Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.754693

ADAPTIVE DIGITAL IMAGE WATERMARKING WITH CONVOLUTIONAL NEURAL NETWORKS: ADDRESSING VARIED WATERMARK CHARACTERISTICS AND IMAGE RESOLUTIONS

M. Narasimhulu[1a)], D. Veera Mounika[2b)], P. Varshini, Amarendra K[3c)], TK Rama Krishna Rao[4d)], P V V S Srinivas*[5e)]

Author Affiliations

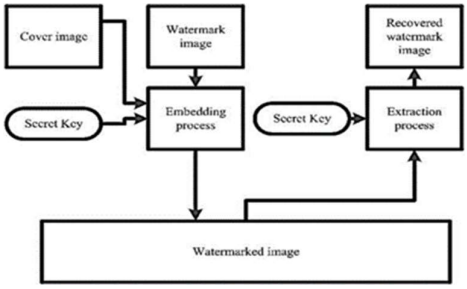
Dept. of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India-522502

Abstract

Due to the simplicity of picture tampering, ensuring the authenticity of digital photographs has grown to be a crucial concern in the age of digital transformation. Researchers have been actively tackling this problem for the past few decades, attempting to create efficient image watermarking methods suited to varied applications. The challenge of developing a watermarking system that balances security and resilience still exists. This article summarizes common watermarking frameworks and identifies the important criteria that need be met before developing new techniques for various purposes. It also examines contemporary developments in digital picture watermarking with the purpose of identifying novel approaches and their accompanying drawbacks. Additionally, the report examines conventional attacks and offers prospective lines of inquiry for further study. This research used a novel blind. A digital picture watermarking technique that functions well with both color and grayscale photos is introduced. The method uses the Discrete Cosine Transform (DCT) as a first step before embedding the watermark. Before performing the DCT, the host image is partitioned into 8x8 nonoverlapping blocks, and the watermark bit is integrated by adjusting the difference between the DCT coefficients of neighboring blocks. The Arnold transform and chaotic encryption are coupled to increase security, resulting in a two-layer security strategy for the watermark. The findings from simulations show that the

suggested method demonstrates resilience to various image processing operations such as compression, sharpening, cropping, and median filtering. The paper studies and evaluates three alternative iterations of this algorithm. In comparison with current methods, the suggested scheme performs better than average in terms of imperceptibility, security, and robustness. Given these benefits, the suggested technique shows promise for use in fields like telemedicine and e-healthcare, providing a reliable solution for hiding electronic health records within medical photographs.

Key Words: Sentence case; Separate by semicolon (;) between keyword



Introduction

Based on how robust the watermark is, digital Three categories of watermarking techniques exist: semi-fragile, fragile, and robust. By doi.org Strong watermarks withstand the majority of image processing techniques and are perfect for copyright protection. With modest adjustments, fragile watermarks vanish, making them good for authentication. Pixel and coefficient domains contain watermarks. Pixel domain is simple, has a high payload, but isn't very robust. Coefficient domain is computationally complex but has excellent robustness. One often used transform is DWT. DCT Favors inexpensive hardware. Copyright protection is best served by embedding in low-frequency coefficients, authentication is best served by high-frequency, and robustness and imperceptibility are best served by mid-frequency. [] In order to overcome the difficulties brought on by the simple copying, modifying, and applications. It also summarizes the study and provides results and metrics. [] A digital watermark needs to have the following essential qualities in order to be useful Flexibility: The algorithm must enable varying levels of resilience, quality, or embedding capacities to be tuned to suit different applications.

Robustness: To prevent illegal removal, the implanted watermarks should withstand typical processing methods such as compression, filtering, cropping, and quantization.

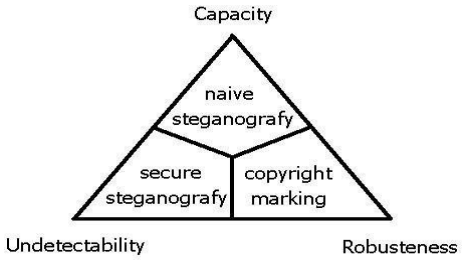
Security: To maintain security, watermarking should rely on secret keys. Without access to these keys, it will be difficult for unauthorized users to identify or erase watermarks.

