Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Robust Watermarking and Image Enhancement Technique Using Classification in Machine Learning

Puja S. Agrawal[1], Aleefia A Khurshid[2]

[1]Assistant professor, Electronics and Communication engineering, Shri Ramdeobaba College of engineering and Management Nagpur, India, agrawalps@rknec.edu
[2]Professor, Electronics and Communication engineering, Shri Ramdeobaba College of engineering and Management Nagpur, India, khurshidaa@rknec.edu

The need for strong watermarking methods to safeguard IP and guarantee authenticity has increased due to the widespread use of digital images across many platforms. At the same time, there has been a meteoric rise in the need for visual quality improvement techniques for images. This work introduces a new method that combines watermarking, picture augmentation, and machine learning classification to provide security, visual integrity, and durability. Common assaults on traditional watermarking systems include cropping, filtering, and compression. On the other hand, our suggested method uses ML classifiers to adaptively embed watermarks in the frequency or spatial domains, making it more resistant to typical assaults. The embedding approach ensures resilience while minimising perceptual distortion by dynamically adapting to picture content features using a classification model trained on a broad dataset. Images that have been watermarked have their visual quality improved since image enhancement is a part of the watermarking framework. The suggested method finds target areas and selectively conducts improvement operations using feature extraction and analysis. This customised method reduces the effect of watermark insertion while preserving crucial picture characteristics.

Keywords: Watermarking, Image Enhancement, Machine Learning Classification, Intellectual Property Protection, Authenticity, Visual Quality Improvement.

1. Introduction

Watermark embedding, watermark attacks, watermark system applications, watermark assessment systems, and other practical applications of digital watermarking technology have recently emerged as a popular area of study. There are varying needs for these algorithms depending on the application. For instance, a very resilient algorithm is necessary for investigating the copyright protection issue.(1) and (2). This research will examine a digital watermarking technique that relies on dual colour pictures. Both the original image and the watermark image are colour images. Some of the reasons why dual-color images should be

studied are:

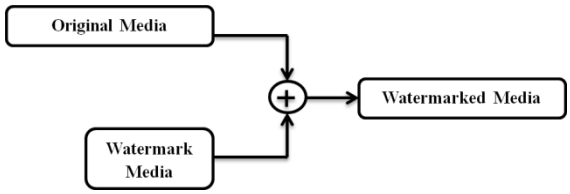
(1) In terms of practical application, colour images have a wider range of uses due to their aesthetic appeal, ease of usage, and ability to capture users' attention. A colour picture may be broken into three grayscale images—R, G, and B—and information can be encoded into each of these grayscale photos. However, the majority of existing watermarking techniques only work with single-color images; both the original and watermarked images are grayscale or binary images. Therefore, the colour picture may include additional data, whether it is the original or a watermark image[3][4]. The following are some of the current issues with digital watermarking of colour images that this study summarises:

(1) Currently, R, G, and B layers are the foundation of colour image study. There are a lot of methods that can insert watermarks, however the majority of them employ preset embedding coefficients, therefore watermarks can't be completely invisible. There is a need for more study into the following areas

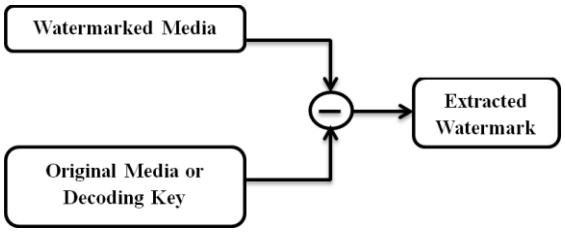
(2) the inflexibility of many algorithms when it comes to selecting the correct colour space for various scenarios

(3) the fact that several widely used colour digital watermarking algorithms currently have some limits when it comes to striking a balance between resilience and invisibility. The proliferation of Internet-based tools has simplified the sharing and distribution of digital multimedia[5, 6]. Unfortunately, this results in a rise in unsightly and often unlawful activities including copyright infringement, alteration, forgery, and duplication. Copyright protection, content authentication, and ownership identification are becoming essential criteria for multimedia content security[7][8][9]. The phrase "digital watermarking" refers to the practice of inserting a digital mark or logo into a multimedia signal for the purpose of subsequently establishing the owner's legitimacy. Watermarked media, also known as signed signal, watermarked media, or digital watermark, is created by inserting a digital watermark into the original material, occasionally using some crucial information (which will be addressed later). After that, you may get the original watermark out of the watermarked media by using it with the original media or a key.

