iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** IV **Month of publication:** April 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.40991

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue IV Apr 2022- Available at www.ijraset.com*

# Digital Watermarking Using Machine Learning

Karan Umredkar[1], Apurva Ware[2], Savita Rajput[3], Prof. Jaya Jeshwani[4]
[1, 2, 3, 4]*Department of Information Technology, Xavier Institute of Engineering*

***Abstract:*** ***Digital watermarking is a technique used for the information of the images that provides security for the confidentiality. The repetitions of the multimedia objects (i.e. audio, video, text, etc.) have been protected by some of the developed digital watermarking techniques. Digital Watermarking is the process of concealing messages in digital contents in order to verify the rightful owner of the copyright protection. In this paper we have proposed a method that would assist its users to embed a watermark to the cover image based on an adaptive approach in a much robust way while maintaining the quality of the cover image. The implementation of this algorithm is based upon cascading the features of DWT and PCA using Bhattacharyya distance and Kurtosis. PCA decompose and compress the watermark, which results in better PSNR and NCC values for the tested images. The proposed algorithm uses Bhattacharyya distance and Kurtosis to detect the scaling and embedding factors making it adaptive to the input image rather than providing constant value. Also, we take one step forward by investigating the construction of feed-forward denoising convolutional neural networks (DnCNNs) to embrace the progress in very deep architecture, learning algorithm, and regularization method into image denoising. Specifically, residual learning and batch normalization are utilized to speed up the training process as well as boost the performance.***

***Keywords: Digital watermarking, DWT-PCA, PSNR, Image denoising, convolutional neural network, DnCNN, residual learning, batch normalization.***

## I. INTRODUCTION

In the present globalization, the presence of the Internet and many image processing tools opens up to a greater degree, the downloading possibility of an image from the internet, altering it without the permission of the authorized person. For this reason and many others, image authentication has become an active and also a vital research area. In signals and images the embedding of watermark may cause alteration in them. Digital watermarking stands for embedding a signature signal, called watermark into a digital cover image, in order to confirm ownership, verify faithfulness or integrity of the cover, and it may also related to the audio, images, video or text. People can now get multimedia information more quickly. However, digital media have the characteristics of rapid dissemination and easy modification. They can easily be tampered with and spread illegally. As a result, piracy and infringement are becoming more and more widespread. Multimedia information security has become the focus of attention and digital watermarking technology is a Health effective technology.

## II. NEED OF WATERMARKING

Watermarking methods are based on the human visual system in which it cannot be recognized due to tiny difference. In these techniques, the cover-image is used to hide the secret information and the stego-image is the cover- image with the secret data embedded inside. It hides the secret information in general files secretly first and then transmits these files through network, because they look the same as general files, they can escape from the attention of illegal interceptors easily and therefore the secret information is not easy to be attacked.

## III. WORKING DOMAINS

Watermark embedding can be of two types, spatial domain or frequency domain. Frequency domain techniques are considered better as they increase imperceptibility. Discrete Cosine Transform (DCT) is a lossy compression technique in frequency domain where data is lost when the original image is reconstructed from compressed image. Discrete Wavelet Transform is a lossless compression technique. In this method the cover image is divided into four sub-frequency bands: LL, HL, LH, and HH using the Haar wavelet transform. Haar wavelet is used to convert given frequencies; in this case, image matrix into square spectral signal. Similarly, the watermark image is also divided into these sub-frequency bands. Now cover image's LL-band is embedded with watermark image LL-band with the help of embedding and scaling factors. Inverse DWT is applied using this embedded LL-band with host image's LH, HL, and HH bands to form the embedded image. Now watermark image is extracted from this image by applying the process in a reverse manner using Inverse DWT.

