INTELLIGENT WATERMRKING ON DIGITAL IMAGE

SONAM KHATIK Department of Electronic & Comm. Engineering College, Jabalpur Jabalpur M.P. India Sonam0205eckhatik@gmail.com
AGYA MISHRA Department of Electronic & Comm. Engineering College, Jabalpur Jabalpur M.P. India agyamishra@gmail.com

ABSTRACT

Watermarking technology play and important role in preventing violation as it allowed in imperceptible or perceptible water marking depending on the requirement in the multimedia data to identify the legitimate owner or detect malicious tampering of the documents.

This paper uses convolutional neural networks (CNNs) to propose an interesting watermarking technique that imperceptibly hides an image inside a cover image and outperforms other state-of-the-art schemes in terms of visual quality and robustness according to simulation results and performance comparisons.

For example:- we hide secret image in the cover image with the help of lots of networks like CNN DNN etc. In this paper used CNN network for hiding a secret image in the cover image.

This paper successfully explains the digital watermarking technique on digital images based on convolution neural network by analyzing various values of PSNR's and accuracy by different attack level.

watermarking or digital watermarking is a technique that involves embedding digital marks or indicators into machine learning models or datasets to enable their identification. Faced with the explosion of content generated by Artificial Intelligence, this approach has become essential.

Keywords:-
Digital, watermarking, CNN, Insertion, Extraction, Watermark, PSNR, ERROR BIT RATE.

I INTRODUCTION

A common type of neural network used for tasks involving natural language processing is the CNN (Convolutional Neural Network). It works particularly well when dealing with data sequences, like text[1]. CNNs can be used in NLP to perform language modelling, machine translation, and text classification.

Digital watermarking is the process to protect the hidden, information into the digital media to preserve the ownership of those media data. Many approaches have been introduced to obtain the watermark to be active as well as robust to removal of different attacks. Based on extraction methods, digital image watermarking approaches can be split into two main categories named Blind-watermarking and Non-Blind water marking[2].

PURPOSE-

The purpose of this paper is to demonstrate the hiding of a secret image within an cover image using Convolutional Neural Networks (CNN). After applying CNN, an encoded image, termed as a watermarked image, is obtained. The experimental results are conducted under two cases. In the first case, a cover image of JEC building of size 351x388 is utilized along with a secret image of JEC logo sized 200x200. Subsequently, metrics such as PSNR (Peak Signal-to-Noise Ratio) value accuracy and error bit rate are calculated. The same procedure is followed for case study 2, where the cover image remains the same (JEC building), but a different secret image is embedded within it.

The significant portion of the cover image, e.g. the low frequency components have to be modified in order to encode the information in reliable and robust way.

In this paper firstly take 2 image 1st one is cover image and 2nd one secret image. By CNN hide the secret image in cover image.

we felt that hiding a perticular image inside another image is easy but should be done with the help of some technology so we sucked CNN and hid one image inside another image and we found that Also on paper everyone has given the same technique like DWT, DNN but accuracy is less, PSNR is less so we increased its accuracy by using CNN.

1.1 APPLICATION

A CNN can have multiple layers, each of which learns to detect the different features of an input image. A filter is applied to each image to produce an output that gets progressively better and more detailed after each layer[3].

IICONCEPT

Convolution neural network (also known as ConvNet or CNN) is a type of feed-forward neural network used in tasks like image analysis, natural language processing, and other complex image classification problems.

