Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.3, December : 2024

SECURE AND REVERSIBLE DATA EMBEDDING IN ENCRYPTED IMAGES USING DEEP LEARNING AND GENERATIVE ADVERSARIAL NETWORKS

Mrs Dipali R.Surana, Department of Computer Engineering, K.C.T Late G.N.Sapkal College of Engineering, Nashik, India
Prof. (Dr.) Nilesh R. Wankhade, Department of Computer Engineering, K.C.T Late G.N.Sapkal College of Engineering, Nashik, India

ABSTRACT

These days, uploading images on social media and outsourcing photos to the cloud are both trendy and extra, making it challenging to protect the privacy of the photo's owner. For instance, a number of private images of a Hollywood actor were recently stolen from iCloud. To prevent the outflow of picture contents, there are two prevalent ways in Unit 2: hidden writing and knowledge activities. While secret writing addresses the issue of privacy, the messy cipher text codes with unique font are easily spotted by attackers who might potentially breach the accounts of secret writing users.

Data activity technology inserts messages into covers such as images, sounds, and videos. This conceals the communication mechanism itself from the attacker and safeguards the content of hidden files. Reversible and non-reversible knowledge activities are available in unit 2. Reversible knowledge activity in images refers to a method whereby the original image content is preserved even after embedded messages, such as labels, annotations, or authentication information, are recovered from encrypted images without affecting the original contents. To fully extract the concealed message on the receiving side, the original image must be entirely restored. a number of uses, including law enforcement, the medical field (where patient information is kept confidential, for example), and the military, when the physical possession of highly sought-after secret knowledge is needed. Additionally, changeability is required for this application since it requires lossless recovery of the original image.

Keywords:
Deep Hiding, GAN Model, Deep Neural Network

I. INTRODUCTION

Digital images are widely used in the publishing, journalism, medical, military, and other areas. Consequently, it's essential to protect digital image integrity and copyright. 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. A variety of technologies, such as watermarking and image authentication, being created for photos in addition to their intended uses. 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. Knowledge concealment can be classified into two categories: irreversible knowledge concealment and reversible knowledge concealment (RDH), depending on whether the recipient would definitely recover the quilt image.

Data hiding in video may provide a means by which the original cover can be restored without loss of quality provided the embedded messages—such as image data, labels, annotations, or authentication information are recovered from the encrypted images without gaining access to the original contents. To fully extract the concealed message on the receiving end, the original image must be entirely recovered. a number of uses, including law enforcement, the medical field (where patient information is kept confidential, for example), and the military, where the ability to conceal secret

information is highly valued. Additionally, this program requires changeableness because it requires lossless recovery of the original image.

We suggest a Reversible Image Transformation (RIT) paradigm for image camouflage. Reversible image transformation techniques, or RIT-based frameworks, allow for the lossless restoration of the original image by shifting its content to that of the cover image, protecting the original image's privacy. As a result, RIT can be thought of as a unique encryption method known as "Semantic Transfer Encryption (STE)".Given that the camouflage image is in plaintext, outsiders cannot easily notate it, and they can simply insert further data into the image using standard RDH techniques for plaintext images.

II. LITERATURE REVIEW

The paper titled[1] "Digital Image Steganalysis Based on Visual Attention and Deep Reinforcement Learning" by Donghui Hu, Shengnan Zhou, Qiang Shen, Shuli Zheng, Zhongqiu Zhao, and Yuqi Fan, published in *IEEE Access* on March 8, 2019 (Volume 7, pp. 25924-25935), focuses on enhancing digital image steganalysis using a novel approach that combines visual attention mechanisms with deep reinforcement learning (DRL) Traditional approaches either use feature-based methods (which require manual feature extraction) or deep learning techniques that may not fully utilize image patterns effectively