As the watermark image is embedded in the cover image, it tends to affect the visual quality of the cover image. Hence, dimensionality reduction is required so that only the significant components required to generate an image (in this case, watermark image) are selected, and all other insignificant components are removed. This process is known
as Principal Component Analysis (PCA). In this process, only
significant components are preserved. Now, these components are embedded in the cover image to form a watermarked image by maintaining their visual behavior. For the adaptive watermarking technique, the embedding factor should be adaptive. In DWT algorithm the embedding equation requires a constant coefficient to be multiplied, in order to get that perfect embedding factor trial and error was used.

So, in order to reduce any error in calculation of embedding factor we need to use adaptive technique that determines the embedding factor based on the cover image.

This was achieved by using Bhattacharyya Distance and Kurtosis. Bhattacharyya Distance is used to measure the similarity between two signals, whereas Kurtosis is used to check the probability distribution of the signal.

For checking imperceptibility and robustness, the PSNR ratio and NCC ratio are calculated. Imperceptibility is determined by PSNR (Peak Signal to Noise Ratio), which is calculated using the cover image and the watermarked image.

NCC (Normalized Cross-Correlation), which is calculated using an original watermark image and extracted watermark image determines the robustness.

For checking robustness, different attacks were performed on the embedded images including Noise attacks (Salt and Pepper, Gaussian) and Geometric attacks (Cropping attack and Rotation). Most of the watermarking algorithms developed earlier have a static embedding factor. In this paper, we have proposed a digital watermarking algorithm, which has an adaptive embedding factor. Thus, any image can be used as a cover image, and any image can be used as a watermark image. Adaptive Embedding factor makes the system more flexible, robust and imperceptible against attacks.

## IV. RELATED WORK

Name of paper: “DCT-DWT Based Digital Watermarking and Extraction using Neural Networks"

Author: R S Kavitha , U Eranna , and M N Giriprasad Research Scholar, Ballari Institute of Technology and Management, Ballari, KTK. Department of ECE, JNTUA Ananthapuramu, AP, India. 2020 International Conference on Artificial Intelligence and Signal Processing (AISP)

A hybrid algorithm was developed and proposed to digitally watermark image. The systems uses two techniques to produce a strong watermark. Discrete cosine transform is first applied to obtain the visible watermarked image. Further, the discrete wavelet transform is applied to embed an invisible watermark into the image. This hybrid technique makes the watermarks strong and effective. On the other hand, extraction of watermark and the original image was also carried out using an extraction algorithm using a two stage neural network.

Name of paper: “A Proposed Digital Image Watermarking Based on DWT-DCT-SVD”

Author: Yuqi He , Yan Hu Computer science and technology, Wuhan University of Technology 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference(IMCEC 2018)

In this paper the survey of the digital watermarking, its frame work, their requirements and applications are presented. Apart from it there is a brief and comparative discussion on the various techniques of the digital image water-marking along merits and demerits. In the digital watermarking techniques the emphasis is on fragile and robust watermarking because the watermarking in the robust watermarking are designed in such a way that it can be detected evenafter a various attempts made for the removal of watermark and in fragile water-marking watermark brings for the purpose of authentication of the digital data.

Name of paper: “Image Watermarking Based On DWT, DCTand SVD Technique”

Author: Prof. R. D. Salagar1 , Miss. Akshata S. Kamatagi International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 6 June 2015

In this paper, three watermarking techniques DWT, DCT and SVD have been used. In the image watermarking, the useful implementation of image with respect to embedding the watermark into host image using the DWT, DCT and SVD are most significant part to achieve imperceptibility and better visibility. Therefore the proposed algorithm provides the good quality of watermarked image. Higher PSNR results in better quality of image. Lower MSE results in low errors.

Name of paper: "Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising"
Author: Kai Zhang, Wangmeng Zuo, Yunjin Chen, Deyu Meng, and Lei Zhang
In this paper, a deep convolutional neural network was proposed for image denoising, where residual learning is adopted to separating noise from noisy observation. The batchnormalization and residual learning are integrated to speed up the training process as well as boost the denoising performance. Unlike traditional discriminative models which train specific models for certain noise levels, our single DnCNN model has the capacity to handle the blind Gaussian denoising with unknown noise level. Moreover, the paper showed the feasibility to train a single DnCNN model to handle three general image denoising tasks, including Gaussian denoising with unknown noise level, single image super-resolution with multiple up-scaling factors, and JPEG image deblocking with different quality factors.

