International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 07, July 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Reversible Data hiding in Encrypted Images using Deep Neural Network and GAN Model

Akshata A. Patil [1], Dr. J.E. Nalavade [2]

[1,2] *Computer Science and Engineering,*

Rajarambapu Institute of Technology, Rajaramnagar (India)

[1]*akshatapatil2596@gmail.com*

[2]*jagannath.nalavade@ritindia.edu*

Abstract

Nowadays, photos area unit shared through social media and that we got to security of photos. Thus we'd like to use coding and steganography technique in order that we will hide the key message in to the image and the other way around. Within the planned system we have a tendency to apply lossless reversible technique for embedding and extracting the info. Reversible information concealing may be a technique wherever we will infix secret data into cowl image by slightly modifying the pixel values. During this paper we have a tendency to gift a replacement methodology of mixing the model like convolution neural network and generative adversarial networks to get the meaningful encrypted pictures for RDH. Four-stage specification is intended for the experiment, together with the concealing network, the encryption/decryption network, the extractor, and therefore the recovery network. Within the concealing network, the key information area unit embedded into the image through residual learning. 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 and thus the hidden message totally extracted on the receiving aspect. The many applications like social control, Medical application as an example 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 to calculate the embedding capability of image and finding the standard of image exploitation SSIM.

Keywords- *Data Hiding, Deep Neural networks, GAN model.*

I. INTRODUCTION

Digital pictures square measure wide utilized in media, publishing, medicine, military, and other fields. Therefore, it's necessary to save the copyright and integrity of digital pictures. Because the image itself has the characteristics of an enormous quantity of knowledge, high correlation, and high redundancy between pixels, it cannot be wont to write the image with the common text encoding formula. On top of functions, varied technologies are developed for pictures, like image authentication and watermarking. As a branch of digital watermarking technology, knowledge concealment could be an important technology to ensure the security of counseling.

Knowledge concealment may be enforced in many alternative ways to realize the aim of useable embedding of secret knowledge. Depending on whether or not the receiver will recover the quilt image, knowledge Concealment may be divided into two types: irreversible knowledge concealment and reversible knowledge concealment. Data concealing in the footage may be a way by which the initial cowl can lossless recover once the embedded messages unit of measurement is extracted e.g., image data, labels, notations, or authentication info into the encrypted pictures while not accessing the initial contents.

We propose a Reversible Image Transformation (RIT) framework. RIT-based frameworks shift the content of the first image to the content of the canopy image and therefore defend the privacy of the first image, and changeableness means they'll be lossless reconditioned from the reworked image. Thus RIT is often viewed as a special secret writing theme, known as "Semantic Transfer secret writing (STE)".Because the camouflage image is a kind of plaintext, it'll avoid the notation of the outsiders, and therefore the outsiders will simply implant further knowledge into the camouflage image with ancient RDH strategies for plaintext pictures.

Reversible information concealing within the encrypted image (RDHEI) becomes a hot topic, and a great deal of algorithms are projected to optimize this technology. However, these algorithms cannot deliver the goods robust embedding capability. Thus, during this paper, we have a tendency to propose a sophisticated RDHEI theme supported lossless element conversion (LPC). Totally different from the previous RDHEI algorithms, LPC is galvanized by the coplanar map coloring question, and it performs a dynamic image division method to divide the initial image into irregular regions rather than regular blocks as within the previous RDHEI algorithms. Within the method of LPC, element conversion is performed by region; that's, pixels within the same regions are reborn to an equivalent conversion values, which is able to occupy a smaller size, and so the accessible area is reserved to accommodate further information. LPC may be a process; therefore the original image is lossless recovered on the receiver facet.

II. RELATED WORK

Weiming Zhang ET. Al aims to enhance the scheme proposed that was different from previous strategies that encrypt a target image into a cowl image. Reversible image transformation supported reversible image transformation that transfers the linguistics of the original image to the linguistics of another image and shields the privacy of the first image with the same size. By Reversible image transformation, and restoring the first image from the encrypted image in an exceedingly lossless and secure modified approach. 2 RDH strategies together with PEE-based RDH and UES area unit adopted to insert further information within the encrypted image to satisfy different wants on image quality and embedding capability [1]

Zhenxing Qian et added paper proposes a scheme of reversible records hiding in encrypted pix with the use of dispensed supply coding. After encrypting the authentic photograph bits of MSB planes are decided on and compressed to make room for the extra mystery records.

