International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 09 | Sep 2022 www.irjet.net p-ISSN: 2395-0072

Reversible Data hiding in Encrypted Images using Deep Neural Network and MSB Prediction

Yojana Patil [1], Prof. P.S. Powar [2]

[1]*student, computer engineering, AMGOI wathar, Maharashtra India*
[2] Professor, *computer engineering, AMGOI wathar, Maharashtra India*

Abstract - *Nowadays, photos are shared through social media, and we got to the security of photos. Thus, we'd like to use coding and steganography techniques to hide the critical message in the image and the other way around. Within the planned system, we tend to apply a lossless reversible process for embedding and extracting the info. Reversible information concealing may be a technique wherever we infix personal data into a cowl image by slightly modifying the pixel values. This Paper used the replacement methodology of mixing the model like convolution neural networks and generative adversarial networks to get meaningful encrypted pictures for RDH. The four-stage specification is intended for the experiment, together with the concealing network, the encryption/decryption network, the extractor, and the recovery network. First, the critical information area unit is embedded into the image within the concealing network through residual learning. Then, within the encryption/decryption network, the quilt image is encrypted into a meaningful image, referred to as the embedded image, through GAN, then the embedded image is restored to the decrypted image. The initial image is required to be recovered; thus, the hidden message is extracted from the receiving aspect. The many applications like social control, medical applications, for example, are keeping patients' data secret, and military applications where the property of secret hidden information is in high demand. Also, this application desires lossless recovery of the initial image. Another approach is calculating the embedding capability of the image and finding the standard of image exploitation SSIM.*

Key Words*: *Data Hiding, Deep Neural networks, GAN model.

1. INTRODUCTION

Digital footage is widely used in media, publishing, medicine, military, and alternative fields. To preserve the integrity of photographs, it is imperative not to waste their content. The image has its own characteristics, such as large amounts of data, high co-relation, and a common secret writing formula. On top of functions, such as image authentication and watermarking, a variety of technologies have been developed for footage. Data concealment is a branch of digital watermarking technology that may be essential to confirming the security of a subject matter. Knowledge concealment could also be implemented in various ways to comprehend the aim of useable embedding of secret data. Whether or not or not the receiver can recover the quilt image, data Concealment could also be divided into irreversible data concealment and reversible data concealment. Information concealing within the footage could also be how by that the initial cowl will losslessly recover once the embedded messages unit of measuring is extracted, e.g., image data, labels, notations, or authentication data into the encrypted footage, whereas not accessing the initial contents. We propose a Reversible Image Transformation (RIT) framework. RIT-based frameworks shift the primary image's content to the cover image's content, and so defend the privacy of the primary image. Quality suggests that they will be losslessly restored from the reworked image. therefore, RIT has commonly viewed as a secret writing theme referred to as "Semantic Transfer secret writing (STE)."Because the camouflage image may be quite a plaintext, it's going to avoid the notation of the outsiders. So, the outsiders can implant more data into the camouflage image with ancient RDH methods for plaintext footage.

Reversible info concealing inside the encrypted image (RDHEI) has become a hot topic, and plenty of algorithms square measure projected to optimize this technology. However, these algorithms cannot deliver the good's strong embedding capability. Thus, throughout this Paper, we tend to propose a classy RDHEI theme supported by lossless part conversion (LPC). Unlike the previous RDHEI algorithms, LPC is galvanized by the planar map coloring question. It performs a dynamic image division methodology to divide the initial image into unstable regions instead of regular blocks inside the previous RDHEI algorithms. Inside the technique of LPC, part conversion is performed by region; that is, pixels inside identical square measures are regenerated to the same conversion price, which may occupy a smaller size. Therefore, the accessible area is reserved to accommodate more info. LPC could also be a process, so the initial image is losslessly recovered on the receiver side.