## V. PROCESS OF PROPOSED ALGORITHM

The next will introduce the process of watermark embedding and extracting.

### *A. Watermarking Embedding*

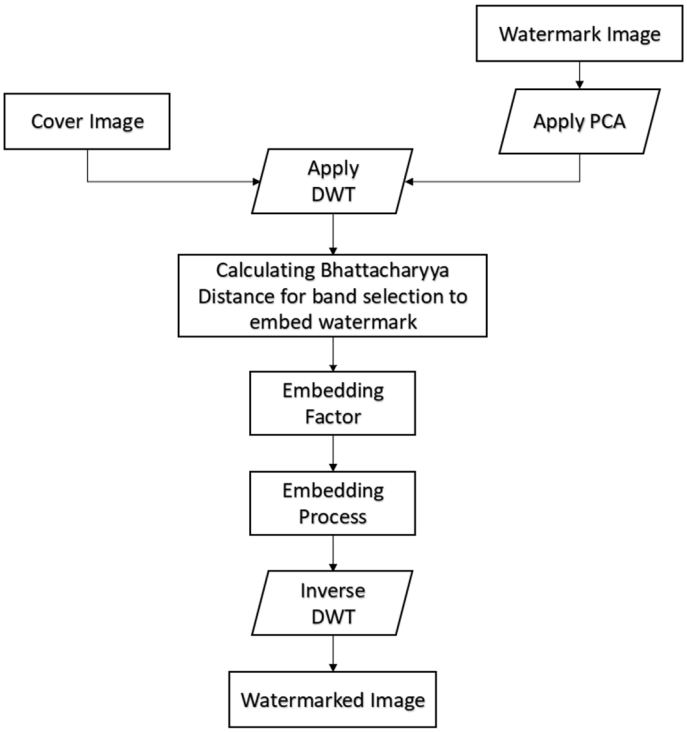



Fig. 1. Watermark embedding procedure

Input: Cover Image(I), Watermark(W)
Output: Embedded Watermarked Image(W')
Step-1: Take the Watermark image W and perform PCA to compress the image w.
Step-2: Apply DWT using HAAR wavelet on the cover image and watermark image.
Step-3: Band selection.
Step-4: Calculate the scaling and embedding factors (α, β).
Step-5: Insert the watermark using the following equation (let's say LL band):
LL' = LL + (β /α) x w
Where, α = Scaling Factor,
β = Embedding Factor
Step-6: Combine the modified LL sub band (LL') with other LH, HL and HH bands of the cover image.
Step-7: Apply inverse DWT to get watermark image.

