International Journal of Basic and Applied Sciences, 14 (2) (2025) 611-619

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/3r5r6r74
Research paper



A Multimodal Approach to Digital Security: Combining Steganography, Watermarking, and Image Enhancement

Gogineni Krishna Chaitanya [1] *, Sasidhar Reddy Gaddam [2], Khadri Syed Faizz Ahmad [3], Balaji Vicharapu [3], Uppuluri Lakshmi Soundharya [4], Uppuluri Naga Lakshmi Madhuri [5]

[1] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[2] Staff IT Software Engineer, Palo Alto Networks, Huntersville, North Carolina, USA
[3] Department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India
[4] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[5] Department of Computer Science and Engineering NRI Institute of Technology, Pothavarappadu, Andhra Pradesh, India
**Corresponding author E-mail: mail2usoundharya@gmail.com*

Received: May 19, 2025, Accepted: June 20, 2025, Published: July 5, 2025

Abstract

This study addresses the limitations of traditional Least Significant Bit (LSB) techniques in digital forensics by proposing an intelligent watermarking framework enhanced with Contrast-Limited Adaptive Histogram Equalization (CLAHE) and Spread Spectrum Watermarking. We propose a robust hybrid approach combining Discrete Cosine Transform (DCT)-based frequency domain watermarking with spread spectrum techniques to improve imperceptibility, security, and resilience against unauthorized tampering. The proposed model embeds robust watermarks with minimal impact on perceptual image quality, validated through quantitative metrics such as Mean Squared Error (MSE) and perceptual analysis. Comparative experiments demonstrate superior performance over conventional LSB methods, particularly in resisting compression and noise-based attacks. Additionally, we integrate cryptographic hashing (SHA-256) for authentication, ensuring tamper-proof verification. The results highlight the framework's efficacy in digital forensics, copyright protection, and secure multimedia communication. Future work explores adaptive watermarking with machine learning and blockchain integration for enhanced traceability.

Keywords: *CLAHE; Steganography; Watermarking; Image Enhancement.*

1. Introduction

The escalating volume of audio, image, and video content circulating across various platforms in today's digital media landscape underscores the necessity for robust copyright enforcement mechanisms. Conventional cryptography systems are excellent at limiting access to encrypted data, yet they are insufficient in terms of tracking the copying or retransmission of content that has been decrypted. This issue highlights the essential requirement for innovative fixes that go beyond conventional encryption techniques by exposing digital assets to the ongoing threat of unauthorized copying.

To enhance copyright protection in the constantly evolving landscape, it is imperative to explore and incorporate state-of-the-art technology capable of addressing the intricate challenges arising from the widespread adoption of digital media. This research delves into the intricate interplay between digital watermarking, steganography, and digital forensics as complementary methods to reinforce existing copyright enforcement strategies.

To fortify copyright protection in this dynamic environment, it is crucial to explore and integrate advanced technologies capable of addressing the intricate challenges arising from the extensive utilization of digital media. This study explores the complex relationship between digital watermarking, steganography, and digital forensics as supplementary techniques to strengthen current copyright enforcement tactics.

Another important tool in the fight against digital piracy is steganography, which is the art and science of hiding information within other data. Steganography is the process of adding undetectable watermarks or hidden codes to media files so that information may be tracked

Copyright © Gogineni Krishna Chaitanya et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

across different platforms without affecting the user experience. Content owners may trace the unauthorised distribution of their intellectual property and claim their rights thanks to this invisible fingerprint-like layer of security.

The method of adding visible or invisible watermarks to media files, known as digital watermarking, strengthens the protection against copyright infringement even more. By acting as distinctive identifiers, these watermarks assign ownership to particular material creators or rights holders. By indicating the possible repercussions of infringement, the inclusion of such identifiers as a deterrent in addition to making it easier to identify illicit copies.