1.1 RElETED WORK

Weiming Zhang ET. Al suggested improving the proposed schemeotherwise, plans to encrypt the image code first a picture on the hood. A transformed image renders linguistics original linguistic image of another incarnation and goals Mystery of the first image with the same size. Because he is converted Image transformation and restoration of the

original image from the file encrypted image in total loss and safe modification Addition 2 RDH strategies along with PEE-based RDH e Units in the UES area have been adopted to include additional information in them encrypted image to fulfill various requests for the image, for example Ability to abstract [1]

Zhenxing Qian et added that the paper proposes a reversible recording scheme hidden in encrypted pixels using distribution supply coding. After encrypting the original image, the fragments of the MSB plane are identified and compressed to accommodate the additional mystery files.On the receiving side, the hidden records are removed only with the embedded key, and the original image is restored only with the encryption key. When each of the embedded and encrypted keys must be difficult for the recipient, the hidden records can be completely removed and the original image perfectly restored [2]

In this article, Xiaochun Cao et al. develop a unique technique called HC_SRDHEI that inherits the advantages of RRBE and the variable property of RDH strategies in encrypted images. Is our technique used much more to hide information compared to the other progressive options? Information hiding is simply an element substitution to replace the offered space with additional secret data. The unit area for information extraction and the canopy image can be separated, and the unit area is error-free. Experimental results on three datasets indicate that our average MER will approach one. Seven times larger because the previous best other technology. The performance analysis suggests that our design approach has excellent potential for meaningful applications. [3]

Xinpeng Zhang proposed a painting proposing lossless, reversible, and mixed record concealment schemes for ciphertext content encrypted using public-key cryptography with probability and homomorphism properties. In lossless mode, the pixel values of the ciphertext content are changed to new values to embed the additional entries in the LSB plans of the ciphertext content pixels. In this way, the embedded records can be extracted immediately from the encrypted domain, and the embedding process of the forms no longer interferes with the decryption of the plaintext's unique image. In the reversible scheme, the reduction of the histogram is pre-processed before encryption, and 1/2 the pixel values of the ciphertext content are modified to embed the records. On the receiver side, data can be extracted in plain text form. [4]

This is how J. Malathi implemented a RICH (Stable Image Data Hiding) argument in the cryptographic domain. It demonstrates a public key change mechanism that allows North America to implant data through pure XOR operations even when they no longer need access to the critical encryption key. For the decoder function, it is recommended to use a strong two-elegance SVM classifier to distinguish between encrypted and unencrypted image patches, North American active sanctions in the US separate the embedded message together and then the single dead image signal [5]

1.2 PROPOSED SYSTEM

In proposed system develop a system that implements camouflages that allow users to embed additional data into camouflages without accessing the original content, it is necessary to restore the original image, ideally without loss, and to completely remove hidden messages on a receiving side.

Modules

The system has the following modules.

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

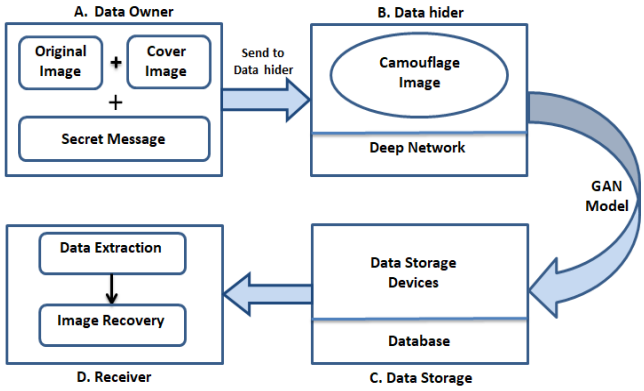


Fig.1. Proposed Architecture

Data Owner

The data owner area takes care of that

a. Input image: The original cover image is a color image

b. Encrypt one image into another image: The original image is encrypted into another plaintext image using a key. In the next step, camouflage images are generated, and they are input into the data hider.

Data Hider

The Data Hider section has some of the following functionalities.

a. Data Encryption: Secret data is embedded into camouflage images using a data-hiding key. Input to the Data storage device is a camouflage image with personal data. Data storage devices are the next module.

Data Storage Device

The Data Storage devices section deals with

a. Data Embedding: Stored (maybe external) additional information on camouflage images can be located using any RDH display to open pictures of text.

b. Data Removing: The Storage devices (maybe outsiders) can be added to Camouflage Photos using any classic flat RDH imaging method. The camouflage formatted image is forwarded and the data is added as an input to the receiver.