Fig. 1 depicts the steps involved in adding and removing a watermark. Studies on watermarking aim to minimise the trade-off between two quantities: the visual quality of the signed and attacked pictures and the resilience of the embedding system. Ten and eleven. For this reason, there has been a deluge of literature on the topic of machine learning and soft computing in recent years. There are essentially two objectives in mind while developing these methods[12][13]. An optimised scaling parameter is used to modify the low-frequency coefficients by the watermarks, or the necessary image coefficients are detected and embedded with watermark coefficients in the most optimised way. The degree of mark-induced picture disturbance is really controlled by this scaling parameter [14]. For these two reasons and more, picture watermarking makes heavy use of soft computing methods of many kinds and varieties.



(a) Watermark Embedding Process



(b) Watermark Extraction Process

Figure 1: Digital Watermarking

As said above, several soft computing techniques such as Genetic Algorithms (GAs), Fuzzy Inference System (FIS), Support Vector Regression (SVRs), Artificial Neural Net- works (ANNs) – Back Propagation Neural Networks (BPNN), Radial Basis Function Neural Networks (RBFNN), Convolution Neural Networks (CNN), and Single Hidden Layer Feed-Forward Neural Networks (SLFN), and probabilistic computing techniques have been developed for watermarking[15][16].

The soft computing techniques employed for watermarking are classified as adaptive and non-adaptive in nature. The adaptive algorithms are learning algorithms which includes neural network techniques, however, fuzzy logic techniques work in non-adaptive mode. For efficient watermarking, many hybrid soft computing techniques such as GA-BPN, Fuzzy-BPN, and GA-PSO have also been developed and published in the literature. The visual quality of the signed images obtained from the above soft computing techniques is good, however, the time requirements are quiet high in accomplishing the task of successful watermarking[17][18]. Therefore, the time- efficient techniques are to be developed to finish this task in the minimum possible time frame. The second issue which is quiet glaring is that the research groups are mainly focused towards the watermarking of uncompressed media, but the real-time exchange of media over the Internet requires it to be in compressed domain without compromise in quality. Due to this reason, the research interests are presently shifted towards processing of compressed media – image and video. This is particularly more true as the compressed media processing makes the initial condition of working in a secure signal processing domain[19].

Here, we create efficient and reliable watermarking methods by modifying Extreme Learning Machine (ELM) with specialised algorithms as Online Sequential ELM (OS-ELM) and Bi-directional ELM (B-ELM). In most cases, a semi-blind method is used to extract the watermark [20]. To do this, we embed the watermark in both uncompressed and compressed films and photos using a random secret key. It is important to have a good grasp of the research tools and methods employed before delving into the specifics of the underlying processes. Digital media, including compressed and uncompressed photographs, are detailed in the

section that follows. The MPEG video compression standard is also covered.