*B. Watermarking Extraction*

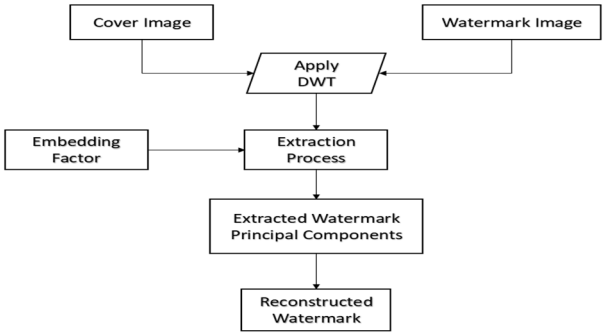


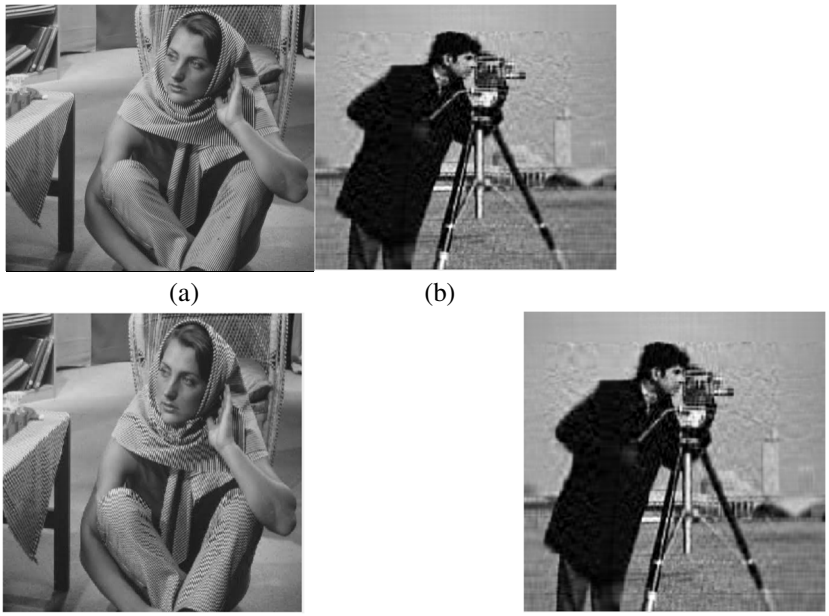

Fig. 2. Watermark extraction procedure

Input: Cover Image(I) and Watermarked Image(I').
Output: Watermark Extracted (wm).
Step-1: Apply DWT using Haar wavelet on the watermarked image.
Step-2: Extract low frequency bands of both images.
Step-3: Obtain scaling and embedding factors (α, β) calculated during the embedding.
Step-4: Extract watermark using following equation:
wm = (LL' - LL) x α / β ……..(5)
Step-5: Reconstruct the watermark and image by applying IDWT (Inverse DWT).

## VI. EXPERIMENTAL EVALUATION

This section will propose experimental results of the proposed method. The algorithm is realized in MATLAB. The cover image used in the algorithm is the standard gray scale image lena of size 512*512. The watermark image is binary watermark image of size 226*226.

*A.*



(a) (b)

(c) (d)

Fig. 3. Eample of the proposed watermarking approach
(a) The original image (b) The original watermark
(c) The watermarked image (d) The extracted watermark

*B.*

(a) (b)

