Reversible Data Hiding with Image Enhancement using CNN

H. Keerthana[1], V.Annapurna[2]
[1]*M. Tech Scholar, DECS, ECE Department, JNTUA College of Engineering (AUTONOMOUS) Anantapuramu, Andhra Pradesh, India*
[2]*M. Tech., Assistant Professor (Adhoc), ECE Department, JNTUA College of Engineering (AUTONOMOUS) Anantapuramu, Andhra Pradesh, India.*

Abstract **- Reversible Data Hiding (RDH) methods have acquired notoriety throughout the most recent twenty years, where information is installed in an image so the first image can be restored. There are so many existing works performed on Reversible Data Hiding. However, this method will produce low quality metrics (PSNR) and data is not secured. As a result of the drawbacks of previous methods, we will propose a watermarking algorithm based on CNN and deep learning algorithms, in which the CNN produces strong inherent image features, which are then combined with the proprietor's watermark succession applying "XOR" activity. The inherent features are generated from input image and the hidden image (binary pattern) is combined with those inherent features by XOR operation. It is secured by a secret key (password) and gives better quality performance (PSNR).**

Index Terms **- Reversible Data Hiding, Retrieval, Image Processing, Embedding & Extraction, Convolutional Neural Networks, Deep Learning, Watermarking.**

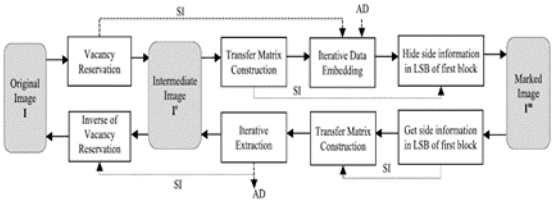
INTRODUCTION

Information hiding (i.e., information implanting) is a communication issue with two significant parts. The idea of information hiding is to disguise a significant mystery message in open information. A review of ebb and flow information hiding as indicated by applications is given by Petit colas who grouped information hiding into a few exploration zones, for example, watermarking, fingerprinting, and steganography. Watermarking and fingerprinting are applied for validation and authority, which identify with signal wellsprings of communications with the end goal of copyright security of computerized media. Steganography is the craft of covered or shrouded composing, which is clandestine communication for mystery messages to hide the presence of a message from noxious assailants snooping on a communication channel. These days, most conventional models of information address the issue of copyright assurance for computerized media; that is, these models centre around the insurance of sign wellspring of communications for planning stenographic frameworks to produce watermarking and fingerprints. The use of watermarking in picture, sound, or video information is generally well known. In the interim, little examination consideration has been paid to the security of the secretive communication channel. At present there is no all-inclusive information hiding model accessible for ensuring the safe communication channel. Communication of advanced information becomes successive these days, on account of its quick access ability. A wide scope of advancements for start to finish insurance are expected to oppose the security dangers in current communication. For present business patterns, computerized media has a critical impact and furthermore there comes the need of making sure about the information/information from unapproved personals. For accomplishing this, the made sure about Personal information should be implanted into advanced substance which is conjoined ordinarily. This idea of ensuring the information is called as watermarking. The critical property of watermarking is its strength to any sort of assaults which thus makes it difficult to isolate the watermark without upsetting or corrupting substance. Computerized watermarking, steganography ` Reversible Data Hiding (RDH) are the kinds of information hiding draws near. Presently a day the information security and information uprightness are the two testing territories for research. There are

countless investigates is advancing on the field like web security, steganography, cryptography. Now and then we found certain twisting in pictures utilized in military, clinical science which is un-satisfactory. Consequently, for information hiding we have a strategy utilizing which we can remove information effectively and after that unique cover substance can be completely recuperated. This strategy is known as reversible information hiding. This procedure is additionally called as lossless, mutilation free, or invertible information hiding method. The reversible information hiding strategies might be generally ordered into three kinds: the distinction extension techniques, histogram alteration techniques, and lossless pressure-based strategies. In the distinction development techniques, the contrasts between two adjoining pixels are multiplied to produce another most un-huge piece (LSB) plane for implanting the extra information. The histogram alteration strategies move the histogram of cover information from its pinnacle point towards its zero focuses and use the cover information at the pinnacle purpose of histogram to convey the extra information. As the third kind of reversible information hiding, the lossless pressure-based strategies utilize factual excess of the host media by performing lossless pressure so an extra space for obliging the extra information can be made.

EXISTING METHOD

RDH is a procedure that conceals information into reversibly computerized media, which is utilized to convey extra information with a subtle way. With the RDH strategy, the secret messages can be separated precisely, and the first picture can be recuperated lossless. RDH is helpful in the uses of marking advanced pictures. Advanced watermarking, steganography and Reversible Data Hiding (RDH) are the sorts of information concealing methodologies. Watermarking is an arrangement of advanced pieces set in a computerized cover document that perceives the record's copyright data.



Steganography is committed for covert communication. It changes the image so that main the shipper and the planned beneficiary can distinguish the message sent through it. Since it is imperceptible, the discovery of restricted information isn't basic. In steganography, the cover document doesn't hold any importance after extraction of restricted information. While in RDH the cover record additionally holds the data like restricted information. The RDH permits one to implant a generally enormous measure of information into a image so that the first image can be recreated from the marked image. This makes it an optimal strategy for applications where one needs to store metadata into the cover signal, while recuperate the first sign without loss after information extraction. We first build the histogram h = h0; h1;::: ; h255 from a grayscale image 'I' sized mr*mc. In the original image, there are M original histogram vacancies, satisfying hi D 0 (M might equal to zero). We combine the least significant histogram bins (i.e. the bins with the least pixels) in h to create more histogram vacancies, because using the original histogram vacancies in the original image can only guarantee a required embedding rate. "Merging hi into hj" refers to changing all pixels with the value 'I' to the value 'j'. The transfer matrix expresses the electrical tunnelling via a particular potential region in a simple way. Consider the Schrödinger equation's stationary solution as an impinging wave from the left lead, partially reflected and partially transmitted through the potential area (scattering region). In this instance, we have BR0.

$$\begin{cases} A_R = m_{11} A_L + m_{12} B_L; \\ 0 = m_{21} A_L + m_{22} B_L; \end{cases}$$

The reflection & transmission amplitudes and coefficients can be simply calculated using these two equations. The reflection amplitude of a particle arriving from the left lead is defined asr =BL/AL,
and it is given by

$$\boxed{r = -\frac{m_{21}}{m_{22}}}$$

The *reflection coefficient* is*:*

$$R = rr^* = |\, r \,|^2 = \left|\frac{m_{21}}{m_{22}}\right|^2$$

For a particle arriving from the left lead, the transmission amplitude to the right lead is equal to AR/AL, and is given by

$$\boxed{t = \frac{1}{m_{22}}}$$

The transfer matrix's unimodularity has been considered. The coefficient of transmission is

$$T = tt^* = |\ t\ |^2 = \left|\frac{1}{m_{22}}\right|^2$$

The property R+T=1 is easily verified. The transfer matrix for a particle incoming from the left lead can be described in terms of transmission and reflection amplitudes t and r.

$$M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} \equiv \begin{bmatrix} 1/t^* & -r^*/t^* \\ -r/t & 1/t \end{bmatrix}$$

The MSB is the highest digit in a digital data bit string, whereas the LSB is the lowest digit. The left end of digital data is highest digit, while the right end is lowest digit, much like in regular number notation. In the binary system, 99 in the decimal system is represented as (MSB) 01100011(LSB). The MSB is 0 and the LSB is 1 in this situation. Considering inter-block interfaces, with a parallel interface, all the bits on the transmitting side and the receiving side correspond, so there is no problem in particular. With a serial- interface, however, all bits are broadcast and received across a single data line, requiring the bit order definitions in the sending and receiving protocols to match. In the case of the above data (number), the data is transmitted and received in the order of "01100011" in the case of MSB first, and in the order of "11000110" in the case of LSB first. Parallel data can be recreated via serial parallel conversion of the receive data if the receiving side matches the transmitting side's transfer mode (MSB/ LSB first).