Receiver

The recipient can be the owner of the content or someone with an authorized key; the receiver will have the key for decryption.

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

2. Objective of the System

1.Embedding additional data (Text/Audio) into camouflage images in a reversible and lossless manner.

2. Camouflage image quality should be improved.

3. Deep neural networks are used to embed and extract data from images

4. To generate a GAN (Generative Adversarial Network) for real-time steganography.

5. The original plaintext image must be recovered without error

Method of Implementation

1.Lossless Reversible Data hiding

Reversible data hiding (RDH) covers data and recovers the original data afterward; embedded data is removed. This method is widely used in medical, military, and law forensics imagery. There is no tolerance for distortion of the unique cover. In the meantime, RDH has been a subject of substantial investigation since it was first presented.

RDH Embedding

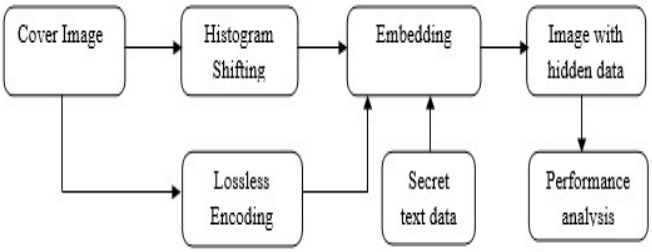


Fig.2. RDH Embedding

RDH Extraction

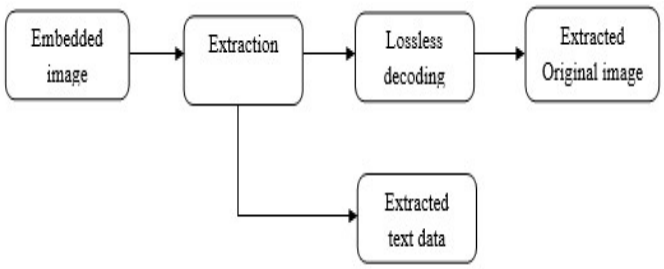


Fig.3. RDH Extraction

2. GAN (Generative Adversarial Network) Model

With the rapid development of information technology, the transmission of information has become strategic. To prevent information from children, information security must be assessed. Therefore, the art of concealing information has become a popular solution. In particular, the reversible data concealment (RDH) technique uses the symmetrical method of transferring and processing symmetrical data in the carrier envelope. Not only can undetected and fully-recognized secret information be transmitted, but it can also be recovered without any corruption by the media envelope. In addition, encryption techniques can protect your email service and your information privately. However, the vector is an encrypted form of ciphers, which has a strong likelihood of attracting attackers. Counter-generative Networks (GANs) generate encrypted images for RDH signaling. The network architecture is designed for a four-phase test, including a hidden network.

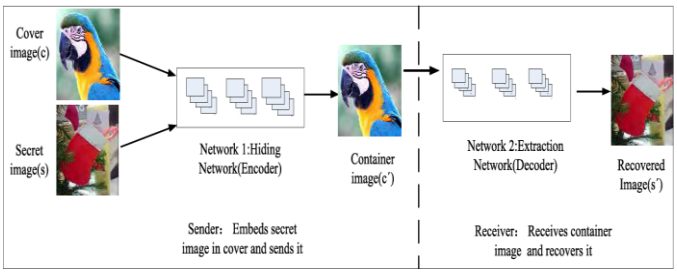


Fig.4. Architecture of GAN

A GAN network architecture is similar to a U-Net network structure in terms of its parameter settings. There are two phases in the hidden network: a contraction phase and an expansion phase. Convolutional neural networks typically have a shrinking phase. Instead of the U-Net network output, this one has a 6-channel 256x256 cascade function tensor input that is supplemented by a 4x4 convolution layer after each down sampling. In order to speed up the training of the network, each convolution is followed by a LeakyReLU activation function and a batch normalization operation. The leakage rule and batch normalization level are used in the no-function model to increase network speed