The paper *"Image Steganography: A Review of the Recent Advances"* by Nandhini Subramanian, Omar Elharrouss, Somaya AL-Maadeed, and Ahmed Bouridane, published in *IEEE Access* (Volume 9, 2021),[2] provides a comprehensive review of recent advancements in the field of image steganography. The authors focus on various techniques, methods, and trends that have emerged over recent years, detailing both the fundamental principles and cutting-edge innovations

The paper titled "Reversible Image Steganography Scheme Based on a U-Net Structure" by Xintao Duan, Kai Jia, Baoxia Li, Daidou Guo, En Zhang, and Chuan Qin, published in *IEEE Access*, Volume 7 (2019),[3] presents a novel steganography technique using a U-Net-based architecture for embedding secret data into images in a reversible manner.The proposed method allows both the embedding and recovery of secret data while perfectly restoring the original cover image, a key feature of reversible steganography

The paper titled "End-to-End Image Steganography Using Deep Convolutional Autoencoders"[4] by Nandhini Subramanian and Ismahane Cheheb, published in IEEE Access, Volume 9, 2021 (pp. 135585-135593), focuses on a novel method for image steganography using deep learning techniquesThe paper presents an end-to-end image steganography framework that utilizes deep convolutional autoencoders (DCAE) to hide a secret image inside a cover image. This approach differs from traditional steganographic techniques, which rely on statistical or mathematical manipulations. Instead, the model learns directly from the data

The paper titled "A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network" [5]by Xintao Duan, Daidou Guo, Nao Liu, Baoxia Li, Mengxiao Gou, and Chuan Qin introduces an innovative approach to image steganography by combining elliptic curve cryptography (ECC) and deep neural networks (DNN)The paper proposes a new image steganography method that focuses on increasing the capacity of data that can be hidden within images while ensuring strong encryption and protection of hidden data through cryptographythe paper presents a cutting-edge approach that leverages modern cryptographic and machine learning techniques to overcome the limitations of traditional steganography methods.

In contrast to earlier methods that encrypt a target image into a cowl image, the authors of this study want to improve the proposed "Reversible information concealing in writes image supported reversible image transformation" [6].

Supported by reversible image modification, this feature preserves the anonymity of the original image while transferring its content from one sizeable image to another. Because the encrypted image resembles a plaintext image, it will evade the notice of the inquisitive cloud server and the cloud server

can use any RDH strategy for plaintext images. Through reversible image transformation, the first image can be securely and completely restored from the encrypted image. Two RDH techniques, namely PEE-based RDH and UES, were utilized to incorporate additional data into the encrypted picture in order to meet distinct requirements for image quality and embedding capacity.

"Lossless and Reversible knowledge concealment in encrypted pictures with Public Key Cryptography" is the title that authors [7] projected in this paper. By avoiding the separation or restructuring of picture elements, these techniques conduct encryption and decryption directly on the quilt pixels, hence reducing the number of encrypted knowledge and the procedural complexity. Because of the homomorphism property, knowledge embedding on an encrypted domain may result in a touch bit distortion in the plaintext domain; however, the embedded knowledge may be retrieved, allowing the original content to be recovered from the directly decrypted picture. Using the combined method, a recipient might retrieve the first plaintext picture after coding, extract another portion of embedded knowledge, and extract a portion of embedded knowledge prior to coding.

A novel "Jiantao Zhou, Weiwei Sun, Li Dong, et al., “Secure reversible image data hiding over encrypted domain via key modulation" was planned by the authors [8] of this study. The information is embedded through the use of a public key modulation method, which prevents the United States from acquiring the cryptographic key and allows the country to introduce the information by simple XOR operations. In order to distinguish between encrypted and non-encrypted image patches at the decoder side, a strong two-class SVM classifier is used, enabling the United States to simultaneously decode both the embedded message and the original image signal. Because of the embedded message, the planned solution has a higher embedding capability and is prepared to completely reconstruct the original image.