On the receiver side, hidden records are extracted with the embedding key only, and the authentic photograph is recovered with excessive best the use of the encryption key only. When each of the embedding and encryption keys is to be hard to the receiver, the hidden records may be extracted absolutely, and the authentic photograph recovered perfectly [2]

In this paper, Xiaochun Cao et al projected a unique technique referred to as the HC_SRDHEI, that inherits the deserves of RRBE, and also the reparability property of RDH strategies in encrypted pictures. Compared to progressive alternatives, are vacated for knowledge concealment by our technique is far larger used? The knowledge information} hider merely adopts the element replacement to substitute the offered room with further secret data. The information extraction and canopy image recovery area unit is severable, and the area unit is freed from any error. Experimental results on 3 datasets have incontestable that our average MER will reach one.7 times as massive because the previous best different technique provides. The performance analysis implies that our projected technique encompasses an excellent potential for sensible applications. [3]

Xinpeng Zhang proposed paintings that propose lossless, reversible, and mixed record hiding schemes for cipher-textual content pix encrypted through public-key cryptography with probabilistic and homomorphism properties. In the lossless scheme, the cipher textual content pixel values are changed with new values for embedding the extra records into the LSB-planes of cipher textual content pixels. This way, the embedded records may be immediately extracted from the encrypted domain, and the records embedding operation does now no longer affect the decryption of the unique plaintext image. In the reversible scheme, a preprocessing of histogram reduce is made earlier than encryption, and a 1/2 of cipher textual content pixel values are changed for records embedding. On the receiver side, data may be extracted as a plaintext manner. [4]

In this J. Malathi, fashion a stable reversible picture data concealing (RICH) topic operated over the encrypted domain. It shows a public key modulation mechanism, that lets North American u.s.a plant the data through clean XOR operations, even as now no longer the need of getting access to the important thing encoding key. At the decoder aspect, advised to apply a robust two-elegance SVM classifier to discriminate encrypted and non-encrypted picture patches, sanction active North American u.s.a together decipher the embedded message, and consequently the unique picture sign dead [5]

III. PROPOSED SYSTEM

To develop a system that implements camouflage images that allows the users to embed additional data, into the camouflage images without accessing the original contents, the original image is required to be perfectly recovered without any loss and the hidden messages completely extracted on the receiving side without any distortion.

Proposed Architecture:

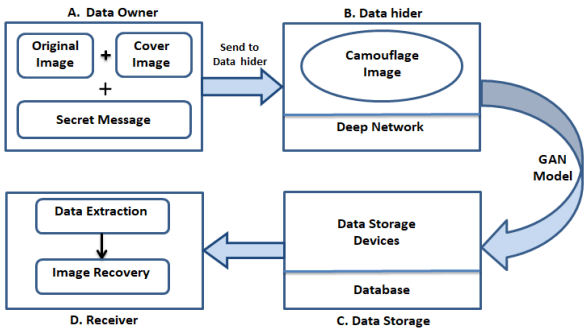

Fig.1. Proposed Architecture

Modules

The system has the following modules.

A. Data Owner

B. Data Hider

C. Data Storage Devices

D. Receiver

Data Owner

The data owner area takes care of that

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: Stored (maybe external) additional information on camouflage images can be located using any RDH display to open images 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 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.

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

Objective of the System

1. To embed the additional data (Text/Audio) into the camouflage images inreversible & lossless mode.
2. To improve the quality of camouflage image
3. To embed and extract the data from the image with the help of deep neural network.
4. To generate GAN (Generative Adversarial Network) for achieving the real time steganography.
5. To recover the original plaintext image without any error.

Method of Implementation

1. Lossless Reversible Data hiding

Reversible data hiding (RDH) is a method which covers data and recovered original data afterward the embedded data is removed. It is an imperative method which broadly used in medical, military and law forensics

imagery. where no distortion of the unique cover is acceptable. meanwhile first presented, RDH has involved substantial investigation attention.

