestionably true that our average MER will be 1.7 times larger than what the best alternative technique offered previously. The examination of performance suggests that our proposed method has a great potential for rational applications [3]

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]

A stable reversible picture data concealing (RICH) subject that functioned across an encrypted domain was fashioned by J. Malathi. It demonstrates a public key modulation approach that enables the United States of America to plant data through clean XOR operations while eliminating the requirement to obtain access to the crucial encoding key. It is recommended that a strong two-elegance SVM classifier be used at the decoder stage in order to distinguish between encrypted and non-encrypted image patches, authorize active North American U.S.A. jointly decipher the hidden message, and as a result, the unique picture sign dead. [5]

## III. Proposed System

The original image must be perfectly recovered without any loss and the hidden messages must be fully extracted on the receiving side without any distortion in order to develop a system that uses camouflage images and enables users to embed additional data into the images without accessing the original contents.

## Proposed Architecture:

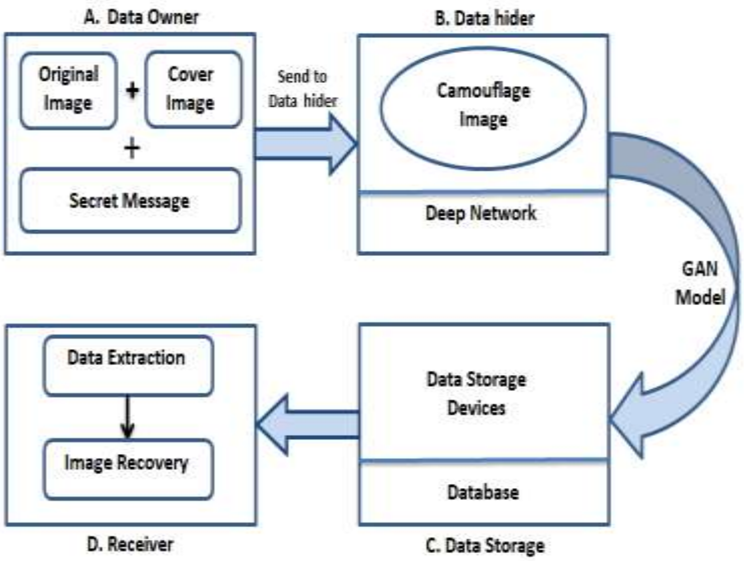

Fig.1. Proposed Architecture

**Modules**
The system has the following modules.

1. Data Owner
2. Data Hider
3. Data Storage Devices
4. Receiver

**Data Owner**
The data owner section deals with

a. Choosing image as Input: The color image is taken as the original cover image
b. 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**
The Data Hider section has some of following functionalities.

a. 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**
The Data Storage devices section deals with

a. Data Embedding: The storage devices (maybe outsiders) can embed additional data into Camouflage images by using any classical RDH method of plaintext images.
b. 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 σ(Dk(Y 0i)) < σ(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.

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

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.

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

### 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

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

## 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. J. Malathi, T. Sathya Priya “Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation” International Journal of Advanced Research in Computer and Communication Engineering, vol.6, Nov 2017.

6. 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.

7. 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.

8. 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.

9. 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, 9314–9323.