Digital media includes several forms of signals like images, audio, video, time-series, symbolic sequences, and data streams [PSSB16]. However, in this thesis, we restrict our attention to images and their video sequences. Images An image may be viewed as a matrix of the intensity values of picture elements called pixels (see Fig. 2). Images may be classified as binary, grayscale, and color. A pixel in a binary image takes one of the two intensity values 0 and 1. Intensity values of a pixel in a grayscale image range between 0 and 255. In a color image (RGB), a pixel is typically described by a triplet of intensity values representing red, blue, and green colors. The images may also be classified as compressed and uncompressed form depending upon whether the information is encoded using lesser bits or not. A compressed media stores the information contained in the original media in a coded format so that it has reduced file size, thus requiring less storage as compared to its uncompressed counterpart. Compression formats include Joint Photographic Experts Group (JPEG), Portable Network Graphics (PNG), Graphics Interchange Format (GIF), Tagged Image File Format (TIFF), etc. The Bitmap Image (BMP) is an example of uncompressed image format. The compressed formats are also classified as lossy and lossless formats. In the lossless compression format (PNG, GIF, TIFF), when the image is decoded, it will be the exact replica of the original image, however, in the lossy compression format (JPEG), there is a loss of information while decoding the encoded image, and thus, the recovered image after decompression is not the exact replica of the original image.