RDH Embedding

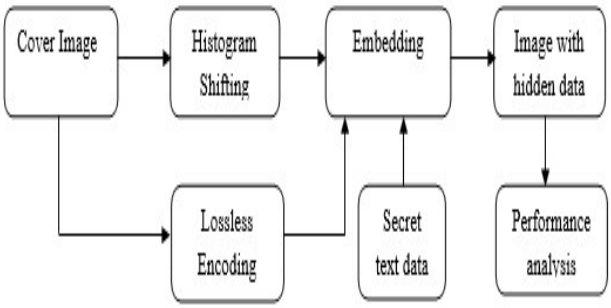

Fig.2. RDH Embedding

RDH Extraction

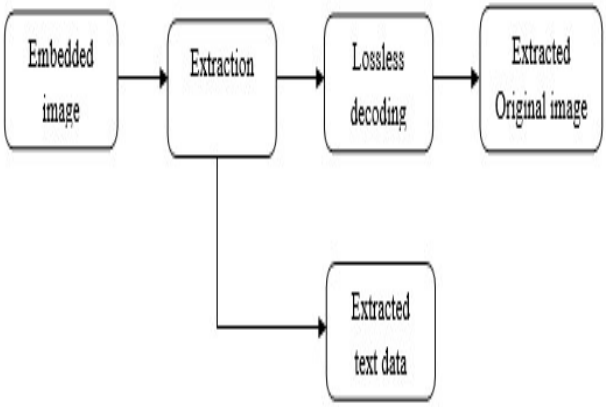

Fig.3. RDH Extraction

2. GAN(Generative Adversarial Network) Model

With the rapid development of information technology, the transmission of information has become strategic. To prevent information of children, information security must be assessed. Therefore the art of concealing information has become a popular solution. The reversible data concealment (RDH) technique, in particular, uses symmetrical method of transferring and processing symmetrical data in the carrier envelope. Not only can undetected and fully-recognized secret information be transmitted, it can also be recovered without any corruption by the media envelope. In addition, the 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.

Pearson Correlation Coefficient

Correlation: The ratio between the produced images and the original (uncompressed) is expressed by the correlation coefficient. 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.

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.Peak Signal Noise Relation (PSNR) is that the ratio between the utmost attainable power of a picture and also the power of corrupting noise that affects the standard of its illustration.

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

4.Mean square Error (MSE) or Mean square Deviation (MSD) of AN expert measures the common of error squares i.e. the common square distinction between the calculable worth's and true value. It's a risk operate, love the first moment of the square error loss.

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

5.SSIM- Structure similarity (SSIM) index for grayscale image or volume A mistreatment referee because 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 object 50 images per class

Software requirement specification

- Python
- Spyder Software

Hardware requirement specification

- Laptop

IV. EXPERIMENTAL RESULTS

1. Main Option for Users

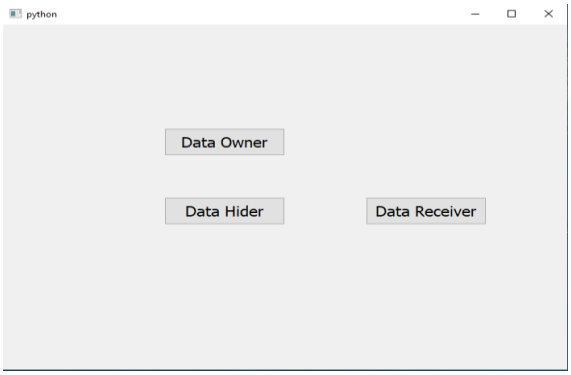

Fig.4. Main Window of Project

Fig.4 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

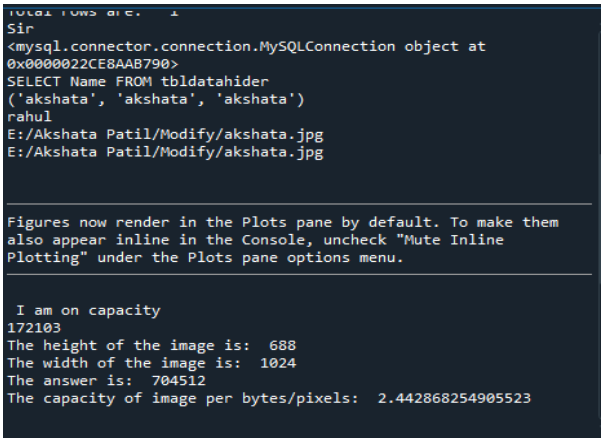

Fig.5. Calculation of Embedding Capacity

Fig.5 Shows embedding capacity of image per bytes/pixels.

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 07, July 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