Leaky Relu:- It is a Relu based activation function. This function runs the gentle slope for negative values instead of converting them to a regular slope. A Leaky Corrected Linear Scale or Leaky ReLU could be a type of trigger operation supported by Relu; However, negative values indicate a gentle slope rather than a flat slope. In addition, the increase constant is determined before the coaching, e.g. no learning takes place during the coaching. Leaky ReLU runs an improved version of the ReLU activation tool. For ReLU activation work, the gradient is zero for all non-zero input values, which could disable the neurons in the region and should cause the ReLU feedback to die. Leaky ReLU was developed to address this disadvantage. Instead of a ReLU activation process acting as zero for negative input values (x), we tend to represent it as a small linear element of x.

f(x)=max (0.01*x , x).

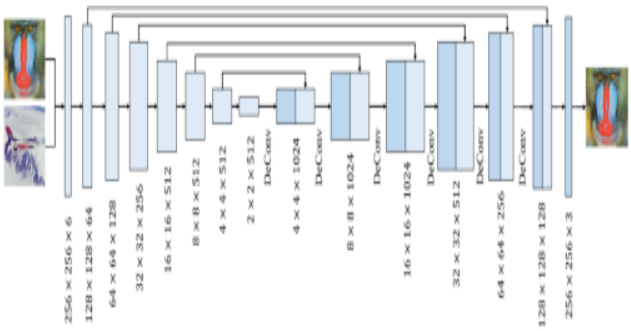
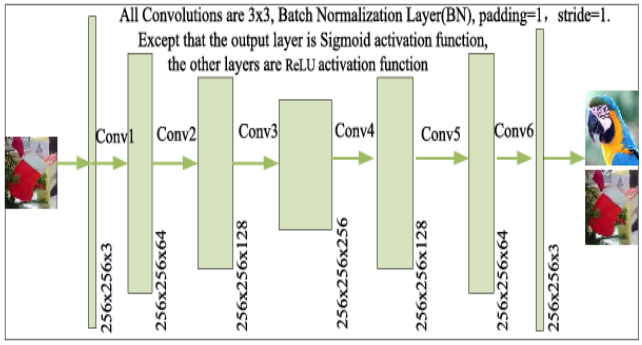


Fig.5. Hiding Architecture of GAN

There is a contraction phase and an expansion phase in the hidden network. Convolutional neural networks typically have a shrinking phase. The U-Net network input is a cascaded 256x256 six-channel functionality tensor, which is further enhanced during down sampling by four-channel convolutions. A LeakyReLU activation function and a batch normalization operation follow each convolution to speed up the network training process. Every time a down sampling step is performed, the number of functional channels is doubled. The number of main channels after seven down sampling operations is 512, and the feature map is 2 × 2. Oversampling the feature map with a deconvolution level (DeConv) smooths the number of main channels in the dilation step. As a result, all oversampling operations are cascaded with the feature map from the reduction stage.



Information can be accurately retrieved from hidden networks using an extraction network architecture. At CNN, the task operation, the activation function, and the pooling level are used to improve the nonlinear learning ability of the neural network. The hidden network, the designed network, has six layers of convolution. CNN is used to learn fitting parameters using nonlinear capabilities. At each level of the network, weight parameters are learned to adjust the mapping between inputs and outputs. The effects of CNN are similar to those of linear multivariate equations if the non-linear operations are ignored

Pearson Correlation Coefficient

Correlation: The correlation coefficient expresses the ratio between the produced images and the original (uncompressed). ρ was calculated as the Pearson Correlation Coefficient (CSP) between images.

Mathematical Formulation

1. Encoding Formula

$$Yi = Ek (Xi),$$

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

The sizes of Xi and Yi are identical.

2. 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

3. An illustration's peak signal to noise ratio (PSNR) represents the ratio between the maximum power of a picture and the power of corrupting noise that affects its quality.

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

4. An expert's Mean Square Error (MSE) or Mean Square Deviation (MSD) measures the common error squares, i.e., the common square difference between calculable worth and true value. The first moment of the square error loss is my favorite moment in this risky operation.

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

5. SSIM- Structure similarity (SSIM) index for grayscale image or volume A mistreatment referee because of the reference image or volume. A worth nearer to one indicates higher image quality.