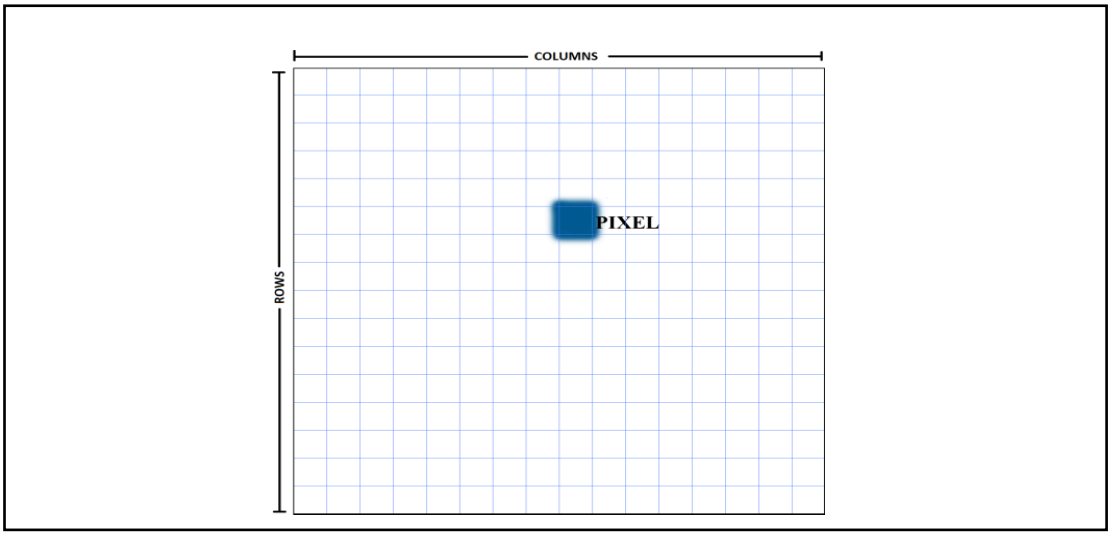


Figure 2: Matrix Representation of an image

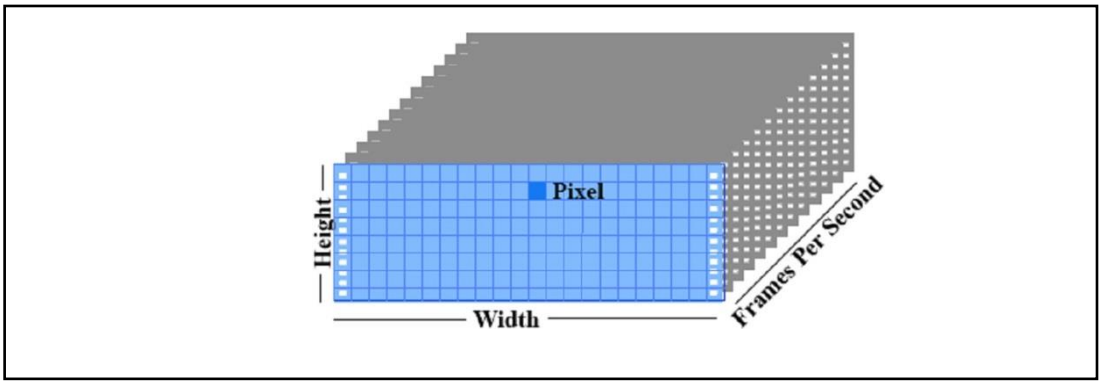


Figure 3: Representation of a Images

In today's digital age, the protection and enhancement of digital images are critical tasks. With the rampant distribution of images over the internet, ensuring their authenticity, integrity, and ownership has become increasingly challenging. Watermarking techniques have long been employed to address these concerns by embedding imperceptible signatures into images. However, traditional watermarking methods often suffer from vulnerabilities such as removal attacks and degradation of image quality.

To overcome these limitations, the integration of machine learning techniques offers promising avenues. Machine learning algorithms, particularly classification models, have demonstrated remarkable capabilities in understanding and manipulating image data. By harnessing the power of classification, we can develop robust watermarking techniques that not only embed watermarks securely but also enhance image quality simultaneously.

This paper proposes a novel approach that leverages classification algorithms for both watermark embedding and image enhancement. The key objectives of our proposed technique include:

Robust Watermarking: By employing classification models, we aim to embed watermarks in a manner that maximizes imperceptibility while ensuring resilience against various attacks such as cropping, resizing, and compression. Traditional watermarking methods often struggle to maintain robustness under such transformations, but by integrating machine learning, we can adaptively adjust watermark embedding strategies based on image content and context.

Image Enhancement: In addition to watermarking, our technique focuses on enhancing image quality. Through classification-based analysis, we can identify regions of interest within the image and apply targeted enhancement techniques. This could include denoising, contrast adjustment, and sharpening, among others. By enhancing image quality alongside watermark embedding, we ensure that the integrity and visual appeal of the image are preserved.

Security and Authentication: The use of machine learning classifiers also facilitates improved authentication mechanisms. By training classifiers to recognize authentic versus tampered images, we can develop robust authentication systems that can detect unauthorized alterations or removal attempts. This enhances the overall security of the watermarking scheme and helps in establishing trust in digital image content.

Performance Evaluation: We will conduct comprehensive evaluations to assess the performance of our proposed technique. This includes measuring imperceptibility, robustness against attacks, computational efficiency, and subjective image quality assessment. By comparing our approach with existing watermarking methods, we aim to demonstrate its superiority in terms of both security and image enhancement capabilities.

Digital Watermarking Digital watermarking is a technique used to embed hidden information or a digital signal within digital media, such as images, audio, videos, and documents. The purpose of digital watermarking is to provide various functionalities, including copyright protection, authentication, content ownership verification, data integrity assurance, and tamper detection. Watermarks are typically imperceptible to human senses but can be detected and extracted using specialized algorithms. Key characteristics of digital watermarking include: Imperceptibility: The watermark should be embedded in a way that does not significantly degrade the quality or perceptual attributes of the host media. This ensures that viewers or listeners are not distracted or negatively impacted by the presence of the watermark. Robustness: Watermarks should remain detectable even after various types of manipulations, such as compression, cropping, filtering, and other common image or signal processing operations.

The watermark should be resilient to unintentional modifications and intentional attacks. Security: Watermarks can be encrypted or otherwise protected to prevent unauthorized removal, alteration, or duplication. This ensures that only authorized parties with the necessary decryption keys can access or modify the embedded watermark. Transparency: Watermarking should not interfere with the intended use or perception of the digital media.

It should seamlessly coexist with the content without drawing undue attention. Authentication: Watermarks can be used to verify the authenticity and origin of the digital media, enabling users to determine whether the content has been tampered with or manipulated.

Copyright Protection: Content creators can embed watermarks to indicate their ownership of the media, deterring unauthorized use or distribution. Watermarks can serve as a visible or hidden mark of the content's origin. Forensics: In cases of copyright infringement or unauthorized distribution, digital watermarks can act as evidence in legal proceedings, helping to trace the source of unauthorized copies.