3. Creation of Camouflage Image

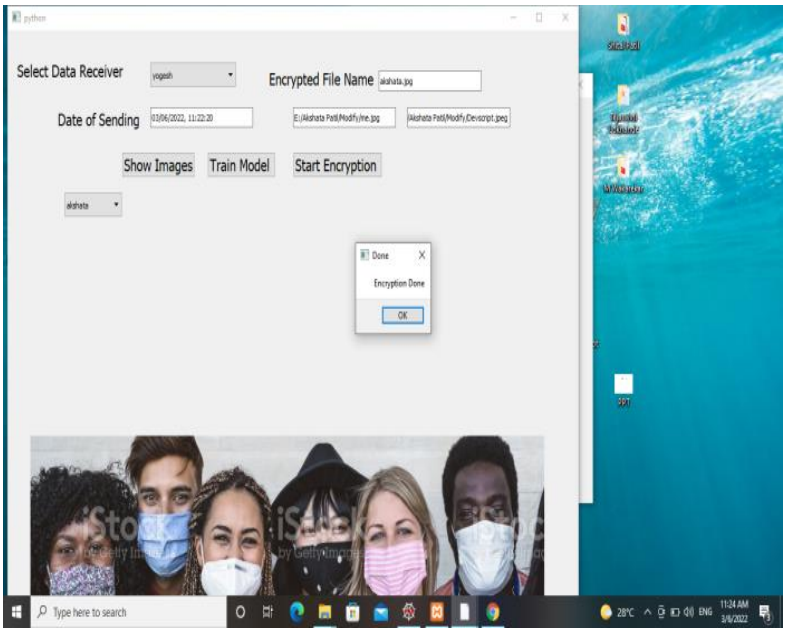

Fig.6. Creation of Camouflage Image

Fig.6 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

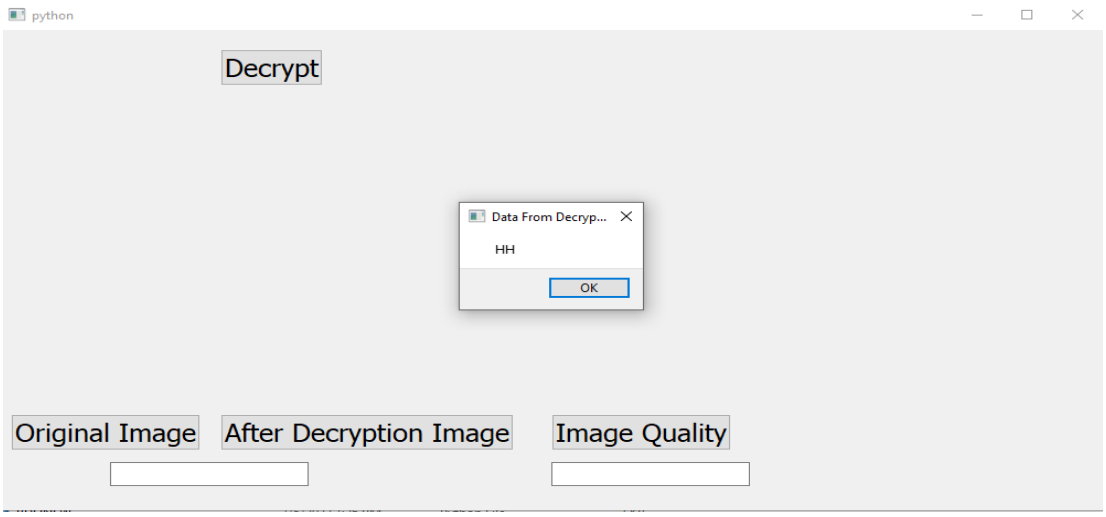

Fig.7. Decryption of Information

Fig.7 show that the receiver can decrypt the authorized File. Here we use an encoder and decoder network for decryption purposes.

International Journal of Advance Research in Science and Engineering
Volume No. 11, Issue No. 07, July 2022
www.ijarse.com
IJARSE
ISSN 2319 - 8354

