Image Steganography For Enhanced Security Using CNN

Chaitali Rane[1], Vaishanavi Tambe[2], Prof. Shafali Gupta[3], Nikita Rathod[4], Manasi Renuse[5]

[1,2,3,4,5]*Department of Computer Engineering, Institute, RMD Sinhgad Technical Institutes Campus*

***Abstract*-Large volumes of text and multimedia material have been transferred via the internet as a result of significant developments in internet technology. As a result, data security is essential. Sharing a variety of sensitive data across an insecure connection exposes it to external threats including hacking. In authentication, information concealment is crucial. Steganography is used in conjunction with cryptography to improve security because cryptography by itself is not very secure. We encrypt the data using an encoding algorithm for the first level of protection. For the second degree of security, the CNN steganography technique is then used to embed the hash code and cypher text into the image. 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**

***Index Terms-Hashing, Partitioning Algorithm, Image, Visual Secret Sharing Scheme*.**

I.INTRODUCTION

The process of secret writing through the encoding and decoding of information is known as cryptography. It is demonstrated in circumstances where two people communicate using an unsecure channel that is susceptible to eavesdropping. The two main categories of contemporary encryption frameworks are symmetric and asymmetric encryption algorithms. The function of the keys in each algorithm serves as the basis for this classification. Both the sender and the recipient of the message must have a shared secret key in order to encrypt and decrypt it using symmetric encryption algorithms (SEA), also known as secret-key encryption (SKE). Both the sender and the recipient of the communication must have two keys for the asymmetric encryption techniques, commonly known as public key encryption (PKE), with one key being private and the other being publicly accessible [1]. The symmetric algorithm has demonstrated its value and significance as well as its capacity to function and endure in the modern day. maintaining the objectives of consistent data integrity and secrecy for both data at rest and messages to be conveyed [2]. An approach that does not require a key is hash cryptography. Rather, the plaintext is used to calculate a fixed-length hash value, which prevents recovery for either the plaintext's length or its contents [3]. Steganography is the process of concealing confidential information in a document. The file may be audio, video, or an image [4]. The encrypted data is embedded into the basic image using the LSB approach [5]. This method uses an XOR operation between the LSB of the image pixel value and the secret data that needs to be concealed. The least important portion of the base image contains the result [5]. Because the overall shift is negligible, the human visual system is unable to detect the modification in the base image. This approach is strongly advised because of its ease of use and minimal loss of image quality [5]. A secret image is encrypted into n shares using the Visual Cryptography (VC) approach, in which each participant has one or more shares. No information about the secret image can be disclosed by anyone with fewer than n shares. The secret image can be directly recognised by the human visual system when the n shares are stacked [6]. Photographs, handwritten documents, pictures, and other forms can all be considered secret images. Another name for exchanging and distributing secret images is a visual secret sharing (VSS) scheme. Although there are several devices with computational capabilities, VC was first motivated by the desire to safely exchange secret photos in noncomputeraided settings.

II. LITRATURE REVIEW

In this paper [1], the primary goal was to examine several approaches to integrating cryptography and steganographic methods to create a hybrid system. Additionally, certain distinctions between steganographic and cryptographic methods were also discussed.

In this paper [2], three common cryptographic algorithms two in symmetric cryptography DES, AES and one in asymmetric cryptography RSA are compared. In this one can simply understand the background history of the algorithm in review and the key functional cipher operation of the algorithm. Accordingly summarizes of strength and weakness of each algorithm under the review is highlight.

In this paper [3],three hybrid encryption techniques are proposed to protect data transfer: symmetric AES is used to encrypt files, asymmetric RSA is used to encrypt AES passwords, and HMAC is used to encrypt symmetric passwords and/or data. MAC is used to safeguard the data or the encrypted key.

In this paper [4], efficient pairing free CP-ABE access control scheme using elliptic curve cryptography has been used for data sharing in sub optimal multimedia applications. Data can be accessed only by specific users that are authenticated by the data owner. Pairing based computation is replaced with scalar product on elliptic curves that reduces the resource and memory requirements for users. The features of both cryptography and steganography are combined by embedding crypto text into an image that enhanced data security, privacy and ownership.