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

6. Pearson Correlation Coefficient

The Pearson method is widely used in statistical analysis, pattern recognition, and image processing. In this case, the applications include two images displayed in one image file.

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

7. Embedding Capacity

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

Dataset Used

http://www.vision.caltech.edu/datasets/

Caltech101 with 101 different types of objects and 50 images per class

Software requirement specification

Python

Spyder Software

Hardware requirement specification

Laptop

IV.EXPERIMENTAL RESULTS

1. Main Option for Users

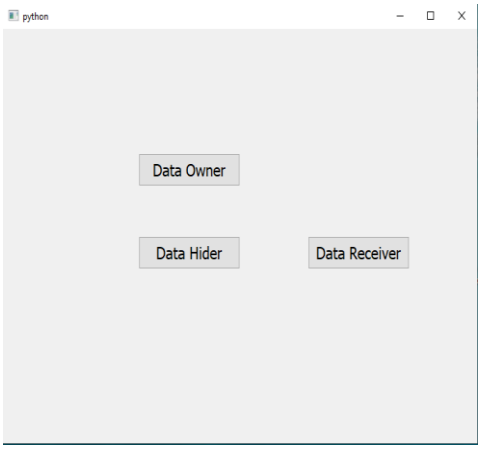


Fig.7. Main Window of Project

Fig.7 shows the Project's Main Window, where the Data owner, Data hider, and Data receiver can log in for a further operation

2. Calculation of Embedding Capacity

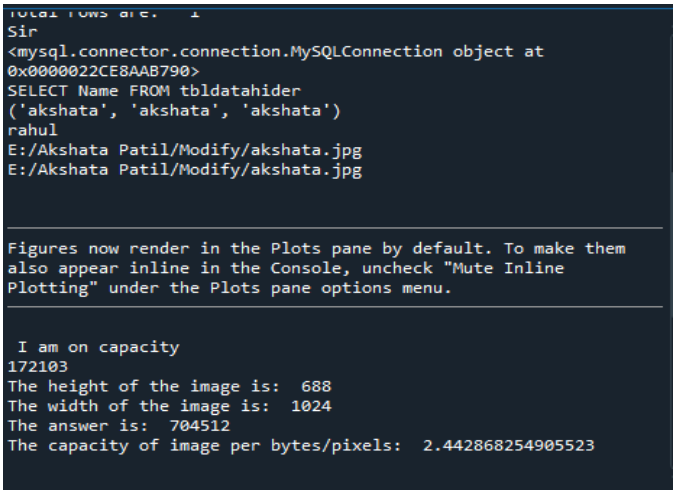


Fig.8. Calculation of Embedding Capacity

Fig.8 shows the embedding capacity of the image per bytes/pixels.

2. Image creation for camouflage

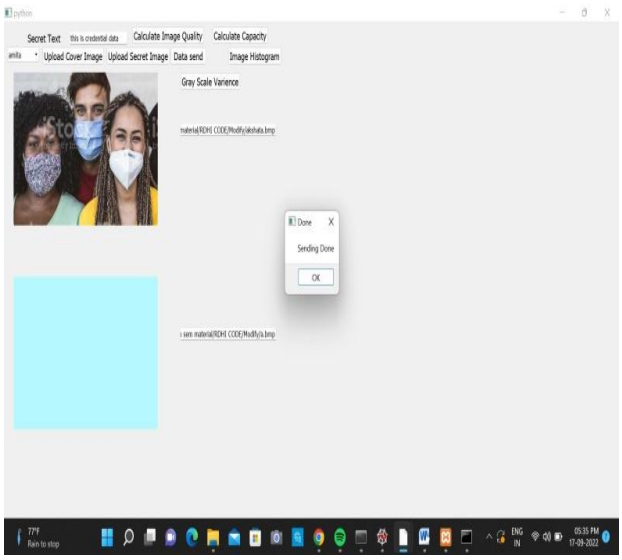


Fig.9. Creation of Camouflage Image

The figure shows the creation of a camouflage image with secret and cover pictures and the entry of the encrypted file name by the data hider. Due to the reversibility of the technique, we combine the two images into a single image