5. GAN Model Evaluation

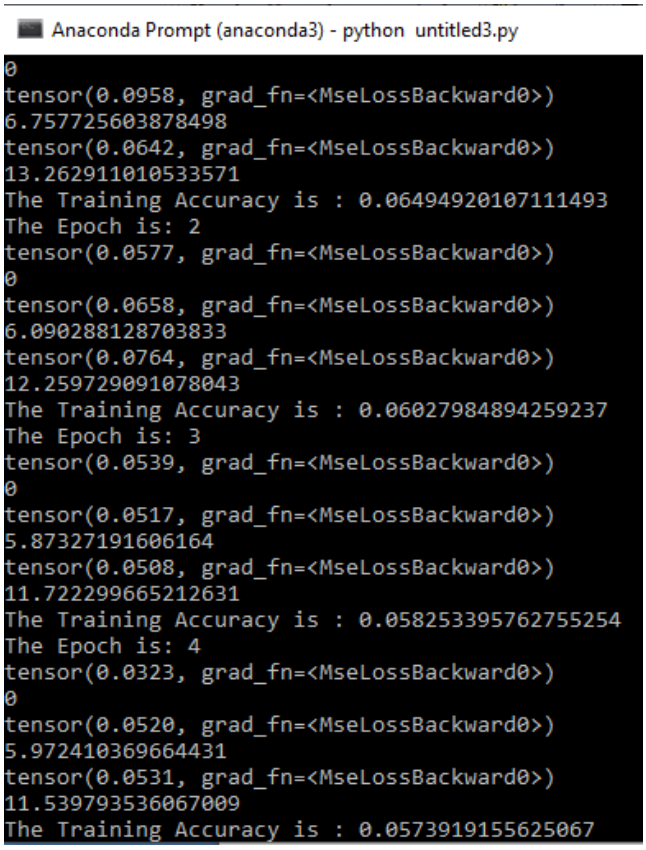

Fig.8. GAN Model Evaluation

The Fig.8 Shows the GAN Model evaluation and iteration

6. Image Quality- Evaluation Metrics

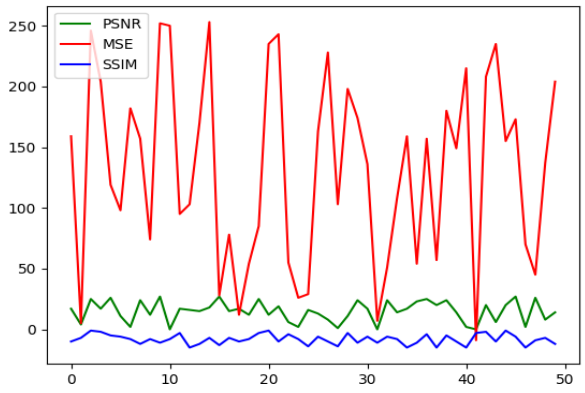

Fig.9. Image Quality –Evaluation Metrics.

The Fig.9 Shows the Image Quality- Evaluation Metrics of PSNR, MSE and SSIM.

7. Evaluation Metrics

Image Name	PSNR	MSE	SSIM
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

Histogram of a picture, like alternative histograms conjointly shows frequency. However a picture bar graph shows frequency of pixels intensity values. In a picture bar graph, the x axis shows the grey level intensities and therefore the y axis shows the frequency of those intensities

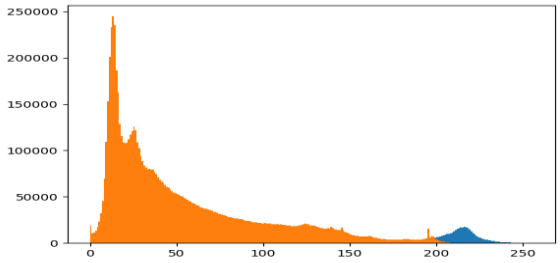

Fig.10. Image Histogram before Encryption

The x axis of the bar chart shows the vary of pixel values. Since its associate degree eight bpp image, meaning it's 256 levels of grey or reminder grey in it. That's why the vary of x axis starts from zero and finish at 255 with a spot of fifty. Whereas on the y axis, is that the count of those intensities. As you'll see from the graph, that almost all of the bars that have high frequency lays within the half portion that is that the darker portion. Meaning that the image we've got is darker. And this may be tested from the image too.

9. Image Histogram after decryption

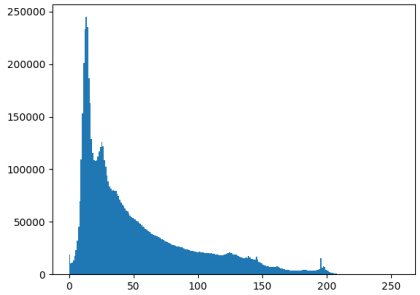

Fig.11. Image Histogram after Decryption

10. Gray Scale Variance

Using the color image process leads to 2 main factors; Foreground color can be a powerful 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 3 phosphorescent screen images are fed into the associated RGB screen, they combine to provide a composite color image. The number of bits that represent each element in the RGB package is commonly referred to as element depth. Consider an RGB image assigned in degrees where each of the blue color images has no experience on an 8-bit image

Fig.12. Gray Scale Variance

The Fig.12 shows the gray scale variance.

11. Co-Efficient Correlation

Fig.13. Co-Efficient Correlation

The Fig13 Shows the Co-Efficient relation between images.

CONCLUSION

In this paper, we have tested a unique framework for reversible data concealment in the encrypted image (RDC-EI) supported reversible image transformation (RIT). It is different from the previous frameworks that encode a plaintext image into a cipher text type. It embeds one image into another image so it defends the privacy of the image. As a result, encrypted images have some of the shapes of plain text images. This paper used the CNN and GAN Model with RDH scheme to encrypt and decrypt the data. In this technique we first calculate the embedding capacity. In this Self GAN model is used for the purpose of minimizing the iterations and improve the accuracy.

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.