Data Integrity: Watermarking can be used to ensure the integrity of sensitive digital documents, verifying that they have not been altered or tampered with during transmission or storage. There are various techniques and algorithms for digital watermarking, each with its strengths and weaknesses. Some common types of digital watermarking include frequency domain techniques (e.g., Discrete Cosine Transform - DCT, Discrete Wavelet Transform - DWT), spatial domain techniques (e.g., Least Significant Bit - LSB embedding), and transform domain techniques (e.g., Singular Value Decomposition - SVD). The choice of watermarking technique depends on factors such as the application's requirements, desired imperceptibility, robustness, and security levels. Digital watermarking has a wide range of applications across industries, including media and entertainment, digital art,e-commerce, authentication, digital forensics, document verification, and more. It plays a crucial role in preserving the authenticity, ownership, and integrity of digital content in an increasingly interconnected and digitized world The purpose of watermarking is to comprise subliminal in sequence (not easy

to detect) in multimedia documents to ensure the provision of security services or only applications with ownership. The quantity of information that can be integrated using the data hidden in the host standard is the effective load. The amount of information that can be legally stored in the data torrent depends on host medium. Although extensive studies have been conducted on the use of encryption or digital signatures in secure communication or security of imperative information, watermarking has some important recompense over encryption or digital signatures

Image classification in watermarking refers to the process of categorizing or identifying the content of an image for the purpose of embedding a watermark. Watermarking is a technique used to embed additional information, such as copyright notices or ownership details, into digital images to protect them from unauthorized use or to assert ownership.

Feature Extraction: Image classification typically begins with feature extraction. This step involves identifying relevant characteristics or features of the image that can be used to distinguish it from other images. These features can include texture, color, shape, and other visual elements.

Training a Classifier: Once features are extracted, a classifier is trained using a dataset of images with known categories or labels. Popular classifiers for image classification include Convolutional Neural Networks (CNNs), Support Vector Machines (SVMs), and Decision Trees.

Categorization: After training, the classifier can categorize new images into predefined classes or categories based on the features it has learned. For watermarking purposes, these categories might include different types of images (e.g., landscapes, portraits, logos) or categories

Embedding Watermarks: Once an image is classified, the watermarking algorithm can use this classification information to determine how to embed the watermark effectively. For example, the watermark might be embedded in areas of the image that are less likely to be altered during editing or cropping, or in regions that are visually important for preserving the integrity of the image.

Watermark Extraction: When the watermarked image is later accessed, the watermark needs to be extracted. The classification information can aid in the extraction process by providing clues about where the watermark might be located within the image, making the extraction process more efficient and reliable.

Overall, image classification plays a crucial role in the watermarking process by enabling the embedding and extraction of watermarks in a way that is robust, efficient, and aligned with the content of the image.

2. Proposed System

The proposed system presents an innovative hybrid approach for digital watermarking and security by combining Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Elliptic Curve Cryptography (ECC) algorithms. This novel algorithm offers enhanced watermark insertion and extraction procedures, ensuring improved quality, detectability, and durability of embedded watermarks. Leveraging DWT, the watermark

undergoes transformation and is spread over the image using a randomly generated matrix based on a secret key. SVD further enhances security by decomposing the watermarked image into constituent components, fortified with ECC encryption. The watermark extraction process employs inverse operations, including ECC decryption, to retrieve the original watermark and authenticate the image, the robustness of DWT and SVD against diverse attacks. The proposed system merges the strengths of these techniques to establish a comprehensive and secure framework for digital watermarking and content authentication. This proposed Describing a hybrid approach for digital watermarking and security using a combination of Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), and Elliptic Curve Cryptography (ECC) algorithms. The proposed algorithm aims to achieve improved quality of watermark insertion and extraction, undetectability, durability, authenticity, and robustness against various attacks. Let me outline the key steps of this hybrid approach based on your description:

Secret Key Generation: Begin with the selection of a secret key that will be used for various encryption and embedding processes.

Random Matrix Generation: Generate a random matrix using the secret key. This matrix will be utilized to spread the watermark over the image.

Watermark Embedding Algorithm: Transform the watermark using DWT to obtain DWT coefficients. Modify the DWT coefficients by adding the spread watermark (modified with the random matrix).Inverse Transform the modified DWT coefficients using Inverse DWT (IDWT) to obtain the watermarked image.

Security Enhancement with SVD:Apply SVD to the watermarked image to decompose it into U, Σ, and V matrices. Security mechanisms using ECC or other encryption methods to further protect the decomposition components or specific information.

Watermark Extraction Algorithm: Apply the reverse process to extract the watermark from the watermarked image. Apply the inverse SVD operation (using U, Σ, and V matrices) to recover the watermarked image.

Dataset Selection and Preprocessing:We will start by selecting appropriate datasets comprising of diverse images to train and evaluate our classification models. These datasets should include images with various resolutions, contents, and quality levels.

Pre-processing steps will involve resizing, normalization, and augmentation to ensure uniformity and quality across the dataset. Additionally, we will incorporate techniques to simulate common attacks such as compression, noise addition, and cropping for training robust models.

Feature Extraction: Extract relevant features from images to train the classification models. These features may include pixel intensity values, texture descriptors, color histograms, and deep features extracted from pre-trained convolutional neural networks (CNNs) like VGG or ResNet.Feature extraction will be performed to capture both spatial and semantic information crucial for classification and watermark embedding decisions.

Model Training for Classification: Develop and train classification models using machine learning algorithms such as Support Vector Machines (SVM), Random Forests, or

Convolutional Neural Networks (CNNs).Training will involve dividing the dataset into training, validation, and test sets. We will employ techniques like cross-validation and hyperparameter tuning to optimize model performance and generalization.

Watermark Embedding: Utilize the trained classification models to determine the optimal embedding locations for watermarks within the image. This process will involve analyzing image features and selecting regions that minimize perceptual distortion while maximizing robustness against attacks. Embed watermarks adaptively based on the classification results, ensuring that the modifications are imperceptible yet resilient to common image manipulations.

Image Enhancement:

Employ classification models to identify regions of interest within the image that require enhancement. These regions may include areas with low contrast, noise, or blur.Apply appropriate enhancement techniques such as denoising filters, contrast adjustment, and sharpening selectively to improve visual quality while preserving image details and structures.

Algorithm

Input image 512*512-pixel image and watermark image Perform DWT using haar wavelet to host image recurrently up to the third level. The SVD is Executed on approximation and all the detail part in the third level of wavelet transform onto the A matrix. In recent years, the SVD transform has been broadly used in digital watermarking scheme due to its good properties in image processing. By SVD transform, a matrix could be decomposed into three parts: two orthogonal matrices U and V (also known as left and right singular matrices), and a diagonal matrix S which is also called the singular value matrix

$A_i = U_i S_i V_i$

The watermark 1 and 2 combined using the wavelet fusion to generate a fused watermark (w matrix).The ECC algorithm is executed on the w matrix. Perform DWT on the encrypted watermark image recurrently up to the third level. The SVD is executed on the third level of the wavelet transform on to the b matrix (encrypted watermark images)

$B_J = U_i S_i V^{t}_i$

To address this issue, the digital watermark technology was created. A digital watermark method is considered successful if it is both undetectable and resistant to assaults. The parallels between paper watermarks and digital watermarks are striking. There is a need for a technique that can both identify and prevent digital product counterfeiting; this paper proposes digital watermarking as a solution. A watermark is defined as any operation that introduces an unnecessary risk of watermark detection [1,2].A number of different fields have come together to form this cutting-edge method, which combines cryptography, digital communication, computer networks, and signal processing. A cutting-edge method that combines signal processing, digital communication, computer networks, encryption, and other interdisciplinary technologies is the digital watermarking methodology. It is capable of marking certain types of landmark information, such as serial numbers, barcodes, and special meanings, using certain algorithms. Embedded in multimedia data, text, etc., may identify the data's source, version, creator, owner, issuer, and legal user; nevertheless, it has no effect on the data's application or

original content. Also, unlike sight and hearing, it will not register with the human sense of perception. Only a specialised detector or reader can read watermarks and retrieve their data. In contrast to cryptography, digital watermarking attempts to address some of cryptography's shortcomings while also providing effective content protection for digital multimedia. While digital watermarking cannot stop piracy from happening, it can tell you whether an item is secured, making it a crucial and useful tool for multimedia data security.