PROPOSED METHOD

As with any other zero watermarking method, the proposed zero watermarking strategy consists of a master share generating stage & an image verification stage. Figure 1 depicts the master share generation stage, whereas Figure 2 depicts the image validation stage. In the two phases, the recently prepared CNN is utilized as a significant piece of our plan. In this part, first we portray the CNN design utilized in the proposed plan and a few hyper-boundaries utilized in the preparation phase of the CNN. Then, we depict the two phases including the proposed method.

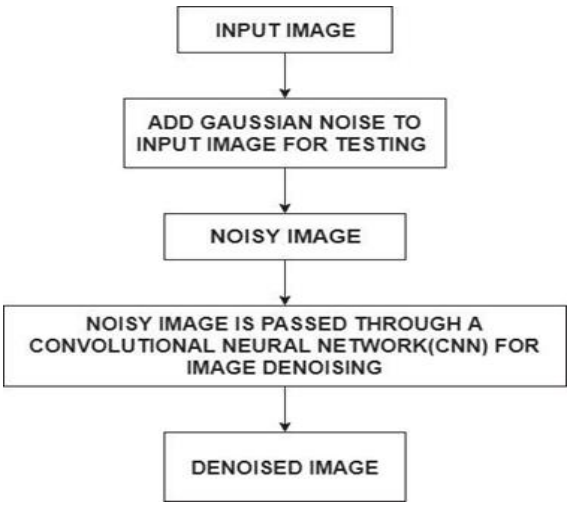


Figure: Method used for denoising

A Convolutional Neural Network (Convent/CNN) is a Deep Learning system that can take in an information image, allocate significance (learnable loads and predispositions) to distinct angles/objects in the image, and then separate them. When compared to previous characterisation calculations, the amount of pre-handling required in a ConvNet is significantly less. While channels are hand-designed in crude schemes, Convents can get familiar with these filters/characteristics with enough preparation.

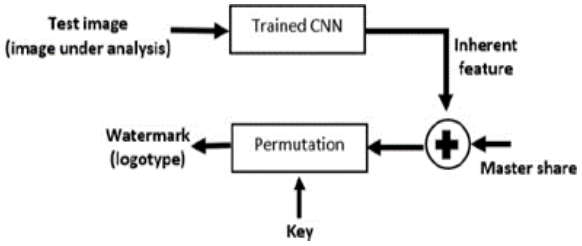


Figure 2: Master Share Generation Stages

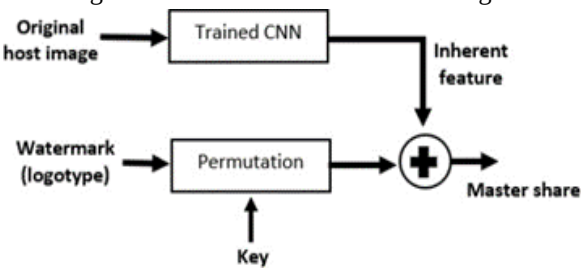


Figure 3: Image verification Stage

Procedure:

Our model contains thirteen convolutional layers and two fully connected layers.

After every three convolutional layers a max pool layer is utilized to reduce the spatial data or information.

For all layers ReLU and Batch normalization layers are used as activation function. Fig given previous express our proposed model architecture.

The training is performed for the purpose to achieve whether image target or not an image target Fully connected layer collects the information about inherent features when the training of CNN is completed.

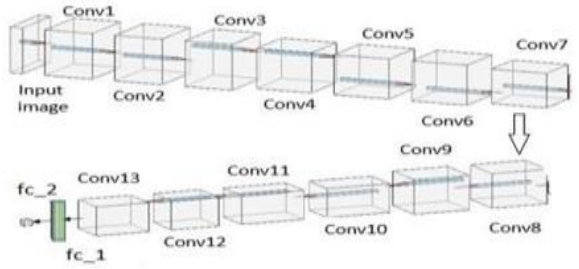


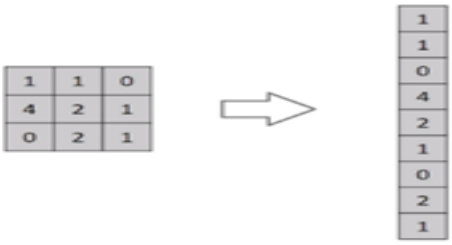
Figure 4: Architecture of CNN model

Convolutional layers:

CNN architecture is introduced in Fig(4), which is made of 13 convolutional layers and two completely associated layers. Since max-pooling activity diminishes the spatial data in the network, we carried out this activity each 3 convolutional layers (After layer3, layer6, and layer9). After each convolutional layer, the neural reactions are standardized involving Batch Normalization method to adjust them through the following layer. The initiation work carried out in all layers is ReLU, besides in the characterization layer, where we utilized "SoftMax" activity. The architecture of the CNN utilized is given by Fig.(4),which comprises of 13 convolutional layers and two completely associated layer referenced previously. With these convolutional layers, the inherent picture highlights have separated. To encode it these pictures, include we utilize two completely associated layers, which are the dependable to create hearty elements of information picture, explicitly, the 100-neurons data contained in the "fc_1" layer. The arrangement of the CNN is given by Table. It is quite important for every convolution cycle, non-linear function ReLU & Batch standardization activity are completed.

Convolution:

Using filters, a ConvNet may successfully detect spatial & temporal dependencies in an image. Because of the reduced no. of boundaries included and the reused weights, the architecture provides a better fit to the picture dataset. As a result, the network may be set up to understand the refining of a superior image.



Flattening of (3x3) image matrix into (9x1) vector

In the case of basic binary images, the technique may show a typical accuracy score when performing class forecasting, but it will has virtually no precision when dealed with complex images with pixel conditions thoroughly.

Convolutional kernel:

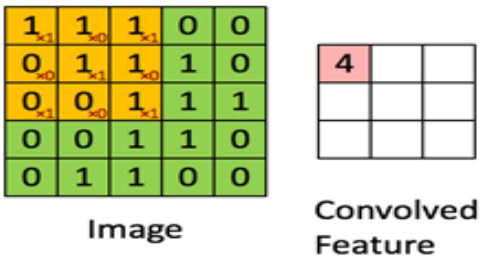
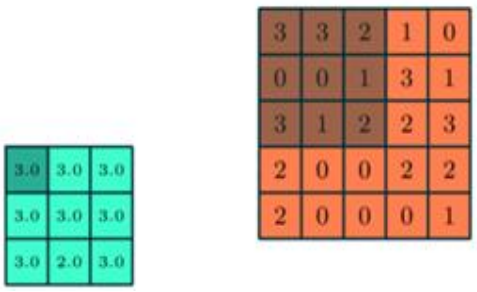


Image Dimensions = 5x5x1(Number of channels, e.g. RGB)

In the above case, the green section resembles our 5x5x1 input image(I). The Kernel/Filter (K) is the element that involves the convolution operation in the initial half of a Convolutional Layer. It is illustrated in yellow. 'K' has been chosen as 3x3x1 matrix. Because Stride Length = 1 (non-Stride), the Kernel shifts 9 times, each time performing a matrix multiplication operation between 'K' and the region 'P' of the picture that the kernel is hovering over.

Pooling layer:



3x3 pooling on 5x5 convolved feature

Pooling is of two types: maximum pooling and avg pooling. The most extreme worth from the piece of the image covered by the Kernel is returned by Max Pooling. Avg Pooling, returns the normal of the relative variety of attributes from the Kernel-covered portion of the image. Max Pooling works as a Noise Suppressant as well. It largely eliminates loud initiations and conducts de-noising. Avg Pooling, essentially does dimensionality reduction as a commotion stifling component. We conclude that Maximum Pooling performs much better than Average Pooling.

Advantages:

a. Convolution Neural Networks leverage local spatial specificity in input
b. It is a quite effective training model.
c. The first and most important benefit of a convolution neural network is instant extraction of features for the specific task.

RESULTS AND DISCUSSIONS

Once the CNN is prepared the inborn element of the image is retrieved from the CNN's Fully Connected Layer-1 (fc_1), which comprises 100 real data, once it is generated. This result information is changed over in binary data using threshold value -0, being positive equal -1, otherwise 0. Binary watermarks design the master divide is created by “XOR” activity among the inherent image's binary sequence include and with a binary watermark that is permuted.

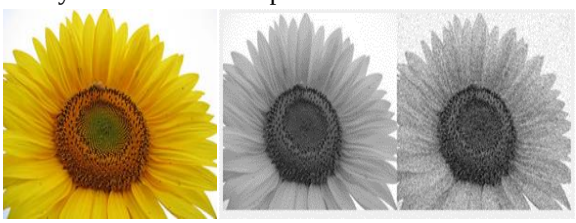


Fig :1.Input Image 2.Input Image and Noised Input Image

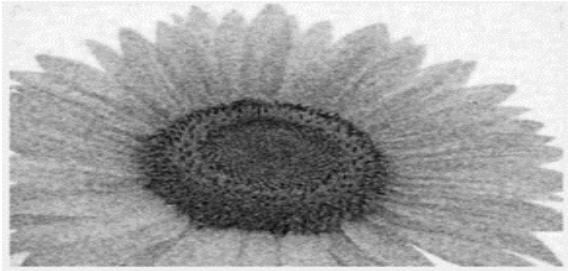


Fig:- Denoised Image

Image in below fig is the image which we want to hide in the source image by CNN algorithm and the training Process of the CNN

Fig: Secret Image

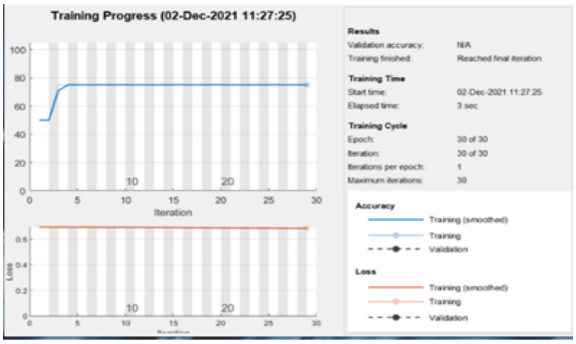


Fig :- Training Process

The above fig is the encrypted image. It is encrypted by the user’s secret key which is used as the same key for both encryption and decryption. The final decrypted image which will obtained by the secret key.

Fig:- Embedded Image

After the secret key is entered and matched with the key .The secret image is retrieved.

Fig:-Decrypted/Retrieved Image

S.No	Existing Model	Proposed Model
1	Bit Error Rate (BER) - 0.3941	Bit Error Rate (BER) - 0.4538
2	PSNR - 20.6942	PSNR - 51.5623
3	SSIM - 0.8677	SSIM - 0.6463

Table: - Comparison of Metric values with existing model and proposed model

The above Table gives the comparison of Metric values between existing and proposed methods. It states that improved PSNR value is improved. From these tables, we assume that greater robustness can be offered by our proposed method.

CONCLUSION

By extracting inherent features of image from trained CNN network our article proposed a new watermarking technique known as Zero-Watermarking Technique. XOR operation is performed in the feature extraction process. This developed model of watermarking is best suitable for telemedicine applications. Best results is produced when compared to existing models and also removes noise that presents in the image.

REFERENCES

[1] Y.-Q. Shi, X. Li, X. Zhang, H.-T.Wu, and B. Ma, ``Reversible data hiding: Advances in the past two decades," IEEE Access, vol. 4, pp. 3210_3237, 2016.

[2] J. Fridrich, M. Goljan, and R. Du, ``Invertible authentication," Proc. SPIE, Secur. Watermarking Multimedia Contents III, vol. 4314, pp. 197_208, Aug. 2001.

[3] J. Fridrich, M. Goljan, and R. Du, ``Lossless data embedding_New paradigm in digital watermarking," EURASIP J. Adv. Signal Process., vol. 2002, no. 2, Dec. 2002, Art. no. 986842.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, ``Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253_266, Feb. 2005.

[5] J. Tian, ``Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890_896, Aug. 2003.

[6] J. Tian, ``Wavelet-based reversible watermarking for authentication," Proc. SPIE, Secur. Watermarking Multimedia Contents IV, vol. 4675, pp. 679_690, Apr. 2002.

[7] D. M. Thodi and J. J. Rodriguez, ``Prediction-error based reversible watermarking," in Proc. Int. Conf. Image Process., Oct. 2004, pp. 1549_1552.

[8] D. M. Thodi and J. J. Rodriguez, ``Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721_730, Mar. 2007.

[9] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, ``Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354_362, Mar. 2006.