International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 19-26

Reversible Data Hiding Using MSB Prediction

Yojana J. Patil
Prof .Powar P.S
Computer Science and Engineering
Ashokrao Mane Group Of Institution vathar, Kolhapur, India.

ABSTRACT:-
Nowadays, outsourcing photos to cloud and sharing photos through social media is additional and fashionable those at identical time build it difficult to guard the privacy of photo's homeowners. for example, recently several non-public photos of Hollywood actor leaked from iCloud. There are a unit 2 common approaches, secret writing and knowledge activity, to guard image contents from outflow. Though secret writing solves the privacy downside, however the untidy codes of cipher text with special type area unit straightforward to cause the eye of attackers WHO can conceive to jailbreak the accounts of secret writing users.
Data activity technology embeds message into covers like the image, audio or video, that not solely protects the content of secret file, however additionally hides the communication method itself to avoid the attacker's attention. There are unit 2 varieties of knowledge activity, Reversible, and Non- reversible. Reversible knowledge activity in pictures may be a technique by that the initial cowl will losslessly recover when the embedded messages area unit extracted e.g., image data, labels, notations or authentication info into the encrypted pictures while not accessing the initial contents. The initial image is needed to be utterly recovered and therefore the hidden message fully extracted on the receiving facet. several applications like enforcement, Medical application as an example keeping patient's info secret, a military application wherever the physical property of secret hidden knowledge is of high demand. Also, this application needs lossless recovery of the initial image and thus the requirement of changeability.
Keywords—: Deep Hiding, GAN Model, Deep Neural Network

Date of Submission: 28-04-2022 Date of acceptance: 09-05-2022

I. INTRODUCTION

Digital pictures square measure wide utilized in media, publishing, medicine, military, and other fields. Therefore, it's necessary to safe the copyright and integrity of digital

pictures. Because the image itself has the characteristics of 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. For 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 absolutely recover the quilt image, knowledge Concealment may be divided into two types: irreversible knowledge concealment and reversible knowledge concealment (RDH).

Data concealing in footage may be a way by that the initial cowl can losslessly recover once the embedded messages unit of measurement extracted e.g., image data, labels, notations or authentication info into the encrypted pictures while not accessing the initial contents. The initial image is needed to be utterly recovered and therefore the hidden message fully extracted on the receiving aspect. several applications like enforcement, Medical application as an example keeping patient's info secret, a military application wherever the invisibleness of secret hidden knowledge is of high demand. Also, this application needs lossless recovery of the initial image and hence the requirement of changeableness.

We propose a framework of Camouflage of Image by Reversible Image Transformation (RIT). RIT-based frameworks shifts the content of the original image to the content of cover image and thus protect the privacy of the original image, and reversibility means that they can be lossless restored from the transformed image. Therefore RIT can be viewed as a special encryption scheme, called "Semantic Transfer Encryption (STE)".Because the camouflage image is in a form of plaintext, it will avoid the notation of the outsiders, and the outsiders can easily embed additional data into the camouflage image with traditional RDH methods for

plaintext images.

II. LITERATURE REVIEW

In this paper authors aims to enhance scheme of proposed "Reversible information concealing in writes image supported reversible image transformation" [1] that was totally different from previous strategies that encrypt a target image into cowl image. Reversible image transformation supported reversible image transformation that transfer the linguistics of original image to the linguistics of another image and shield the privacy of the first image with same size. as a result of the encrypted image has the shape of a plaintext image, it'll avoid the notation of the curious cloud server and it's free for the cloud sever to settle on one among RDH strategies for plaintext pictures By Reversible image transformation, and restore the first image from the encrypted image in an exceedingly lossless and in secure approach. 2 RDH strategies together with PEE-based RDH and UES area unit adopted to insert further information within the encrypted image to satisfy totally different wants on image quality and embedding capability.

In this Paper authors [2] projected "Lossless and Reversible knowledge concealment in Encrypted pictures with Public Key Cryptography" [2] With these schemes, the picture element division/reorganization is avoided and therefore the encryption/decryption is performed on the quilt pixels directly so the number of encrypted knowledge and therefore the procedure complexness are lowered. Thanks to knowledge embedding on encrypted domain might end in a touch bit distortion in plaintext domain thanks to the homomorphism property, the embedded knowledge may be extracted and therefore the original content may be recovered from the directly decrypted image. With the combined technique, a receiver might extract a section of embedded knowledge before coding, and extract another part of embedded knowledge and recover the first plaintext image once coding.