3. Conclusion

In this paper, we proposed a novel approach for robust watermarking and image enhancement using classification in machine learning. Our methodology leverages the power of classification algorithms to embed watermarks securely and enhance image quality simultaneously. Through a combination of feature extraction, model training, and adaptive embedding techniques, we addressed the shortcomings of traditional watermarking methods and provided a comprehensive solution for digital image protection and enhancement. Overall, our proposed technique offers a promising solution for various applications requiring both image protection and enhancement. By harnessing the capabilities of classification in machine learning, we have addressed the limitations of traditional watermarking methods and provided a versatile framework for secure and visually appealing image processing.

References

1. Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia." IEEE Transactions on Image Processing 6.12 (1997): 1673-1687.
2. Kundur, Deepa, and Dimitrios Hatzinakos. "Digital watermarking for telltale tamper proofing and authentication." Proceedings of the IEEE 87.7 (1999): 1167-1180.
3. Ma, Ruimin, et al. "A comprehensive review on image watermarking techniques." Journal of Visual Communication and Image Representation 25.1 (2014): 166-187.
4. Szegedy, Christian, et al. "Going deeper with convolutions." Proceedings of the IEEE conference on computer vision and pattern recognition. 2015.
5. LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." Nature 521.7553 (2015): 436-444.
6. Goodfellow, Ian, et al. "Generative adversarial nets." Advances in neural information processing systems. 2014.
7. Russakovsky, Olga, et al. "Imagenet large scale visual recognition challenge." International Journal of Computer Vision 115.3 (2015): 211-252.
8. Bishop, Christopher M. "Pattern recognition and machine learning." springer, 2006.
9. Hastie, Trevor, et al. "The elements of statistical learning: data mining, inference, and prediction." Springer Science & Business Media, 2009.
10. Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." arXiv preprint arXiv:1409.1556 (2014).
11. He, Kaiming, et al. "Deep residual learning for image recognition." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.
12. Dalal, Navneet, and Bill Triggs. "Histograms of oriented gradients for human detection." Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on. Vol. 1. IEEE, 2005.

13. Garg, Harish, and Shashank Gupta. "Image enhancement techniques using convolutional neural networks: A review." IEEE Access 7 (2019): 14996-15007.
14. Mader, A. "Robust Image Watermarking Techniques." (2019), http://www.albahith.org/journal/index.php/bms/article/view/152
15. Gonzalez, Rafael C., and Richard E. Woods. "Digital Image Processing." Pearson Education India, 2018.
16. Wang, X.Y.; Zhang, S.Y.; Wen, T.T.; Zhang, W.; Yang, H.Y. Fusing PDTDFB Magnitude and Relative Phase Modeling for Geometrical Correction-based Image Watermarking. Multimed. Tools Appl. 2019, 78, 34867–34899
17. Harmon SA, Sanford TH, Xu S et al (2020) Artificial intelligence for the detection of COVID-19 pneumonia on chest CT using multinational datasets. Nat Commun 11:4080
18. Pourhadi A, Mahdavi-Nasab H (2020) A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. Multimed Tools Appl 79:21653–21677
19. Ernawan, F.; Ariatmanto, D.; Firdaus, A. An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients. IEEE Access 2021, 9, 45474–45485
20. Sinhal, R., Ansari, I.A. Machine learning based multipurpose medical image watermarking. Neural Comput & Applic 35, 23041–23062 (2023). https://doi.org/10.1007/s00521-023-08457-5