The purpose of this study, written by authors [9], is to improve the DSC-galvanized method of "Reversible Data Hiding in Encrypted Images Using Slepian-Wolf Distributed Source Encoding." After the content owner encrypts the original image using a stream cipher, the knowledge-hider compresses a number of selected bits extracted from the encrypted image to provide space for the important data. It is possible to separate the proposed technique with two entirely different keys. Through the use of the embedding key, the hidden knowledge may be fully recovered, allowing the secret writing key to nearly reconstruct the original image in high quality. The recipient will extract the key information and unquestionably retrieve the original image if they possess both the embedding and secret writing keys. The planned method avoids the sender's room reservation activities while achieving a high embedding payload and reasonable image reconstruction quality.

In order to improve the relationship between neighbor pixels in encrypted images, Ling Du, Xingxing Wei, Dan Meng, and Xiaojie Guo [10] proposed a novel method called the HC_SRDHEI. This method takes into account patch-level sparse representation when hiding secret data, while also inheriting the benefits of RRBE and the separability property of RDH methods. The space freed up for data concealing was superior to cutting-edge alternatives. The data hider merely uses the pixel replacement technique to fill in the extra secret data that would otherwise be available. There are no errors in the data extraction or the cover picture recovery, which may be done separately.

The suggested method's average MER can reach 1.7 times as great as that of the previous best alternative method, according on experimental results on three datasets. Based on the performance research, it appears that the suggested strategy has excellent potential for real-world implementations.

The paper titled "An Adaptive Steganography Approach for Live Video Streams Based on Edge Analysis and Frame Variability" by Sushma R B and Majula B.R (2023)[11] proposes a novel steganographic method designed specifically for live video streams. The main objective of the paper is to enhance the security and efficiency of hidden data transmission within video streams, leveraging edge detection and frame analysis to adaptively conceal information.

The paper titled *"Robust Steganographic Algorithm based on Wavelet Transform"* [13]by Cătălin Rizea, Călin Bîră, and Mihai Stanciu discusses the development of a new robust steganographic algorithm that utilizes wavelet transforms. Steganography is a method of concealing information

within other non-secret data to prevent detection, commonly used in digital imagesThe paper introduces a wavelet-based steganographic technique that enhances robustness and imperceptibility. The algorithm primarily focuses on embedding secret data within the high-frequency components of an image after applying the wavelet transform

Deep Neural Network and GAN-Based Reversible Data Hiding in Encrypted Images: A Privacy-Preserving Approach[21]2023focuses on developing a secure method for embedding data into encrypted images while maintaining privacy. The primary goal is to leverage advanced machine learning techniques, such as Deep Neural Networks (DNNs) and Generative Adversarial Networks (GANs), to implement Reversible Data Hiding (RDH). RDH allows secret data to be embedded into an image and then extracted later, while also enabling the original image to be fully restored after data extraction

Nilesh R Wankhade, Ujwalla H Gawande,Need of fundus image analysis: [22]a review2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT),1348-1353Publisher,IEEEFundus image is the evidance of the most of the eye diseases like diabetic retinopathy, gloucoma, hyper tension, etc. As diabetic retinopaty is a asymtotic disease, It is very important to analyse the fundus image regularly to avoid blindness. This paper presents different, methods and algorithms used in the automated detection of Diabetic Retinopathy. Many researchers propose different approaches for automated Diabetic Retinopathy identification using image processing methods, and this paper deals with the analysis of various methods available for automated diagnosis which have been recently introduced.

III. PROPOSED SYSTEM

To create a system that uses camouflage images and allows users to embed extra data into the images without accessing the original contents, the original image must be fully recovered without any loss and the hidden messages must be fully extracted on the receiving side without any distortion

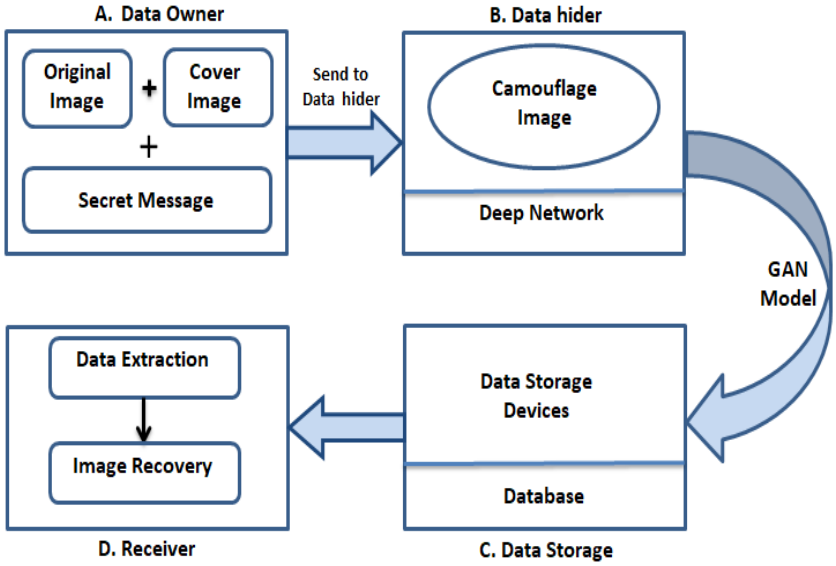

Figure 1. Proposed System Architecture

MODULES

The following modules, along with the necessary functional requirements, are suggested for the system.

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

1. Data Owner

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.3, December : 2024

The section on data owner's addresses
Selecting an image to be entered:
a. The original cover image is a color image.
b. Selecting the Cover Image as the Input: The Color Image is used as the Cover Image.
Secret Text: A Hidden Message Embedded in the Picture

2. Data Hider

A is covered in the Data Hider section. Data Encryption: Secret data was inserted into the camouflage image to conceal it. The disguised image with the secret data in this format is sent as an input to the data storage device. The next module is the data storage device module.

3. Data Storage Device

The section on data storage devices addresses

a) Data Embedding: Using any traditional RDH technique for plaintext images, the storage devices (which could be external parties) can embed more data within the camouflage image.
b) Data Removal: Using any traditional RDH method of plaintext pictures, storage devices (which may be external parties) can extract additional data from a camouflage image. The receiver receives the created camouflage image together with extra data as an input.

4. Receiver

The recipient may be the content's owner or someone else with the authority to decrypt it:

a) Picture decryption: The receiver receives the camouflage image that was produced by the data hider. The image is decoded and the data is recovered.

GAN Model: -

GAN is a four-stage encoding decoding architecture. GAN has its own encoding and recovery architecture so the speed is increases. The encryption/decryption network, the extractor, and the recovery network. In the extractor, 100% of the secret data are extracted through the residual learning framework, same as the hiding network. Lastly, in the recovery network, the cover image is reconstructed with the decrypted image and the retrieved secret data through the convolution neural network. GAN's most advanced method of neural networks. In this we are having two main neural networks that is generator and discriminator.

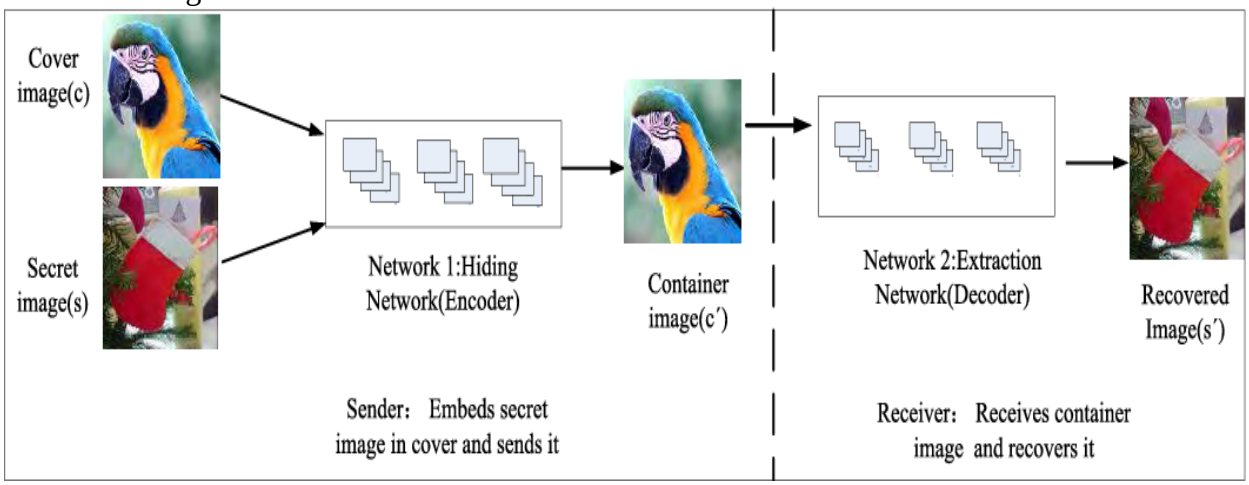

Figure 2. Architecture of GAN

The specific network architecture parameter settings are similar with the U-Net network structure; the hiding network has a contraction phase and an expansion phase. The contraction phase is a typical convolution neural network structure. At this time, unlike the U-Net network, the input of the network is 256×−256 cascading 6-channels feature tensor, which is completed by a 4×4 convolution layer in each down sampling process. Each convolution is followed by a LeakyReLU activation function and Batch Normalization operation to speed up network training.

IV. CONCLUSION

In order to enable reversible data concealing, we present a novel framework for reversible image transformation (RIT) that is backed by RDH-encrypted pictures in this research. Unlike previous frameworks that encode a plaintext image into a cipher text type, RIT-based RDH-EI protects the privacy of the original image by converting its linguistics to the semantic of another image. Since the encrypted image seems like a plaintext image, the curious cloud server won't discover it. The cloud server can use any RDH algorithm to engraft a watermark on plaintext photos.

V.REFERENCES

1. onghui 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 2015.
11. Sushma R B,Majula B.R “An Adaptive Steganography Approach for Live Video Streams Based on Edge Analysis and Frame Variability”2023
12. jiate liu,yun cao”Channel Attention Image Steganography With Generative Adversarial Networks”2022
13. Cătălin Rizea; Călin Bîră; Mihai Stanciu”Robust Steganographic Algorithm based on Wavelet Transform Wavelet Transform”Uses wavelet transformation to enhance robustness against attacksThis paper proposes a new robust algorithm for hiding information in the visual information of images,2022
14. 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 The Discrete Cosine Transform(DCT) is used to transform the secret image, and then the transformed image is encrypted by Elliptic Curve Cryptography(ECC) to improve the anti-detection property of the obtained 2020(IEEE)February 11, 2020.
15. Liu, J., & Cao, Y. (2022). Channel attention image steganography with generative adversarial networks.
16. Harba, E. S., Harba, H. S., & Abdulmunem, I. A. (2021). Advanced intelligent data hiding using video stego and convolutional neural networks.

17. Turing, A., et al. (2016). Reversible steganography using quantum encryption.
18. Anderson, R., et al. (2014). Deep steganography for high-resolution images.
19. Ghasemi, B., et al. (2012). High capacity steganography based on genetic algorithms.
20. Puech, W., et al. (2008). Data hiding in encrypted images using reversible watermarking
21. Jagannath Nalawade,",Deep neural network and GAN based reversible data hiding-Privacy preserving Approach,2023
22. Nilesh R Wankhade, Ujwalla H Gawande,Need of fundus image analysis: a review2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT),1348-1353Publisher,IEEE