In this paper authors [3] planned a unique "Reversible image knowledge concealment (RIDH) theme over encrypted domain". the info embedding is achieved through a public key modulation mechanism, that permits United States to introduce the info via straightforward XOR operations, while not accessing the key cryptography key. At the decoder aspect, a robust two-class SVM classifier is intended to tell apart encrypted and non- encrypted image patches, permitting United States to conjointly decipher the embedded message and also the original image signal. The planned approach provides higher embedding capability and is ready to utterly reconstruct the initial image likewise because the embedded message.

In this paper authors [4] aims to enhance scheme of "Reversible Data Hiding in Encrypted Images Using Slepian-Wolf Distributed Source Encoding", which was galvanized by DSC? Once the initial image is encrypted by the content owner employing a stream cipher, the knowledge-hider compresses a series of chosen bits taken from the encrypted image to form spare area to accommodate for the key data. With 2 completely different keys, the planned technique is severable. The hidden knowledge may be fully extracted victimization the embedding key, and therefore the original image may be just about reconstructed with prime quality victimization the secret writing key. If the receiver has each the embedding and secret writing keys, receiver will extract the key knowledge and absolutely recover the initial image. The planned technique achieves a high embedding payload and sensible image reconstruction quality and avoids the operations of room-reserving by the sender.

In this paper Ling Du, Xingxing Wei, Dan Meng, Xiaojie Guo [5] proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separability property of RDH methods in encrypted images for a better relation between neighbor pixels, we propose consider the patch-level sparse representation when hiding the secret data. Compared to state-of-the-art alternatives, the room vacated for data hiding. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. The data extraction and cover image recovery are separable, and are free of any error. Experimental results on three datasets shows that the proposed method has average MER can reach 1.7 times as large as the previous best alternative method provides. The performance analysis implies that proposed method has a very good potential for practical applications.

III. PROPOSED SYSTEM

To develop a system which implement camouflage images which 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.

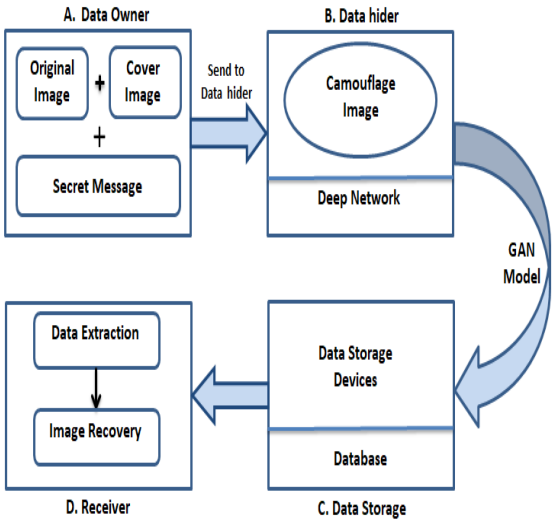

Figure 1. Proposed System Architecture

Modules

The system is proposed to have the following modules along with functional requirements.

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

1. Data Owner

Data owner section deals with

a. Choosing image as Input: Color image is taken as the original cover image

b. Choosing Cover Image as Input: Color Image is taken Cover Image for Input Image.

c. Secret Text:- Secret Message to be Embed in the Image

Data Hider

Data Hider section deals with

a. Encryption of Data: Secret data to be embedded in image concealed the camouflage image. Camouflage image with secret data so formed is passed as an input to the, Data storage device. Next Module is data storage device module

Data Storage Device

Data Storage devices section deals with

a. Data Embedding: The storage devices (may be outsiders) can embed additional data into Camouflage image by using any classical RDH method of plaintext images.

b. Data Removing: The Storage devices (may be outsiders) can extract additional data from Camouflage image 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

Receiver can be either the content owner or any authorized person for decryption.

a. Image decryption: Camouflage image so formed from the data hider is received by the receiver. Image is decrypted and data is recovered.