Imperceptibility: To ensure that their existence does not lower the quality or human perception of the content, watermarks should be unnoticeable in digital music or invisible in photographs. Peak signal-to noise ratio (PSNR) measurements and subjective evaluations are frequently used to assess this. Instantaneous processing Watermark [] By describing the inputs, outputs, and features of watermarking systems for various goals, the suggested model helps to characterize these techniques. It facilitates the development of watermarking features based on application needs and makes it possible to analyse these schemes in detail. A flawed computational analysis caused by an incomplete model may introduce technological weaknesses and protocol vulnerabilities that adversaries could exploit. The study also looks at prospective assaults to identify the advantages of the opposition in various circumstances.

Image Watermarking Backgrounds and Frameworks

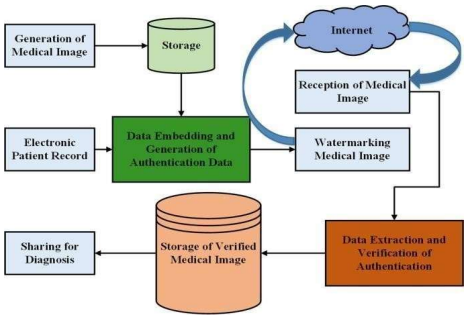
The spread of worldwide computer networks and multimedia platforms has facilitated widespread access to digital content. Watermarking digital images is essential for preventing unlawful distribution, copying, alteration, and illegal possession of digital data. With the advent of digital technology in 1988, traditional paper watermarking has developed. Host signals contain watermarks, which are later retrieved and used as proof of owner validity. To achieve a harmony between invisibility, resilience, and capacity in digital picture watermarking that is in line with The Just Noticeable Difference (JND) model, information entropy, and human visual perception (www.mdpi.com) are utilized. [] Digital picture watermarking comprises two basic steps: embedding and extraction in a secure communication context.

The cover image is first preprocessed to establish its capacity for integrating information, and



its entropy is then evaluated. Using a secret key, an optical image encoding technique is utilized to embed a watermark picture into the high entropy areas of the host image. Pre-processing the watermarked image is a step in the extraction process. After that, the laser beam patterns' amplitude and phase information are extracted, and their entropy is assessed in order to choose a high entropy value for the watermark extraction. This guarantees imperceptibility and robustness. Both processes use security keys: the embedding process for the watermark is controlled by a function, while the extraction procedure is accomplished by a decoder function. This strategy yields straightforward, reliable, and imperceptible watermark image reconstruction from the watermarked image. Watermarked Image, DW = E (I, ETP, W, K) he watermarking process involves an encoding algorithm E, using the cover image I, information entropy ETP, watermark image W, and security key K. The watermark extraction is achieved with a decoding algorithm e, resulting in the watermark image W'.

Design Requirements of Image Watermarking System:



A watermark must be identifiable even after typical signal processing techniques like filtering, compression, and transformations have been used in digital picture watermarking systems. Methods like spread spectrum and redundant embedding can be used to achieve robustness.

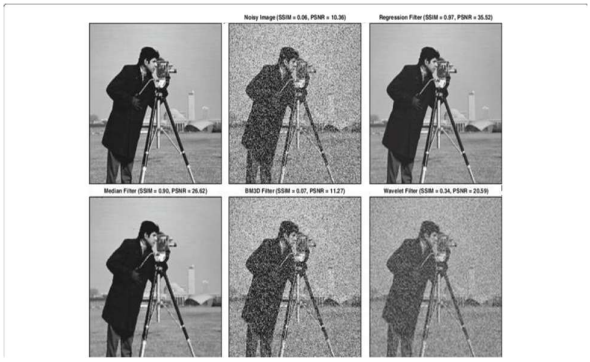
Unauthorized users should find it challenging to remove or tamper with the watermark thanks to a robust watermarking mechanism that can withstand a range of attacks. Different watermarking algorithms can have varying degrees of robustness, and they can be categorized as robust, fragile, or semi-fragile depending on how well they resist different types of attacks.