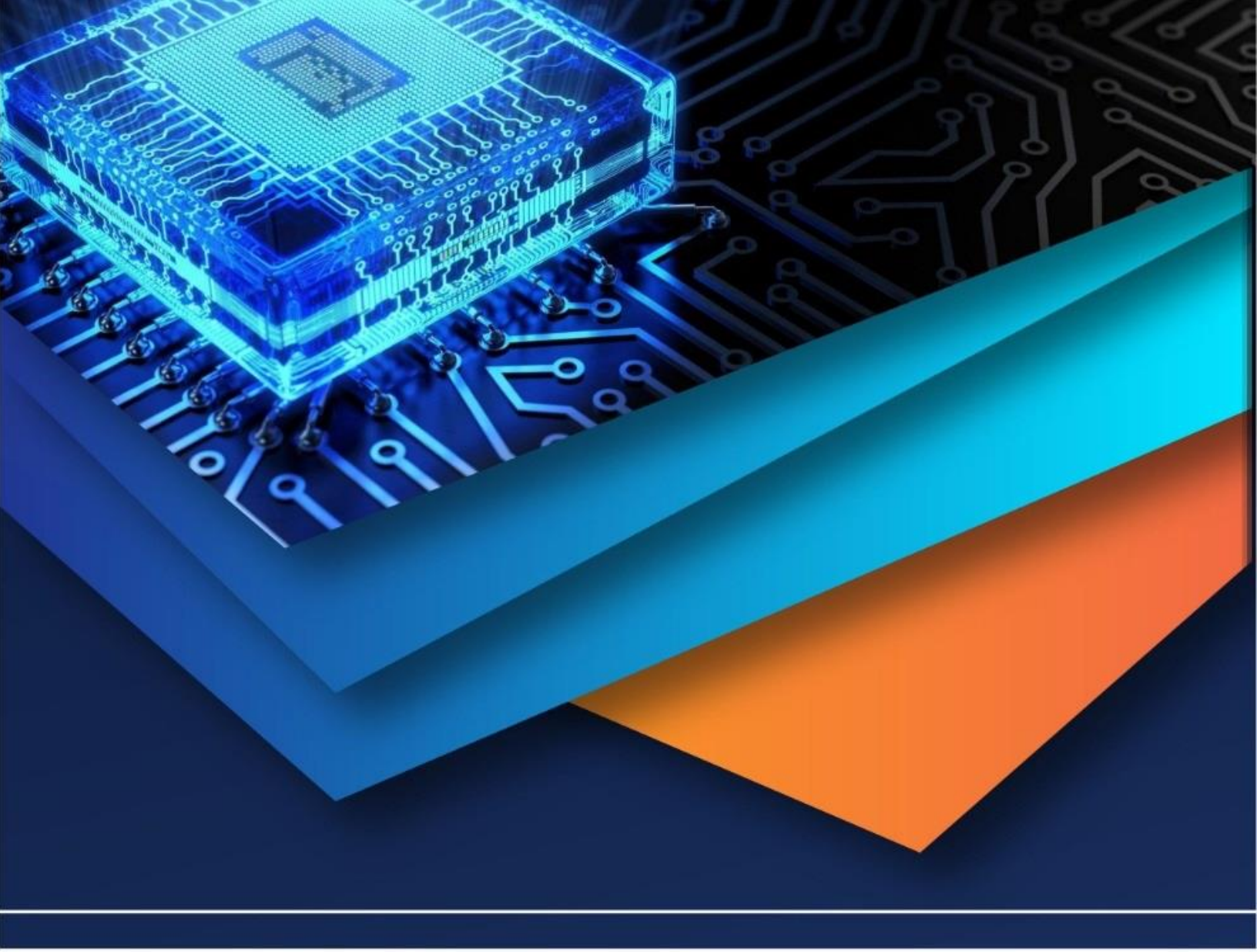
(c) (d)

Fig. 4. Eample of the proposed watermarking approach
(a) The original image (b) The original watermark
(b) The watermarked image (d) The extracted watermark

## REFERENCES

[1] R S Kavitha , U Eranna , and M N Giriprasad "DCT-DWT Based Digital Watermarking and Extraction using Neural Networks" , 2020 International Conference on Artificial Intelligence and Signal Processing (AISP)
[2] Purnima Pal, Harsh Vikram Singh, Sarvesh Kumar Verma "Study on Watermarking Techniques in Digital Images", Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)
[3] Prof. R. D. Salagar1 , Miss. Akshata S. Kamatagi "Image Watermarking Based On DWT, DCT and SVD Technique", International Journal Of Engineering And Computer Science Volume 4 Issue 6 June 2015
[4] Yuqi He , Yan Hu "A Proposed Digital Image Watermarking Based on DWT-DCT-SVD",2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference(IMCEC 2018)
[5] Ahmed A Mohammed1, Bilal A Jebur1 and Karam M Younus "Hybrid DCT-SVD Based Digital Watermarking Scheme with Chaotic Encryption for Medical Images", International Ninevah Conference on Engineering and Technology (INCET 2021)
[6] Hai Tao, Li Chongmin, Jasni Mohamad Zain, Ahmed N. Abdalla "Robust Image Watermarking Theories And Techniques: A Review" , Journal of Applied Research and Technology, Vol. 12, February 2014
[7] Jaya Jeswani, Tanuja Sarode, "A Hybrid DCT and DWT Color Image Watermarking in RGB Color Space" IJSCIT, vol. III, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY