e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

IMAGE STEGANOGRAPHY FOR ENHANCED SECURITY USING CNN

Chaitali Rane[*1], Vaishnavi Tambe[*2], Shafali Gupta[*3], Nikita Rathod[*4], Manasi Renuse[*5]

[*1,2,4,5]SPPU, Computer, RMD Sinhgad School Of Engineering, Warje, Maharashtra, India.

[*3]Professor, SPPU, Computer, RMD Sinhgad School of Engineering, Warje, Maharashtra, India.

ABSTRACT

As there is large advancements in internet technology, there has been huge text as well as multimedia data transfer over the internet. Due to this data security is a vital necessity. Various sensitive data is shared over the insecure channel, making it prone to hacking and external threats. Information hiding plays an important role in authentication. As Cryptography alone is not that secure, so we use Steganography along with cryptography to enhance security. For the first level of security we use CNN algorithm for encryption of the information and hash code which is generated by MD5 hashing algorithm for authentication. Then the cipher text and hash code are embedded in the image using LSB steganography algorithm for the second level of security. Then the image is fragmented into multiple parts for the third level of security, so that if a hacker retrieves the message he will only get partial text. After transmission the receiver receives the message, they reverse the process to obtain the information and they can also authenticate the message using hash code. This way triple security is achieved for safe transmission of data.

Keywords: CNN, Partitioning Algorithm, Image, Visual Secret Sharing Scheme.

I. INTRODUCTION

Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages. It is evidenced in situations where communication is established between two parties over an insecure medium which can be easily eavesdropped. The modern encryption frameworks are broadly classified into two groups which are symmetric and asymmetric encryption algorithms. This classification is based on the role of the keys in each algorithm. The symmetric encryption algorithms (SEA), also called secret-key encryption (SKE) require both the message sender and the receiver to be in possession of a common secret key for encrypting and decrypting the message. The asymmetric encryption algorithms, also called public key encryption (PKE), require both the message sender and the receiver to two keys in which one key is available to the public while the other is a private one [1]. The symmetric algorithm proven its worth and importance and its ability to serve the purpose and survive to the recent days. Preserving the goals of consistent confidentiality & integrity of messages and data to be transferred and Data on rest [2]. Hash cryptography is a technique that does not use a key. Instead, a fixed-length hash value is computed based on the plaintext which makes it impossible to be recovered for either length of the plaintext or the contents [3].

Steganography is the technique of hiding secret data within a file. The file can be image, audio or video [4]. LSB technique is applied to embed the encrypted data into the base image [5]. This technique applies XOR operation between the secret data to be hidden and the LSB of the image pixel value. The result is embedded in the least significant bit of the base image [5]. The human visual system cannot recognize the variation in the base image since the overall shift is insignificant. Due to its simplicity and low degradation in image quality, this algorithm is highly recommended [5].

Visual Cryptography (VC) is a technique that encrypts a secret image into n shares, with each participant holding one or more shares. Anyone who holds fewer than n shares cannot reveal any information about the secret image. Stacking the n shares reveals the secret image and it can be recognized directly by the human visual system [6]. Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in noncomputer-aided environments; however, devices with computational powers are ubiquitous.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:12/December-2024 Impact Factor- 8.187 www.irjmets.com

II. LITERATURE SURVEY

In this paper [1], Steganography, the practice of hiding data in digital media, is evolving with deep learning (DL) techniques to enhance security. This review explores current methods, their advantages and challenges, and highlights the potential for advancing secure communication.

In this paper [2], Steganography is a method of securely hiding messages within a cover image to protect sensitive information. This review discusses various techniques, including the Discrete Cosine Transform (DCT), RSA, Blowfish, and hash-least significant bit (LSB) approaches. It introduces a novel method that minimizes image bit variance for enhanced security, combined with cryptography to encrypt data before embedding it. Multiple hashing algorithms further strengthen security by encrypting and decrypting the steganographic images, ensuring safe data transmission even if intercepted.

In this paper [3], This review explores image steganography, focusing on securing data through hidden communication in digital images, a widely used medium. It highlights various methods' strengths and weaknesses, emphasizing the importance of enhancing techniques to protect information from unauthorized access in the dynamic landscape of secure communication.

In this paper [4],This study introduces a novel adversarial attack method for deep steganography (DS), targeting both white-box and black-box scenarios. Unlike existing methods, it not only detects covert communications but can also modify or remove hidden images. Experimental results on Tiny ImageNet and MS COCO datasets show that the attack maintains high image quality while successfully altering or deleting secret content..

In this paper [5], This study proposes a cancer classification method using ensemble learning and particle swarm optimization for feature selection on microarray datasets. The method achieves high accuracy, with 100% for leukemia, 92.86% for colon, 86.36% for breast cancer, 100% for ovarian, and 85.71% for central nervous system cancer, outperforming existing methods and improving baseline ensemble techniques by 12%.