The trade-off among imperceptibility, robustness, and capacity

Robustness for Various Attacks:

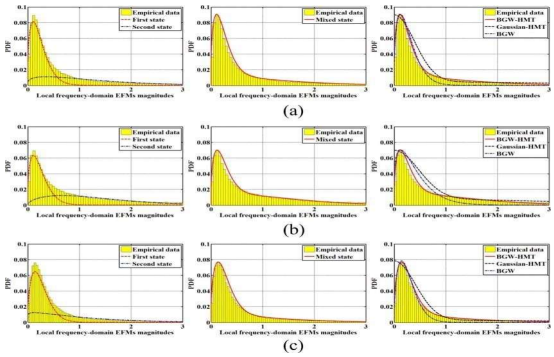
Robustness tests were run using the training weight set on the evaluation dataset. Various attack kinds and intensities were used, and examples of the attacked images are shown in By weakening or deleting the watermark, these assaults aim to use the image without permission, either purposefully or accidentally. However, certain attacks severely destroy the image, making them unusable afterward. These assaults were nevertheless included for comparison with earlier works. The results of the experimental robustness, particularly the bit error rate (BER) at s = 1. For each form of attack, the BER values tend to rise when attack power does as well. Notably, the rotation assault affects image data most significantly at 45 degrees. As a result, the BER rises. up to a 45degree rotational angle, but after that point, it becomes less. This finding implies that the suggested network was successfully trained without being too tailored to a particular attack strength. As shown by consistently low bit error rates (BERs) below 10%, the study of the table values demonstrates a good level of robustness in the majority of pixel-value change attack scenarios. This robustness applies to a variety of attacks, with the exception of certain circumstances. These exclusions include assaults using larger Gaussian filters (7x7 or above), attacks using Gaussian noise with a standard deviation () greater than 0.08, and attacks using JPEG compression settings higher than quality level 40. The system impressively demonstrates amazing resilience when attacked with salt-and-pepper noise addition, highlighting its ability to successfully survive such interruptions. The technology efficiently protects the integrity of watermarked images from rotation attacks when it comes to geometrical attacks. When exposed to crop and crop-out, though images. On the other hand, the system encounters larger BERs, exceeding 50%, when subjected to crop and crop-out attacks. The system also struggles to remain resilient against dropout attacks that reach 30%. It is important to note that the proposed method reacts to various attacks differently, leading to differing BERs. This emphasizes how crucial it is to provide specialized solutions to efficiently counter particular sorts of attacks.

Invisibility–Robustness Controllability:



Controlling the trade-off between robustness and invisibility is essential in a watermarking

system because it enables users to give either one priority depending on their particular demands. In our method, this control is accomplished by employing a strength scaling factor, represented by the letter "s." A smaller value is given to "s" when invisibility is prioritized above robustness, whereas a larger number is utilized when greater robustness is a priority. We performed tests with values increasing from 0.5 to 2 to assess the system's robustness, controllability, and invisibility against a variety of threats. The findings are shown in, which also shows modifications to robustness and invisibility for various types and intensities of attacks. Figure 7a shows a decrease in a watermark, as expected. As's' rises, (WM) invisibility increases. On the other side, by doi.org for each attack, robustness steadily gets better with increases,' while keeping performance trends in line with variations in attack power. This highlights forcefully how us suggested strategy successfully and flexibly controls the delicate balance between invisibility and resilience, enabling users to customize the system to their particular needs.



Analysis of Previous Methods:

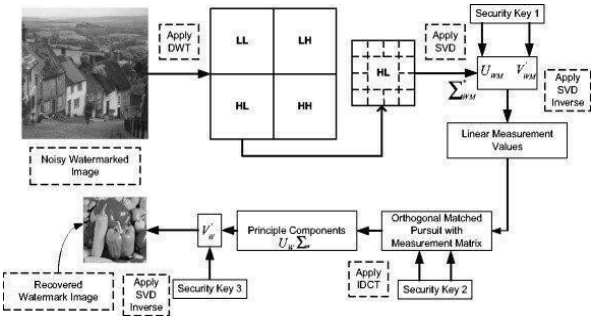
Spatial and transform domains are They fall into two major categories (doi.org) digital picture watermarking techniques fall. With this technique, the watermark is immediately included in the pixel values of the host image. Typical spatial domain methods include:

The watermark is injected into the least significant bits of the image pixels using the LSB (Least Significant Bit) Embedding basic technique.

Spread spectrum approaches: By dispersing the watermark data across the entire image, these techniques make the watermark resistant to a variety of attacks.

Techniques for the area of space using visual models: These techniques ensure that The doi.org watermark is used. undetectable by taking into account the features of the human visual system (HVS).

Watermarking that transforms the host image into a new image is referred to as watermarking of transform domains. By doi.org the coefficients of the modified data are embedded with the



watermark (for example, frequency domain). DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) (www.ijtrs.com) (modernloveok.com) are two popular transform domain approaches. These techniques are frequently used for image compression and work well for incorporating watermarks. (www.ijtrs.com) Singular Value Decomposition (SVD): SVD-based methods alter the image's singular values to obscure the watermark.

Quantization strategies These techniques embed the watermark in the transform coefficients via quantization These approaches can be used in various situations and applications because each has advantages and disadvantages. Depending on the precise needs of the watermarking task, such as imperceptibility, resilience, and capacity, a particular approach be put to use. The section at doi.org of image watermarking approaches into three categories—domain-based, perception-based, and document-based—is shown in. Spatial domain (using image pixels) and spectral domain (using frequency components) are further categories for domain-based approaches. This review focuses on perception-based, spectral domain, and spatial domain watermarking systems while considering the many content types, including text, image, audio, and video (doi.org) (www.datapine.com) and video.

Related works:

The field of digital picture watermarking has been studied from many angles and with many different methods

Picture watermarking: Watermarking approaches that directly insert themselves into an image's spatial domain are explored under this heading. By doi.org This category includes techniques like spread spectrum and LSB (Least Significant Bit) embedding.

Watermarks are embedded into transformed coefficients using transform domain techniques, which concentrate on changing the host image into other domains (For instance, www.datapine.com) frequency domain). In this field, techniques Singular value decomposition (SVD), discrete wavelet transform (DWT), and discrete cosine transform (DCT) are based on the (doi.org) (www.hindawi.com) frequently used.

Perceptual watermarking: This technique ensures that watermarks are undetectable to the human eye by taking into consideration how people see images. They frequently use visual representations to attain robustness and Security: By depending on encryption and cryptography methods, research is being done to improve the robustness of watermarks against various attacks.

Digital picture watermarking has a variety of uses, including copyright protection, authentication, medical imaging security, and multimedia content protection, which are all explored by researchers.

Steganography and Watermarking: To (www.datapine.com) in order create hybrid techniques, some study investigates the borders between steganography (which conceals the existence data) as well as (www.datapine.com). watermarking (which embeds data within the material). Metrics for Evaluating Watermarked Images: Research is now being done going to (archive.org) provide metrics for evaluating the quality, resilience, and imperceptibility of watermarked images. For this aim, metrics like SSIM (Structural Similarity Index) and PSNR (Peak Signal-to-Noise Ratio) are frequently utilized. Researchers are increasingly examining the

application of machine learning (doi.org) and artificial intelligence for embedding and extracting watermarks,
As well as for detecting and preventing attacks.

These topics represent the broad and varied body of relevant research in the subject of digital picture watermarking, which is always evolving as security requirements and technology do. In their notable work, Petit colas and colleagues presented a digital watermarking model with a focus on information hiding. While they provided an overview of the technique, the formal definitions of inputs, outputs, and component functions were omitted, limiting the completeness of the model. Take the (www.datapine.com) as an example. selection or generation of the watermarking key and the mark (representing a hidden serial number or copyright message) should be explicitly defined. Careful thought must enter the data pine website. creation of a reliable digital color image watermarking method. It ought to be blind and function in the frequency range. Dual encryption methods like Arnold transformation and Chaos should (www.datapine.com) be applied to provide robustness. Additionally, Hamming error correction, which has the advantage of being 2-D, can increase defense against attacks. Depending on how susceptible a frequency is to attacks, the method should involve embedding the watermark at several middle frequencies with different watermark values. Better watermark embedding is ensured by this adaptive method.

Structure of Watermarking Network to Be Trained:

A watermarking network's structure typically consists of Many (www.datapine.com) crucial elements. The encoder is in charge of incorporating the watermark into the source image or signal. It frequently uses methods like perceptual modelling, transform domain embedding, or spatial domain manipulation.

Decoder: The decoder's task is on (doi.org). to remove the watermark from images or transmissions that have a watermark. It ought to be able to precisely recover the embedded data.

Loss Function: A loss function accustomed to calculating how much the original and decoded watermarks differ from one another. To (www.datapine.com) in order to reduce this discrepancy, it directs the training process.

Training Data: To properly train the network, you need high-quality, labelled datasets. Pairs of the original photos or signals and their watermarked counterparts are included in this data.

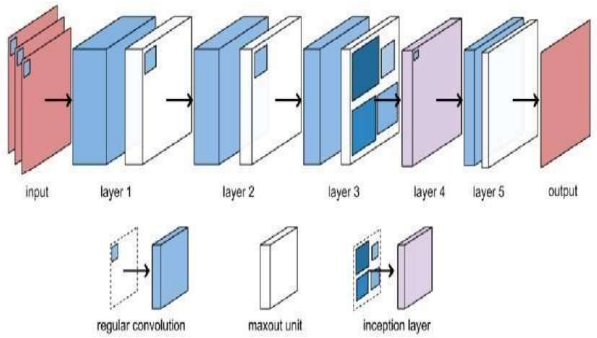
Neural network design: The particular architecture may change. However, makes use of deep neural networks, such as convolutional neural networks (CNNs) for image watermarking. The embedding and extraction of watermarks are processes that these networks learn. Algorithm for Optimization: To optimize the network's parameters during training and reduce the loss function, optimization techniques like stochastic gradient descent (SGD) or Adam are utilized.

Hyperparameters, which must be adjusted for the best network performance, include learning rates, batch sizes, and the quantity of training epochs.

Evaluation metrics: The network's performance is evaluated Regarding (doi.org) imperceptibility, robustness, and data recovery using metrics like PSNR, SSIM, or bit error rate (BER) (doi.org)

In light of the (doi.org) individual watermarking method used and its goals, such as copyright

protection, authentication, or content verification, the watermarking network's precise composition and components may change. The network comprises pre-processing networks for both the host and watermark, a watermark embedding network, and a watermark extraction network. It notably features relatively shallow CNN architecture with a maximum depth of 13 CNN layers. The network's structure and components were determined empirically based on extensive experiments. Another key feature is the watermark preprocessing network, which increases the watermark's resolution to match the host's URL (doi.org) image, contrary to previous approaches that reduced the host image's resolution. This is done to maintain host image information and enhance watermark invisibility, supported by experimental results showing the challenge of achieving invisibility while maintaining robustness. Additional features (doi.org) of the network are discussed in the following sections.



Results and discussions:

Many of them (www.datapine.com) tests using various types and intensities of attacks on the assessment dataset were used to properly test the watermarking system's robustness. discussions and findings related to the robustness of the system. To evaluate the watermark's resistance, a variety of attacks were used in the experimentation. illustrates a few of the photographs that have been the target of these assaults, which provide illustrations of how the watermark has reacted to varied threats. Attacks like this were carried out to gauge the system's capacity to defend the watermarked photos' integrity and ownership. However, it is clear from the figures that several strikes severely damaged the photos, making them useless. To be consistent with earlier research methods, these attacks were nevertheless included for comparison analysis. gives a summary of the research results with the scaling factor set to 1 (s = 1), especially the bit error rate (BER). The robustness of the watermark is quantified using the BER values. As the strength of the applied assault increases, it is shown that the BER tends to rise. This pattern suggests that the watermark becomes less imperceptible under stronger attacks, increasing the risk of watermark extraction mistakes. One interesting finding is connected to the rotation attack. It is discovered that the rotation substantially distorts the image data, particularly at an angle of 45 degrees. As a result, the BER rises up to a 45-degree rotation angle. But as the angle continues to vary from 45 degrees after this point, the BER starts to fall. This action demonstrates that the suggested network was successfully trained to handle several rotation angles and retained robustness against rotation-based attacks without becoming unduly specialized in any single angle. In conclusion, the robustness experiments' findings As evidence, the (doi.org) suggested watermarking method successfully maintains its resilience against a variety of attacks, helping to safeguard the ownership and integrity of digital images.

The network also demonstrates adaptability to various assault strengths and angles, demonstrating its usefulness in real-world circumstances.

Conclusions:

This study makes use of convolutional neural networks (CNNs) (www.researchgate.net) to introduce a digital picture watermarking method that allows for flexibility in the (doi.org) resolution. host image and watermark (WM) information. This method enables utilizing (doi.org) a strength factor to alter the tradeoff between robustness and invisibility. The host image's resolution is matched by the WM preprocessing network, emphasizing invisibility. The embedding network makes use of CNNs to produce the watermarked image while maintaining resolution. Comparable to the doi.org WM information recovery network, the extraction network uses CNNs to reduce resolution. To verify WM resilience, we ran attack simulations with a constant distribution within each mini batch. Notably, this network is made up of straightforward CNNs rather than layers that depend on resolution, for instance, www.datapine.com Fully Connected (FC) layer, guaranteeing adaptability to input image resolution. Additionally, it utilizes randomly generated WM data for each mini batch during training and is unrelated to WM knowledge. The evaluation included tests for invisibility and robustness against various geometric and pixel-value alteration assaults across various host picture resolutions and WM information. The results showed exceptional performance, outperforming state-of-the-art methods, especially in cases involving significant attacks. As a result, our approach shows itself to be both useful and adaptable. We were able to effectively manage Aaltodoc.Aalto.fi is the complementary link between robustness and invisibility by altering the strength factor. As a result, we think that our suggested approach has a lot of potential as a digital image watermarking solution.

With no restrictions on the image hosted by dl.acm.org or WM data, it allows for the flexible embedding and extraction of WMs without the need for additional training. The utility of the method can be further increased by fine-tuning utilizes randomly generated WM data for each mini batch during training and is unrelated to WM knowledge.in invisibility and robustness to satisfy certain user requirements.

References:

1. S. Sinha Roy, A. Basu, and A. Chattopadhyay, Multimedia Tools and Applications, "On the implementation of a copyright protection scheme using digital image watermarking," (dl.acm.org) (www.ijrte.org) vol. 79, no. 19–20, pp. 1312513138, Jan.2020, doi: 10.1007/s11042-02008652-9.

2. J.-E. Lee, Y.-H. Seo, and D.-W. Kim, "Adaptive to the Resolution of Image and Watermark: Convolutional Neural Network-Based Digital Image Watermarking," Applied Sciences, (www.mdpi.com) vol. 10, no. 19, p. 6854, Sep. 2020, doi: 10.3390/app10196854.

3. P. Lefèvre, P. Carré, and P. "Use of rank metric codes in digital image watermarking," by Gaborit, (doi.org) Image Communication in Signal Processing, www.ijrte.org vol. 74, pp. 119–128, May 2019, doi: 10.1016/j.image.2018.12.015.

4. J. Cox, Digital Signal Processing, "A Review of (doi.org) Watermarking Principles and Practices 1" for Multimedia Systems, pp. 461–485, doi: 10.1201/9781482276046-17.

5. H. Nyeem, W. Boles, and C. Boyd"The formal model, fundamental properties, and potential attacks of digital image watermarking," (doi.org) EURASIP Journal on Advances in Signal Processing vol. 2014, no. 1, Aug. 2014, doi: 10.1186/1687-6180-2014-135.

6. Adaptive digital image watermarking for color images in frequency domain, G. S. Kalra, R. Talwar, and H. Sadawarti, Multimedia Tools and (www.tandfonline.com) Applications, vol. 74, no. 17, pp. 6849–6869, (www.hindawi.com) doi: 10.1007/s11042-014-1932-3, March 2014

7. Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," IEEE Access, vol. 6, pp., N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat 19876–19897, 2018, doi: 10.1109/access.2018.2808172.

8. Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "A strong and safe method for watermarking digital images with (core.ac.uk)"

9. logistic and RSA encryption," Expert Systems with Applications, vol. 97, pp. 95–105, May 2018, doi: 10.1016/j.eswa.2017.12.003.

10. U. A. Bhatti et al., "Hybrid Watermarking Algorithm With Arnold Scrambling and Chaotic Encryption Using Clifford Algebra," IEEE Access, vol. (core.ac.uk) 8, pp. (www.researchgate.net) 76386–76398, 2020, doi: 10.1109/access.2020.2988298.

11. M. Yamni, H. Karmouni, M. Sayyouri, and H. Qjidaa, "Image watermarking with separable fractional Charlier-Meixner moments" https://www.researchgate.net

12. Journal of the Franklin Institute, vol. 358, no. 4, pp. 2535–2560, Mar. 2021, doi: 10.1016/j.jfranklin.2021.01.011.

13. E. E.-D. Hemdan, "An effective and reliable watermarking method using wavelet fusion, multi-level DWT, and single value decompression with jumbled medical images," (springerlink.com)

14. Multimedia Tools and Applications, vol. 80, no. 2, pp. 1749–1777, Sep. 2020, doi: 10.1007/s11042-020-09769-7.

15. A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, Future Generation Computer Systems, "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," (link.springer.com) vol. 86, pp. 926– 939, Sep. 2018, doi: 10.1016/j.future.2016.11.023.

16. M. Begum and M. S. Uddin, "Digital Image Watermarking Techniques: A Review," Information, vol. 11, no. 2, p. 110, Feb. 2020, doi: 10.3390/info11020110.