In this paper [5], In order to minimise processing cost, text encryption has been accomplished by combining the Hill cypher with the elliptic curve cryptography technique. Forty percent of the DCT coefficients that are applied to the secret image are embedded in the base image. The DCT coefficients and encrypted data have been embedded into the image using the LSB technique.

In this paper [6], A colour image watermarking algorithm based on Singular Value Decomposition, Discrete Wavelet Transform, and Discrete Cosine Transform (DWT-DCTSVD) is proposed. The host colour image must first be converted from RGB to YUV colour space. After that, the brightness component Y is subjected to a layer of discrete wavelet transform. The low frequency is then separated into blocks using a discrete cosine transform, and SVD is performed on each block. Lastly, add a watermark to the cover photo.

In this paper [7], A novel approach that combines cryptography and steganography is put forth to secure 24 bit colour graphics. This technique hides an image inside another image using a randomised LSB-based approach. Chaotic theory is then used to encrypt the generated stego image. This new integrated approach guarantees improved data hiding capabilities, image security, and lossless secret data recovery. Additionally, it offers the notion of three levels of security: transmission via splitting, cryptography, and steganography.

In this paper [8], In order to conceal a hidden message in both words and images, steganography approaches are compared. In the field of steganography, a number of techniques are employed.

In this paper [9], a novel approach to visual cryptography with the additional capability of authentication based on steganography for hiding digital signature of the secret image was proposed. A new steganography method is used for hiding secret bits in the different blocks of the shares. The method makes no change in the sub-pixels of the shares for hiding binary
„0", but a change is done for hiding binary „1" by flipping a white (black) sub-pixel in one of the blocks of black (white) share The hidden signature can be recovered in the presence of all shares and verified by comparing with the reconstructed digital signature in case of doubt.

In this paper [10], A method of encoding that combines steganography and cryptography is suggested. After completing two stages of data encryption, the encrypted data is concealed within the picture. There are more uses for the image that contains the encrypted text.

III. METHODOLOGY

AES and the LSB method are used in a novel way in the suggested system to increase image security. An existing sharing method could become less secure. Based on this assumption, think about the (k, k) sharing occurrence on each k-member subset depending on a certain relationship as a technique for (k, n) get to structures. Innumerable examples will be needed in n increments for this methodology. In order to aggregate all of the k-member subsets into a few assortments, where cases of different subsets can be replaced by only one, partitioning computations are presented. As the goal of the visual sharing schema, the planned scheme makes it possible to conceal the secrets within the image. Additionally, the covered mystery can only be successfully solved by the authorised user who has the private key.

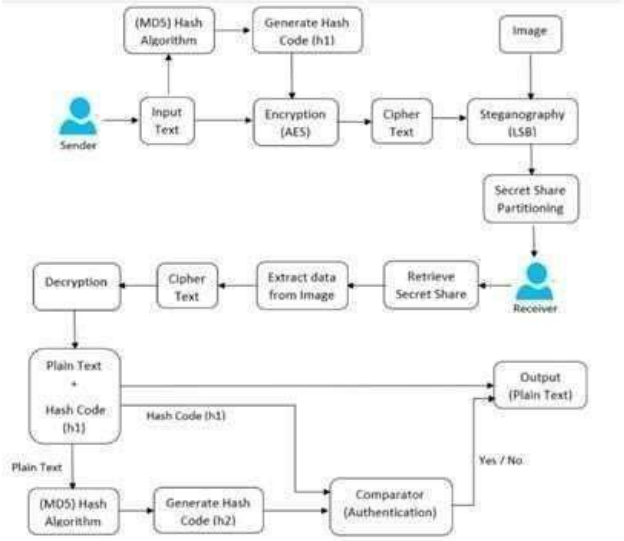


Fig 3.3: System Architecture

3.1 Advantages:

1. Secure and effective text embedding.
2. Uses a sophisticated partitioning method to improve security.
3. Boosts the effectiveness of sharing.
4. High security and increasingly flexible access structures.
5. The cost of processing is lower.
6. The hashing approach can be used to verify the accuracy of messages.