4. Decryption of Information

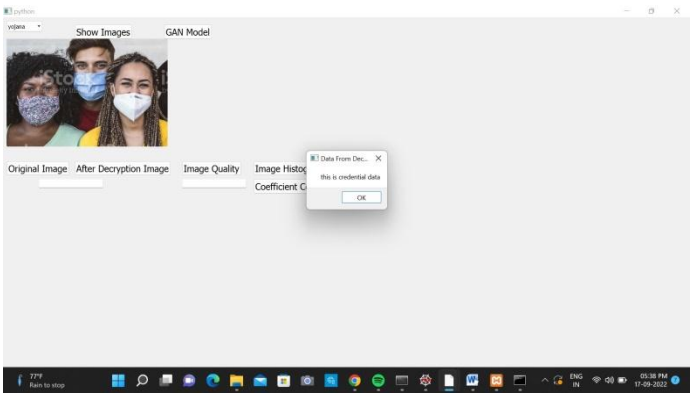


Fig.10. Decryption of Information

The receiver can decrypt the authorized file as shown in Fig.10. To decrypt the file, we use a network of encoders and decoders

5. GAN Model Evaluation

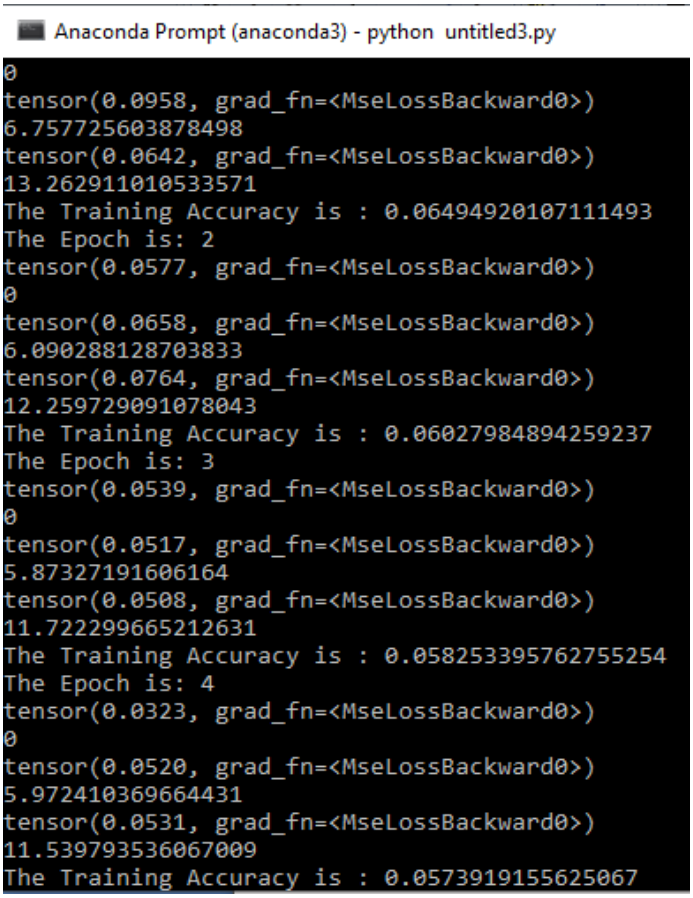


Fig.11. GAN Model Evaluation

Fig.11 Shows the GAN Model evaluation and iteration.

6. Metrics for evaluating image quality

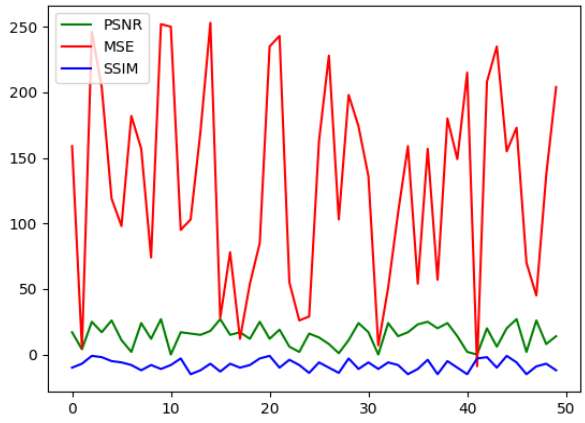


Fig.12 This chart shows PSNR, MSE, and SSIM as Image Quality Evaluation Metrics.