The basic principle of CNN lies in feature learning through convolutional layers. These layers apply filters to input data, extracting meaningful features and capturing spatial hierarchies for accurate pattern

Suppose that we have some N×N

2.1 EQUATION

square neuron layer which is followed by our convolutional layer. If we use an m×m
filter ω, our convolutional layer output will be of size (N−m+1)×(N−m+1).
In order to compute the pre-nonlinearity input to some unit xℓij
in our layer, we need to sum up the contributions (weighted by the filter components) from the previous layer cells:

$$x_{ij} = \sum_{a=0}^{m-1,n-1} \mathrm{w}\,\mathrm{y}^{\mathrm{l}-1}(\mathrm{i} + \mathrm{a})(\mathrm{j} + \mathrm{b})$$

This is just a convolution, which we can express in Matlab via conv2(x, w, 'valid') Then, the convolutional layer applies its nonlinearity:

$$\mathrm{y}\ell\mathrm{ij}=\sigma(\mathrm{x}\ell\mathrm{ij}).$$

2.3 WATERMARK EMBEDDING: -

In this process firstly the grace scale cover and secret images taken and feet format is applied to the image the convolution neural network used for water marking it means hide secret image(jec logo) in cover image(jec building) by applying CNN to both image and multiply by a scaling factor and we added during the embedding process the size of a watermark should be smaller than the cover image frames size of both the image should be made equal since the water mark embedded in this paper precipitate in nature of visible.

IIIPROPOSED TECHNIQUE

Embedding a secret watermark into a given CNN is define as the task of embedding a image. In this section we first present our technical motivation then we show the sketch of proposed method followed by the details of watermark embedding an extension.[4]

For example:- we hide secret image in the cover image with the help of lots of networks like CNN DNN etc. In this paper used CNN network for hiding a secret image in the cover image.

This paper uses convolutional neural networks (CNNs) to propose an interesting watermarking technique that imperceptibly hides an image inside a cover image and outperforms other state-of-the-art schemes in terms of visual quality and robustness according to simulation results and performance comparisons[1].

Watermarking technology play an important role in preventing violation as it allowed in imperceptible or perceptible water marking depending on the requirement in the multimedia data to identify the legitimate owner or detect malicious tampering of the documents[5].

3.1Algorithm for proposed system

1) Firstly, cover image and secret image both is loaded.
2) The cover image and secret image are read using the imread function.
3) The both image are store in a variable X and Y respectively.
4) Cover image and secret image resize by resized function.
5) JEC building take as a cover image for both cases.
6) Using convolution neural network(CNN) hide the secret image in cover image i.e. hide the jec logo(fig no. 2) and another image(fig no. 4) in jec building(fig no.1).
7) This hiding image called the watermarked image.
8) After watermarking process, calculated accuracy by different attack level.
9) The watermarked image,cover image and secret image are displayed using imshow function.
10) Accuracy for different attac Level and PSNR show in table 2 and 4.

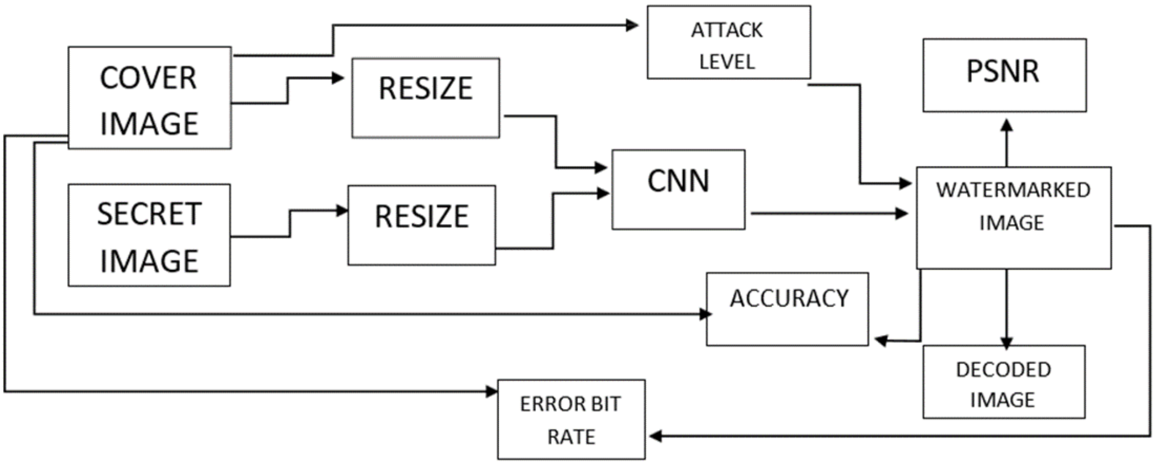


Fig no. 3.1(a) Architecture of CNN based watermarking model

3.2 Comparison of various techniques for DIGITAL IMAGE-

TABLE NO.-1,fig no.-3.2(a)

Sno.	PAPER	TECHNIQUE AND ALGORITHM	MEASUREMENT PRAMETER	ACCURACY/ PSNR
1.	[1]	DNN	Watermark trained test	54.7% 51.89%
2.	[2]	DWT	Learing rate 0.001	41.8%
3.	[3]	DNN	Learing rate 0.002	Non marked-47.5% Marked-47.2%
4.	[4]	CNN	Learing rate 0.001	
5.	[5]	CNN	Learing rate 0.002	

IV EXPERIMENTAL RESULTS:-

4.1 CASE STUDY-1

1) Input Image: The input image has been resized to a standard 551x447.The input image is shown in figure 6.
2) watermarking image: The output image has been resized to a standard 200x200. The watermarking image is shown in figure 6.
3) watermarked image: we watermarked is done using CNN.
4) Image with noise: The image with noise is shown in figures.

Fig 4.1(a)
(input image)

fig 4.1(b)
(secret image)

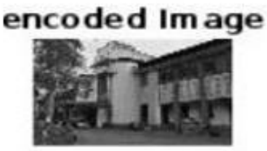


fig 4.1(c)
(watermarked image)

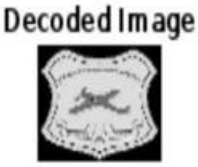


fig 4.1(d)
(decoded image)

4.1.1 ANALYSIS OF CASE STUDY-1

In this process we have used grayscale images jec building as original image and the logo of the JEC Jabalpur as the watermark. For embedding of watermark in the original image the value of scaling factor is varied from

0.01 to 0.005 by keeping constants and best result is obtained for 0.01 as shown in the table The PSNR for the best result is at **49.7432.**The values of the PSNR and accuracy are calculated for various values of the scaling factors as shown in the table1.

According to CASE STUDY 1 we analysis that when be change attack level,accuracy was changed with respect to the time,now we can see plotting the attack level versus accuracy in table 1 when we take cover image JEC building and secret image JEC logo with building size 251X388X3,class unit 8 and logo size 200X200X3,class unit 8.

PERFORMANCE ANALYSIS TABLE NO -2

s.no.	ATTACK LEVEL (db)	ACCURACY (%)	ERROR BIT RATE
1.	0.01	98.99 BEST RESULT	0.59924
2.	0.02	98.07	0.60042
3.	0.03	97.06	0.61371
4.	0.04	96.01	0.61327
5.	0.05	94.90	0.61404
6.	0.06	94.00	0.61286
7.	0.07	93.01	0.61322
8.	0.08	91.91	0.61213
9	0.09	91.10	0.49655
10.	0.1	0.02	0.49655

Fig 4.1.1(e)

4.1.2 ATTACK LEVEL V/S ACCURACY (IMAGES WITH NOISE FOR DIFFERENT ATTACK LEVEL)

Image with noise watermarked image

Attack level-0.01db, Acuuuracy-98.01%, PSNR-49.7432 and BER-0.52822, fig 4.1.2(a)

Image with noise watermarked image

Attack level-0.02db, Acuuuracy-97.99%, PSNR-49.7432 and BER-0.533,fig 4.1.2(b)

Image with noise watermarked image

Attack level-0.03db, Acuuuracy-97.09%, PSNR-49.7432 and BER-0.53575,fig 4.1.2(c)

Image with noise watermarked image

Attack level-0.04db, Acuuuracy-95.98%, PSNR-49.7432 and BER-0.53653,fig 4.1.2(d)

Image with noise watermarked image

Attack level-0.05db, Acuuuracy-94.48%, PSNR-49.7432 and BER-0.51443,fig 4.1.2(e)

Image with noise watermarked image

Attack level-0.06db, Acuuuracy-93.94%, PSNR-49.7432 and BER-0.53782,fig 4.1.2(f)

Image with noise watermarked image

Attack level-0.07db, Acuuuracy-93.00%,PSNR-49.7432 and BER-0.53455,fig 4.1.2(g)

Image with noise watermarked image

Attack level-0.08db,BER-0.61322 Accuracy-92.15%,PSNR-49.7432,fig 4.1.2(h)

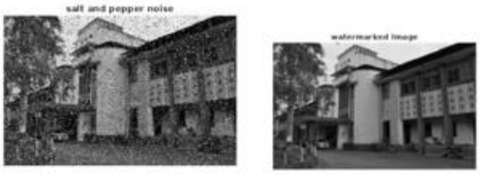


Image with noise watermarked image

Attack level-0.09db, Acuuuracy-91.03%, PSNR-49.743 and BER-0.54004,fig 4.1.2(i)

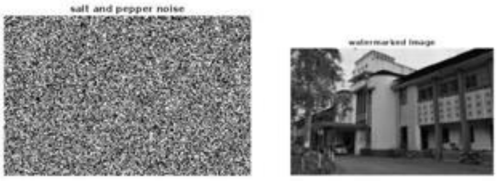


Image with noise watermarked image

Attack level-0.1db, Acuuuracy-0.02%, PSNR-49.7432 and BER-0.44738,fig 4.1.2(j)

4.1.4 ATTACK LEVEL V/S BER (bit error rate)

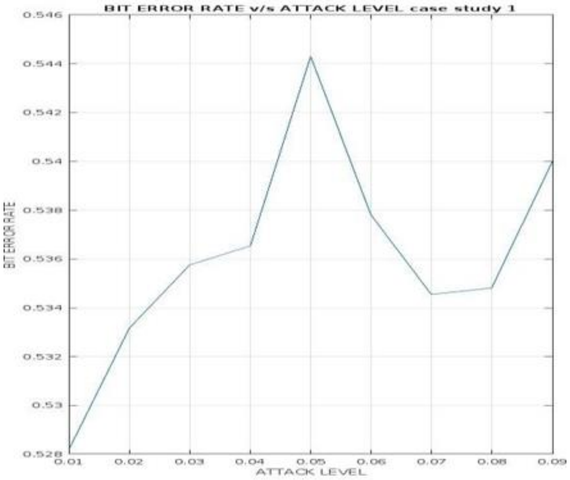


Fig 4.1.3(b)

4.1.3 ATTACK LEVEL V/S ACCURACY

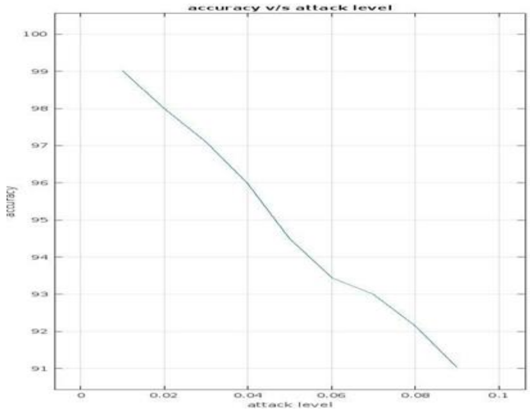


Fig 4.1.3(a)

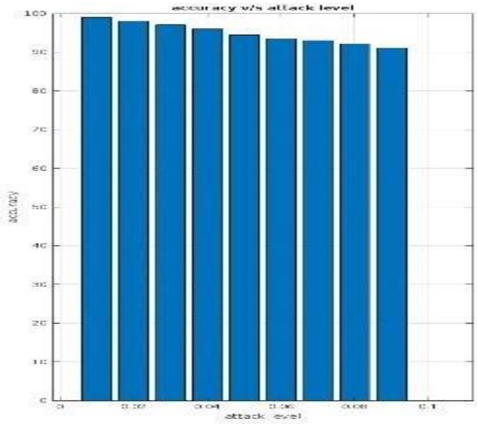
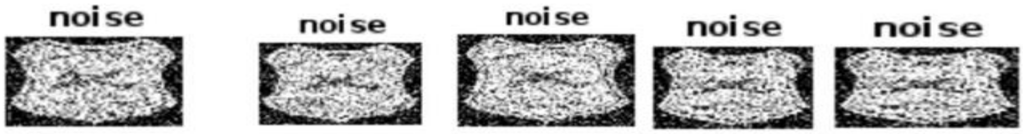


Fig 4.1.4(c)
Bar reprentation for attack level v/s accurac

4.1.5 EXTRACT IMAGES WITH NOISE



Attack level-001 Attack level-0.02 Attack level-0.03 Attack level-004 Attack level-0.05

PERFORMANCE ANALYS FOR EXTRACT IMAGE(Fig no.-4.1.5(a))

ATTACK LEVEL (in db)	ACCURACY (%)
0.01	99.20
0.02	98.36
0.03	97.53
0.04	96.75
0.05	95.88

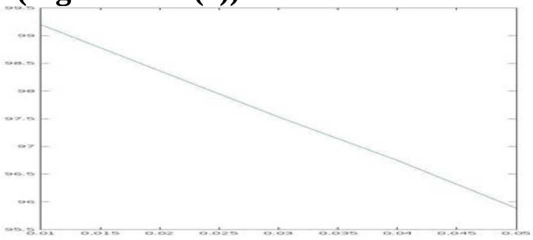


Fig no.-4.1.5(b) ATTACK LEVEL V/S ACCURA

4.2CASE STUDY-2

1) Input Image: The input image has been resized to a standard 551x447.The input image is shown in figure.
2) watermarking image: The output image has been resized to a standard 752x536. The watermarking image is shown in figure no.
3) watermarked image: we watermarked is done using CNN.
4) Image with noise: The image with noise is shown in figures.

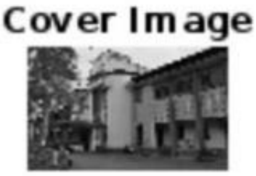


Fig 4.2(a)
(input image)

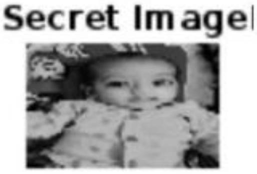


fig 4.2(b)
(secretimage)

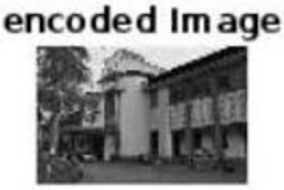


Fig 4.2(c)
(watermarked image)

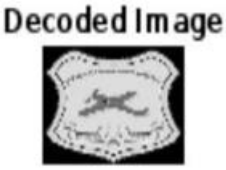


fig 4..2(d)
(decoded image)

4.2.1 ANALYSIS OF CASE STUDY-2

In this process we have used grayscale images jec building as original image and another image as the watermark. For embedding of watermark in the original image the value of scaling factor is varied from 0.01 to 0.005 by keeping constants and best result is obtained for 0.01 as shown in the table The PSNR for the best result is at**49.7342.**The values of the PSNR and accuracy are calculated for various values of the scaling factors as shown in the table 2According to CASE STUDY 2 we analysis that when be change attack level,accuracy was changed with respect to the time,now we can see plotting the attack level versus accuracy in table 2 when we take cover image JEC building and secret image another image with building size 251X388X3,class unit 8,value 752X536X3 unit 8 respectively.

s.no.	ATTACK LEVEL(in db)	ACCURACY(%)	BER (bit error rate)
1.	0.01	98.99 BEST RESULT	0.5992
2.	0.02	98.02	0.6004
3.	0.03	97.06	0.61371
4.	0.04	96.01	0.61371
5.	0.05	94.90	0.61327
6.	0.06	94.00	0.61362
7.	0.07	93.01	0.61404
8.	0.08	91.91	0.61322
9.	0.09	91.10	0.61213
10.	0.1	0.02	0.49655

PERFORMANCE ANALYSIS FOR CASE STUDY-2, Fig 4.2.1(a),Table-3

4.2.2 ATTACK LEVEL V/S ACCURACY (IMAGES WITH NOISE FOR DIFFERENT ATTACK)

Image with noise watermarked image
Attack level-0.01db,
98.99%,PSNR-49.7432
and BER-0.5992,fig 4.2.2(a)

Image with noise watermarked image
Attack level-0.02db,
Accuracy-98.02%,PSNR-49.7432
and BER-0.6004,fig 4.2.2(b)

Image with noise watermarked image
Attack level-0.03db,
97.06%,PSNR-49.7432
and BER-0.61371,fig 4.2.2(c)

Image with noise watermarked image
Attack level-0.04db,
96.01%,PSNR-49.7432,
and BER-0.61321,fig 4.2.2(d)

Image with noise watermarked image
Attack level-0.09db, Acuuuracy-
91.10%,PSNR-49.7432 and BER-0.61213,fig
4.2.2(i)

Image with noise watermarked image
Attack level-0.05db, Accuracy-
Accuracy-94.90%,PSNR-49.7432
and BER-0.61327,fig 4.2.2(e)

Image with noise watermarked image
Attack level-0.06db,
Accuracy-94.00%,PSNR-49.7432
and BER-0.6362,fig 4.2.2(f)

Image with noise watermarked image
Attack level-0.07db, Accuracy-
Accuracy-93.01%,PSNR-49.7432
and BER-0.61404,fig 4.2.2(g)

Image with noise watermarked image
Attack level-0.08db, Acuracy-
Acuracy-91.91%,PSNR-49.7432,
and BER-0.61322,fig 4.2.2(h)

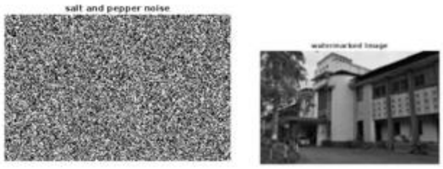


Image with noise watermarked image
Attack level-0.1db, Acuuuracy-0.02%,PSNR-49.7432 and BER-0.49633,fig 4.2.2(j)

4.2.3 ATTACK LEVEL V/S ACCURACY

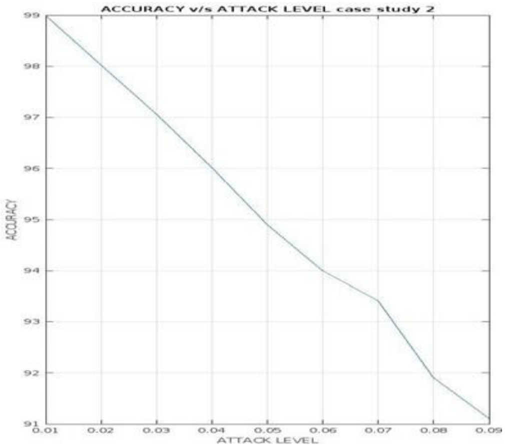


Fig 4.2.3(a)

4.2.4 ATTACK LEVEL V/S BER (bit error rate)

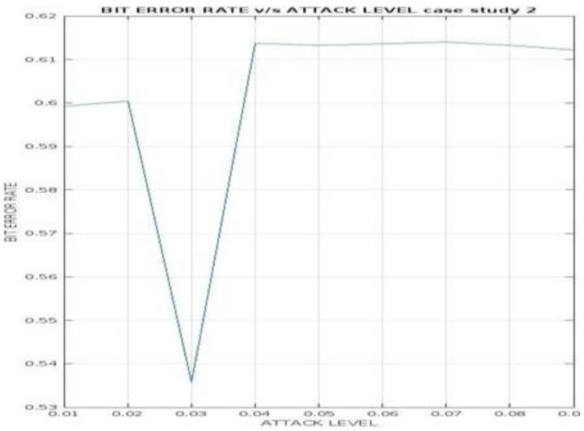


Fig 4.2.4(a)

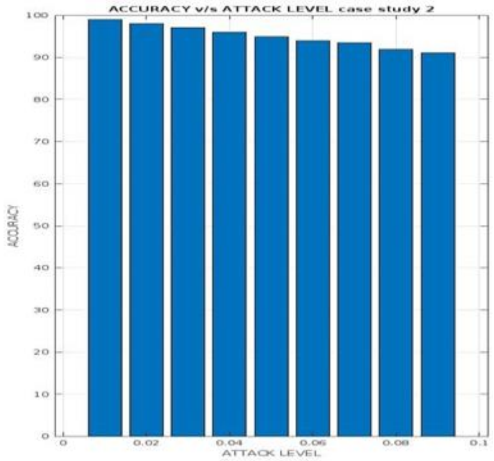
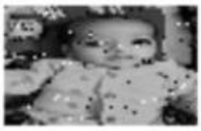


Fig4.2.4(a)
Bar representation for attack level v/s accuracy

4.2.5 EXTRACT IMAGES WITH NOISE



Attack level-001

Attack level-0.02

Attack level-0.03

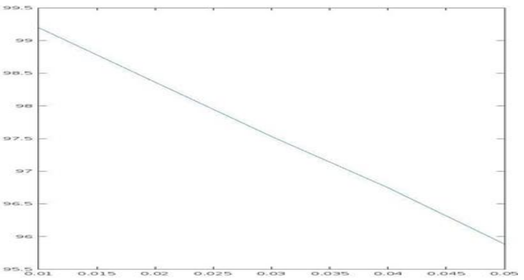
Attack level-004

Attack level-0.05

PERFORMANCE ANALYSIS FOR EXTRACT IMAGE

ATTACK LEVEL (in db)	ACCURACY (%)
0.01	99.20
0.02	98.36
0.03	97.53
0.04	96.75
0.05	95.88

Fig no.4.2.5(a) TABLE NO.- 04



ACCURACY V/S ATTACK LEVEL
Fig no.-4.2.5(b)

4.3 Comparison with existing techniques Table-3.

S.NO.	TECHNIQUEUE	ACCURACY	PSNR
1.	DNN [1]	54.75%	
2.	DWT [2]	41.8%	
3.	DNN [3]	47.5%	
4.	PROPOSED TECHNIQUE	98.99%(in 0.01db attack level)	49.732

Fig no.-4.3(a)

IV CONCLUSION

Intelligent technique is successfully implemented to protect the digital image. In this paper the watermark insertion and extraction was done using the CNN. In this method of water marking we have used feed forward net. As it is shown the result that quality of watermark recovered image and the watermark in the technique is simpler and comparison to CNN which can be verified by the image and the water mark identity to the original image.

References:-

[1]Farah Deeba,Digital Watermarking Using Deep Neurals Network,doc 10.1873/ijmlc.2020.10.932.
[2]Weiping Ding A generalized deep neural network approach for digital watermarking analysis,2471-285X © 2021 IEEE.
[3]Youeli,A survey of deep neural network watermarking techniques,liyue859000040,2020.
[4]Jiangfeng Wang,watermarking in deep neurals networks via error,international symposium on electronic imaging 2020.
[5]jae-Eun Lee,convolution neurals networks-based digital image watermarking adaptive to the resolution of image and watermarking,appl.sci 2020,10,6854;doi10.3390/app10196851[6] Hanzhou Wu,watermarking neural network with watermarked image,IEEE xplore.