3.2 Algorithm:

3.2.1 Encoding:

One method of spatial domain steganography is LSB (Least Significant Bit). The LSB approach is used to embed data inside cover-media, which is another type of data. A picture, sound, or video might be used as the cover material. To conceal the secret data, 8-bit or 24-bit graphics can be utilised as cover images. The image's most important information is carried by the MSBs of its pixels, while its least important information is carried by the LSBs. Behind the cover image's LSBs (Least Significant Bit), the required number of MSBs (Most Significant Bits) of secret data can be inserted. Since the secret data was embedded into the cover image, the resulting stego image resembles the original cover image. However, the more embedded bits of hidden data there are, the less alike the Cover image and Stego image are [7]. 0 is black, for instance. It will not change much if you change the value to 1 because it is still black, albeit a lighter hue.

The following procedures are used to complete the encoding:

1. Make the picture greyscale.
2. If necessary, resize the picture.
3. Change the message's format to binary.
4. Set the output image to be the same as the input image.
5. Go through every pixel in the picture and take the following actions: The pixel value should be converted to binary. (Ask to embed the following portion of the message. (Make a temp variable. (Set temp = 0 if the pixel's LSB and the message bit match. (Set temp = 1 if the pixel's LSB and the message bit differ. (By taking the XOR of the message bit and the LSB of the pixel, the temperature can be set. The output image's pixel is updated to the input image's pixel value + temperature.
6. Continue to update the output image until every message bit is embedded.
7. Lastly, write both the input and output images to the local system.

3.2.2 CNN

The first layer to extract information from an input image is called convolution. Convolution uses tiny squares of input data to learn visual attributes while maintaining the link between pixels. By adding filters, such as identity, edge, sharpen, box, and Gaussian blur filters, convolution of an image with various filters can accomplish tasks like edge detection, blur, and sharpening.

Layer of Pooling

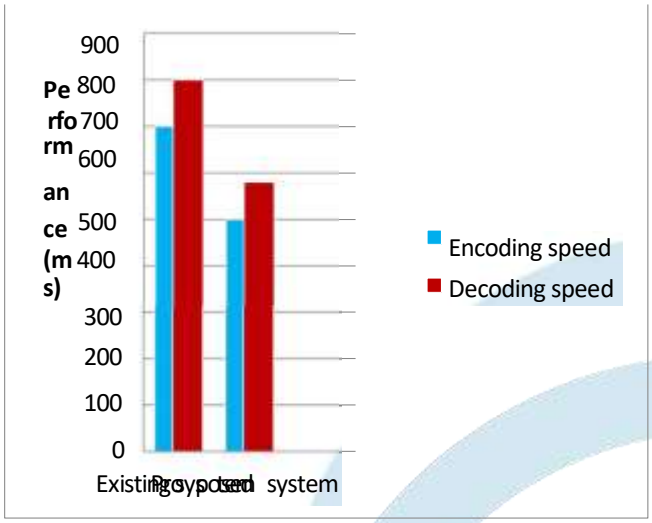
When the photos are too big, pooling layers would lower the number of parameters. Spatial pooling, also known as down sampling or subsampling, lowers each map's dimensionality while preserving crucial data. Completely Interconnected Layer The feature map matrix will be transformed into a vector (x1, x2, x3, …) in this layer. We created a model by combining these attributes with the fully connected layers.

Classifier Softmax

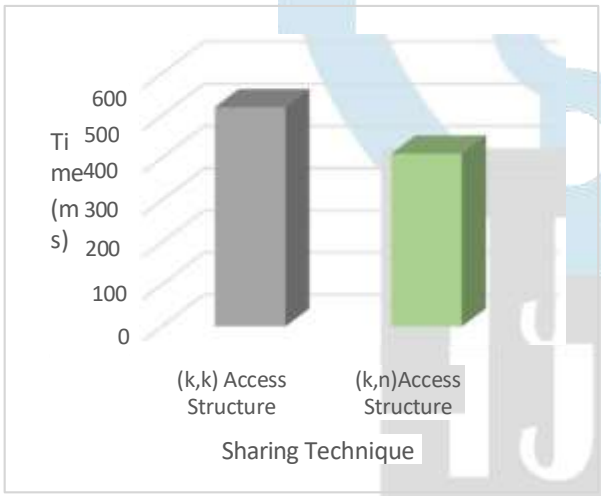
Lastly, we have an activation function to categorise the outputs, like sigmoid or softmax.