Table -1: Evaluation Metrics.

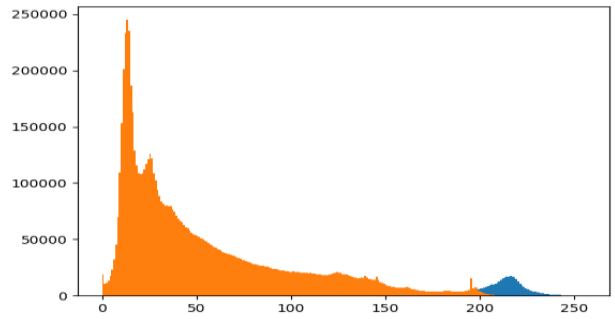
Image Name	PSNR	MSE	SIM
Me.jpg	28.84	254.60	0.89
Devscript.jpg	30.37	178.83	0.86
Test.jpg	39.10	23.96	0.98
Test1.jpg	39.93	19.78	

Table1. Evaluation Metrics.

8. Image Histogram before Encryption

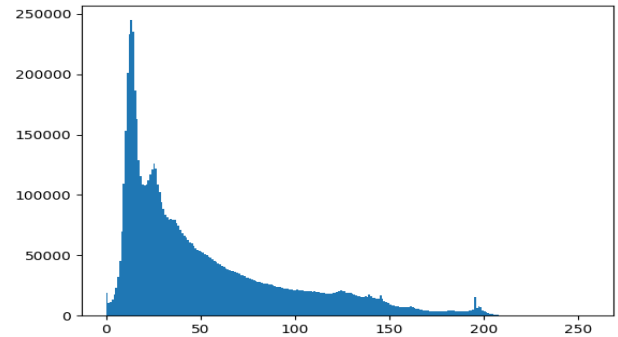
Like alternative histograms, a picture's histogram also shows frequency. Picture bar graphs, however, show the frequency of pixels' intensity values. A picture bar graph shows gray level intensities on the x-axis, and their frequency on the y-axis.

This bar chart shows the variation in pixel values on the x-axis. It's an eight-bit image, so there are 256 levels of gray in it. As a result, the x-axis ranges from zero to 255 with a spot of fifty between them



A count of these intensities can be found on the y axis. The graph shows that almost all of the bars with high frequencies are within the half portion, which is darker. Meaning that the image we've got is darker. And this may be tested from the image too.

9. Image Histogram after decryption



10. Gray Scale Variance

Using the color image process leads to 2 main factors; Foreground color can be a robust descriptor that makes it easier to spot and extract objects from a scene. Second, a man recognizes thousands of shades of color and intensity compared to 24 shades of gray. In the RGB model, each color appears in its main spectral components, red, neutral, and blue. This model is based on the Cartesian coordinate system. Images drawn in the RGB color model contain 3-element images. One for each primary, when these three phosphorescent screen images are fed into the associated RGB screen, they combine to provide a composite color image. The number of bits representing each element in the RGB package is called element depth. Consider an RGB image assigned in degrees where each of the blue color images has no experience with an 8-bit image.

Fig.15 shows the gray scale variance.

11. Co-Efficient Correlation

Fig.16. Co-Efficient Correlation

Fig16 Shows the Co-Efficient relation between images.

3. CONCLUSIONS

Using reversible image transformation (RIT), we present a reversible data concealment framework (RDC-EI). Unlike previous frameworks that encoded plaintext images into ciphertext, this one encodes plaintext images into ciphertext. Embedding an image into another shot protects the privacy of the image. Thus, encrypted photos have some of the same shapes as plain text images. Data encryption and decryption were performed using CNN and GAN models in this paper. This technique begins with embedding capacity. Minimizing iterations and improving accuracy are achieved using Self GAN.

REFERENCES

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

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

[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 were 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