IV. RESULTS

1. Main Window

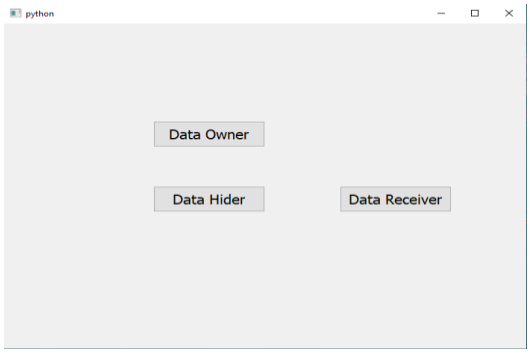

Figure 2. Main Window of Project

The Figure 2 Shows the Main Window of Project where owner, hider, receiver can login for further operation

2. Data Owner Registration

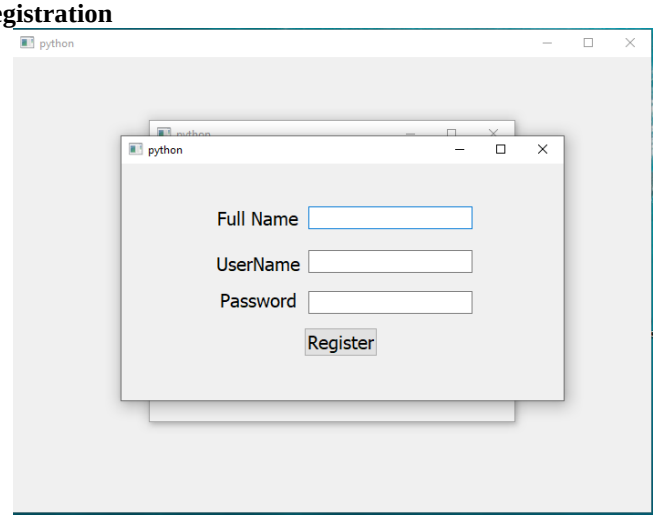

Figure3. Data Owner Registration

The Figure 3 Shows the Data Owner Registration where data owner can enter the details.

3. Data Owner Data in the Database

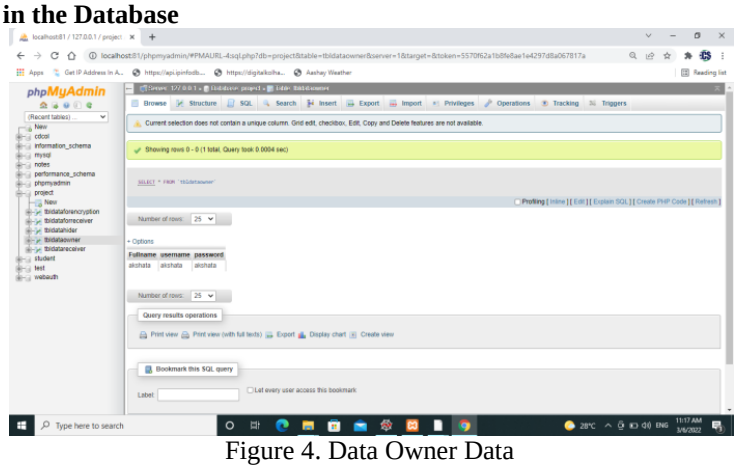

Figure 4. Data Owner Data

The Figure 4 Shows the Data Owner Data is saved into the MYSQL Database.

4. Data Owner Login

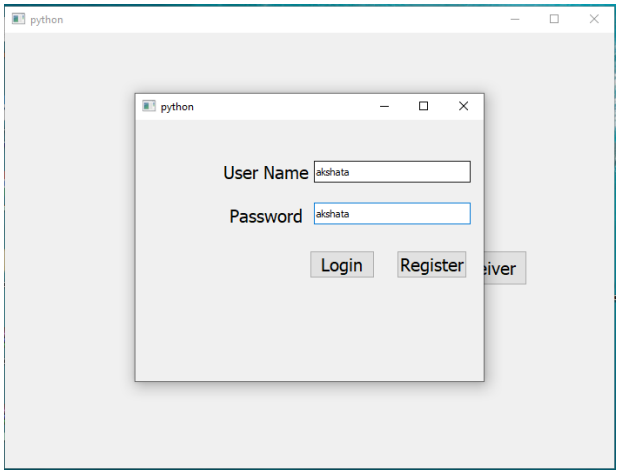

Figure 5. Data Owner Login

The Figure 5 Shows the Data Owner can login with credentials.

5. Data Owner Dashboard

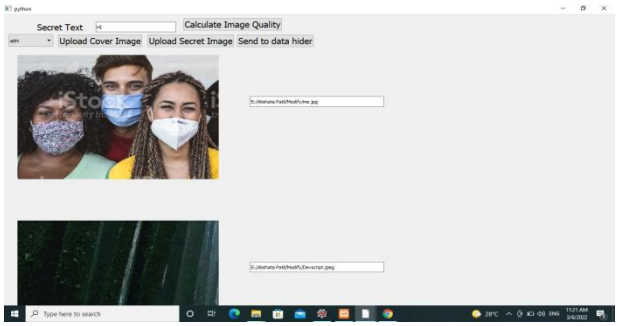

Figure 6. Data Owner Dashboard

The Figure 6 Shows the Data Owner dashboard where owner can select secret plus cover image and enter the sensitive text and send to data hider.