IV. RESULTS

Experiments can be performed on a personal computer with a configuration: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB memory, Windows, MySQL backend database and Jdk 1.8. The application is web application used tool for design code in Eclipse and execute on Tomcat server.



Time complexity of a sharing schema algorithm quantifies the amount of time taken by an algorithm to run as a function of the length of the input.



V. CONCLUSION

Since no noise is produced in the cover image, no one can even tell that data is embedded in the image thanks to the combination of steganography and cryptographic techniques, making it impossible for an interceptor to recover the encrypted concealed data. In terms of security, flexibility, and encryption performance, the encoding cryptographic technique was determined to be the best fit for the project. Since encoding produces stego-images that appear to have excellent visual fidelity while containing concealed data, it was determined to be the most suitable steganography algorithm. Because it increases the data embedding capacity and guarantees data security at three levels—steganography, cryptography, and transmission by splitting—this guarantees the lossless recovery of the secret image at the recipient end. Thus, the primary goal of ensuring information exchange security has been accomplished.

VI. FUTURE SCOPE

Furthermore, the various potential problems of federated learning (e.g., data imbalance) in the SIR scene will be considered.

VII. ACKNOWLEDGMENT

It is our pleasure to acknowledge sense of gratitude to all those who helped us in making this project. We thank our Project Guide Prof. Manisha Desai helping us and providing all necessary information regarding our project. We are also thankful to Dr. Deepali Newaskar (Head of Department of Computer Engineering) for providing us the required facilities and helping us while carrying out this work. Finally, we wish to thank all our teachers and friends for their constructive comments, suggestions and criticism and all those directly or indirectly helped us in completing this project.

REFERENCES

1. [1]Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, “Combination of Steganography and Cryptography: A short Survey”, 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).
2. [2]Aljaafari Hamza and Basant Kumar, “A Review Paper on DES, AES, RSA Encryption Standards”, Proceedings of the SMART–2020, IEEE Conference ID: 50582 9th International Conference on System Modeling & Advancement in Research Trends, 4th– 5th, December, 2020 Faculty of Engineering & Computing Sciences.
3. [3] Eman Salim Ibrahim Harba, “Secure Data Encryption Through a Combination of AES, RSA and HMAC”, Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017.
4. [4]V. Reshma, S. Joseph Gladwin and C. Thiruvenkatesan, “Pairing-Free CP-ABE based Cryptograph Combined with Steganography for Multimedia Applications”, International Conference on Communication and Signal Processing, April 4- 6, 2019, India.

REFERENCES

5. [1]Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).
6. [2]Aljaafari Hamza and Basant Kumar, "A Review Paper on DES, AES, RSA Encryption Standards", Proceedings of the SMART–2020, IEEE Conference ID: 50582 9th International Conference on System Modeling & Advancement in Research Trends, 4th–5th, December, 2020 Faculty of Engineering & Computing Sciences.
7. [3] Eman Salim Ibrahim Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017.
8. [4]V. Reshma, S. Joseph Gladwin and C. Thiruvenkatesan, "Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications", International Conference on Communication and Signal Processing, April 4-6, 2019, India.
9. [5] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images", 2020 International Conference on Artificial Intelligence and Signal Processing (AISP).
10. [6] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.
11. [7] Radha S. Phadte, Rachel Dhanaraj, "Enhanced Blend of Image Steganography and Cryptography", IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).
12. [8] Maisa'a Abid Ali Khodher, Teaba Wala Aldeen Khairi, "Review: A comparison Steganography Between Texts and Images" , FISCAS 2020.
13. [9] Kh. Manglem Singh, Sukumar Nandi2 , S. Birendra Singh1, L. ShyamSundar Singh1, "Stealth Steganography in Visual Cryptography for Half Tone Images", International Conference on Computer and Communication Engineering 2008.
14. [10] Nidhi Menon, Vaithiyanathan V, "Triple Layer Data Hiding Mechanism using Cryptography and Steganography", 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018), MAY 18th & 19th 2018.