In this paper [6], This work introduces an attention-guided GAN for coverless image steganography, which modifies only specific regions of images, preserving their original features. This approach prevents distortion in crucial areas, maintaining the accuracy of disease diagnosis while still embedding hidden information.

In this paper [7],This project explores image steganography, focusing on embedding hidden images using spatial domain techniques. It aims to enhance understanding of steganography's effectiveness for data protection and information security, highlighting its capabilities, limitations, and potential applications..

In this paper [8],This study introduces a new steganography scheme using Henon map particle swarm optimization (HMPSO) and distinction disparity value (DDV) to address challenges in security, imperceptibility, and capacity. The method includes four phases: preprocessing, embedding, extraction, and validation, ensuring robust confidentiality and integrity with high evaluation performance based on metrics like SSIM, PSNR, and chi-square tests..

In this paper [9], This paper introduces a novel chaotic oscillator for designing a robust image cryptosystem, addressing multimedia data security challenges. The cryptosystem is tested across various metrics, including randomness, key sensitivity, and resistance to attacks, proving its reliability for IoT applications from image capture to use.

In this paper [10], This article presents a novel medical image steganography method combining quantum walks, chaotic systems, and particle swarm optimization to ensure long-term data security. The approach achieves a payload capacity of 2 bits per byte and maintains high image quality, with an average PSNR of 44.1, making the stego image indistinguishable from the original, even against quantum or digital device attacks.

III. METHODOLOGY

In proposed system, a novel approach is introduced to improve the security of image using CNN and LSB algorithm. An existing sharing technique is subjected to loss of security. On this premise, consider the strategy for (k, n) get to structures by using the (k, k) sharing occurrence on each k-member subset dependent on specific relationship. This methodology will require countless examples as n increments. Therefore, presents partioning calculations to group all the k-member subsets into a few assortments, in which cases of various subsets can be supplanted by just one. The designed scheme is feasible to hide the secrets into image as the

purpose of visual sharing schema. Only the authorized user with the private key can additionally uncover the covered mystery effectively.

IV. CONCLUSION

The use of cryptographic algorithms together with steganography makes it impossible for interceptor to recover the encrypted hidden data as by using this technique no one can even know that data is embedded into the image as there will be no noise created in the cover image. CNN cryptographic algorithm found to be most suitable algorithm in terms of Security, Flexibility, and Encryption performance for the project. LSB found to be the most appropriate Steganography Algorithm as it results in stego-images that contain hidden data yet appear to be of high visual fidelity. Hence this ensures the lossless recovery of the secret image at the receiver end, as it enhances the data embedding capacity and also ensures the security of data at three levels: Steganography, Cryptography, and Transmission by splitting. So, the main objective which is to provide security in information sharing is achieved.

V. REFERENCES

[1] 1Anfal Shihab Ahmed, 2Melad Jader Saeed.,A Deep Dive into Deep Learning-Powered Steganography for Enhanced Security: Review, March-2024

[2] Abdullah Alenizi1 , Mohammad Sajid Mohammadi2 , Ahmad A. Al-Hajji2 and Arshiya Sajid Ansari.,"A Review of Image Steganography Based on Multiple Hashing Algorithm.,15 August 2024

[3] Avantika Bisht1 , Annu Singla2 , Kamaldeep Joshi3.,"A Review on Image Steganography Techniques"07 July 2024

[4] Fangjian Tao 1,2 , Chunjie Cao 1,2,*, Hong Li 1 , Binghui Zou 1,2, Longjuan Wang 1,2 and Jingzhang Sun 1,2.,"Adversarial Attack for Deep Steganography Based on Surrogate Training and Knowledge Diffusion".,: 29 May 2023

[5] Nashat Alrefai1 • Othman Ibrahim1.,"Optimized feature selection method using particle swarm intelligence with ensemble learning for cancer classification based on microarray datasets".,28 February 2022

[6] Ambika 1,*, Virupakshappa 1 and Deepak S. Uplaonkar.,"Deep Learning-Based Coverless Image Steganography on Medical Images Shared via Cloud †"18 January 2024

[7] Pooja Bhatt, Bhavik Pargi, Ritesh Kumar.,"Enhancing Security through Advanced Image Steganography Techniques".,, March, 2024

[8] Ali Salem Ali , 1 Suray Alsamaraee , 2 and Aya Ayad Hussein.,"Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity".,June 2024

[9] Li Li1 , Ahmed A. Abd El-Latif 2,* , Sajad Jafari 3,4, Karthikeyan Rajagopal 5 , Fahimeh Nazarimehr 3 and Bassem Abd-El-Atty.,"Multimedia Cryptosystem for IoT Applications Based on a Novel Chaotic System Around a Predefined Manifold".,January 2022.

[10] Bassem Abd-El-Atty.,"A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks"., September 2022.