6. Data Hider Login

The Figure 7 Shows the encrypted file is saved in the folder with the given name.

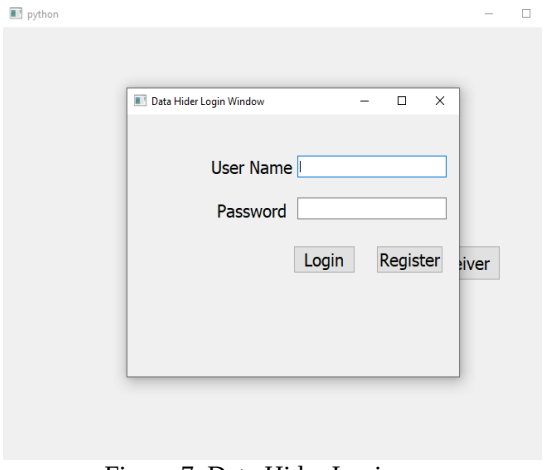

Figure 7. Data Hider Login

The Figure 7 Shows the Data hider Login with credentials.

7. Creation of Camouflage Image

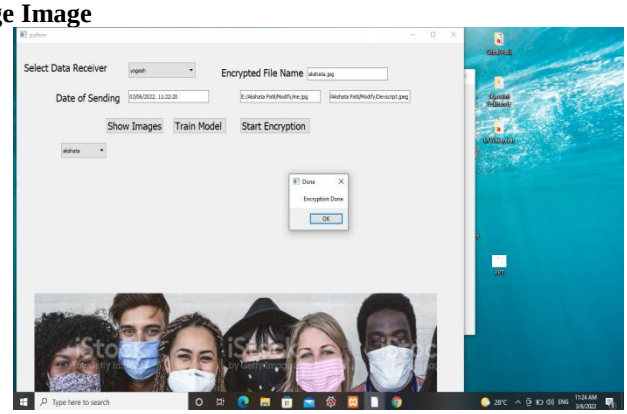

Figure 8. Creation of Camouflage Image

The Figure 8 Shows the creation of camouflage image with secret and cover image and also data hider enter encrypted file name.

8. Encrypted File Name

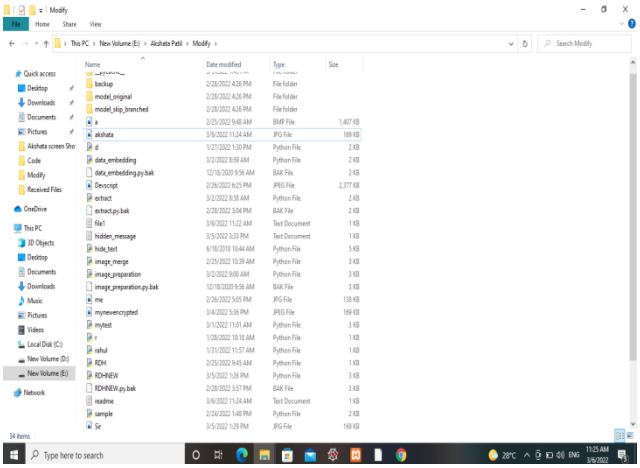

Figure 9. Encrypted File Name is saved

9. Data Receiver Login

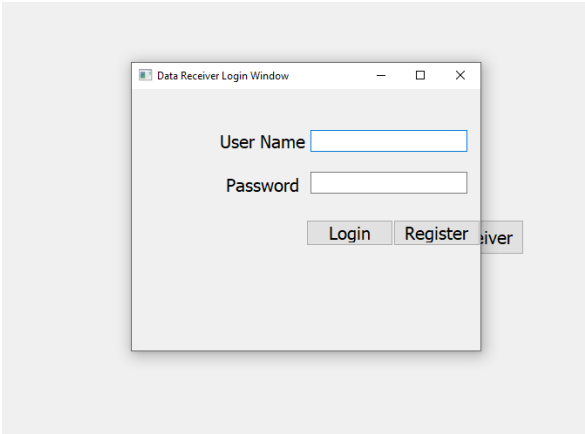

Figure 10. Encrypted File Name is saved

The Figure 10 Shows that receiver can login with credentials

10. When Receiver Select Unauthorized File

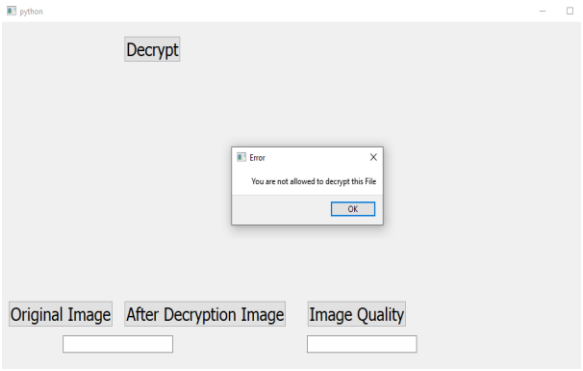

Figure 11. Unauthorized File Selection

The Figure 11 shows that when receiver select any unauthorized file that time system does not give access to decrypt the file.

11. Data Decryption

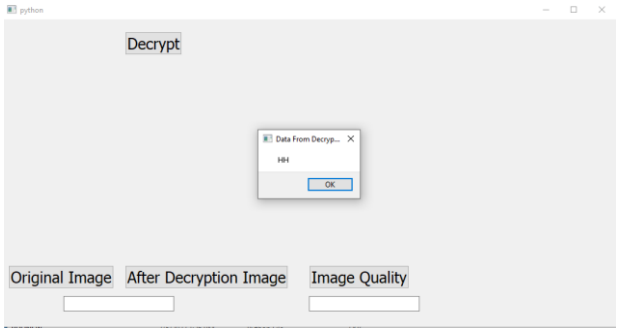

Figure 12. Data Decryption

The Figure 12 shows that receiver can decrypt the authorized File.

12. Showing Quality of Image with PSNR

Figure 13. PSNR Quality

In the figure 13 Shows the PSNR Quality of image means MSE of image is zero.

13. Selection of Image

Figure 14. Selection of Image

The Figure 14 shows that Selection of image for quality checking.

V. CONCLUSION

In this paper we tend to propose a unique framework for reversible data concealment in encrypted image (RDH-EI) supported reversible image transformation (RIT). Totally different from previous frame- works that encode a plaintext image into a cipher text type, RIT-based RDH-EI shifts the linguistics of original image to the semantic of another image and therefore defend the privacy of the original image. as a result of the encrypted image has the shape of a plaintext image, it'll avoid the notation of the curious cloud server and it's free for the cloud sever to settle on anyone of RDH strategies for plaintext pictures to engraft watermark.

REFERENCES

[1]. Donghui Hu , Shengnan Zhou, Qiang Shen, Shuli zheng ,Zhongqiu Zhao, And Yuqi fan(IEEE) March 8, 2019 “Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning” IEEE Access VOLUME 7,2019 pp.25924-25935.

[2]. Nandhini Subramanian, Omar Elharrouss, Somaya AL-Maadeed, Ahmed Bouridane “Image Steganography: A Review of the Recent Advances” IEEE Access VOLUME 9,2021 pp.23409-23423.

[3]. Xintao Duan, Kai Jia, Baoxia Li, Daidou Guo, En Zhang, AND Chuan Qin ” Reversible Image Steganography Scheme Basedon a U-Net Structure” IEEE Access VOLUME 7,2019 pp.9314-9323.

[4]. Nandhini subramanian, ismahane cheheb “End-to-End Image Steganography Using Deep Convolutional Autoencoders” IEEE Access VOLUME 9,2021 pp.135585-135593.

[5]. Xintao duan , daidou guo , nao liu , baoxia li , mengxiao gou, and chuan qin “A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network” IEEE Access VOLUME 8,2020 pp.25777- 25788.

[6]. Weiming Zhang, Hui Wang, Dongdong Hou, Nenghai Yu, “Reversible Data Hiding in Encrypted Images by Reversible Image Transformation,” IEEE Trans. on multimedia, August 2016.

[7]. Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, “Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography,” IEEE Trans. on Circuits and Systems for Video Technology, 2015.

[8]. Jiantao Zhou, Weiwei 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, no. 3, pp. 441-452, Mar. 2016.

[9]. Zhenxing Qian, and Xinpeng Zhang, “Reversible data hiding in encrypted image with distributed source encoding,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[10]. Xiaochun Cao, Ling Du, Xingxing Wei, et al., “High capacity reversible data hiding in encrypted images by patch-level sparse representation,” IEEE Trans. On Cybernetics, vol. 46, no. 5, pp 1132-1143, May.