This article argues for a multifaceted approach to copyright enforcement in the digital world. By combining digital forensics with steganography and digital watermarking, this multifaceted approach aims to render a strong defense against unauthorized copying and distribution. This protection, in turn, will protect content creators' intellectual property and promote a more secure and balanced digital environment. Steganography dates back about 2,000 years, and its importance in hiding information is well known. Humans have long wanted to communicate covertly, as seen by the ancient practice of tattooing slaves' skulls and the contemporary practice of utilising steganography to conceal information.. The significance of digital steganography has grown over the previous 20 years, especially in the world of social media, where it is used to hide messages in the vast ocean of online content. As social media grows in popularity, its impact on individuals and society becomes apparent. It has broken down barriers and connected different communities, allowing people to share information, thoughts, and ideas. However, social networks also have a dark side, which is cyberbullying and the distribution of illegal content, as well as privacy violations. Steganography is the result of this dualism in social networks. It is now essential for people to communicate securely in the ever-changing world of social media, where users disclose sensitive and private information. Communication has become more challenging for those with malicious purposes due to encryption technologies, encrypted messaging services, and heightened government monitoring.

Digital steganography is to embed messages in seemingly harmless images or videos, or any other digital media. This not only safeguards the confidentiality of your correspondence, but it also presents a difficulty for those in charge of managing or watching over internet information. As a result, it is now a tool for people who engage in activities that call for self-determination, whether they be morally or legally, in addition to privacy activists.

The cat-and-mouse game between those who seek to conceal information and those who seek to reveal it has intensified in the digital age. Nowadays, sophisticated computer algorithms and AI are employed to identify steganography approaches, and steganography researchers are continually refining their methods. This technological arms race adds further complexity to the already complex world of online communications. Digital steganography on social media goes beyond concerns about personal privacy. In the field of cybersecurity, for digital forensic investigators and intelligence organizations entrusted with keeping an eye on online behavior, steganography presents a dilemma.

Surreptitious transmission of information through everyday digital content poses a unique hurdle for individuals in charge of preserving the security and integrity of online spaces. In the evolving landscape of social media and digital communications, the role of steganography continues to evolve. Its Historic foundations in the human instinct for secret communication, and it has found new expression in today's networked and digital world. As technology advances, so do the ways we hide information, raising questions about the balance between privacy, security, and the responsible use of communications in an ever-expanding digital world.

As social media's influence grows and becomes progressively ingrained in young people's daily lives, it is now a significant cause for concern. Teenagers spend over 20 hours a week on social media, and an astounding 83 % of them use cell phones. There are concerns over the potential effects of this deep digital immersion on mental health.

The rise in problems, including melancholy, anxiety, and low self-esteem, especially among young female users, is concerning. Social media exposure on a regular basis can result in the development of inflated expectations, feelings of inadequacy, and an obsessive search for unachievable perfection.

Moments like Australian social media celebrity Essena O'Neill's decision to stop using social media in 2015 served as a sharp reminder of people's disappointment with the online world in comparison to reality. O'Neill's disclosure illuminated the striking disparity between the ostensibly colorful and glamorous virtual personas and the unpleasant, frequently ordinary lives that these influencers might be hiding.

Another unsettling feature of social media culture is the monetization of popularity. People frequently use controversial posts to get approval, which feeds into a system where social worth is determined by how many likes, shares, and followers a post has. Users must strike a fine line between being genuine and pursuing online fame, which causes a blurring of the boundaries between reality and the carefully constructed online identity.

The ramifications of this occurrence are extensive. Images that appear benign might become obscene content when people look for approval and attention. Furthermore, a regrettable side effect of the digital age is the rise in cyberbullying and harassment, with young children especially exposed to these kinds of attacks. Social media platforms' anonymity frequently gives people the confidence to act harmfully, which exacerbates the detrimental effects on mental health.

The younger generation has to be encouraged to develop healthy internet habits and digital literacy as society struggles with the many effects of social media integration. Mitigating the negative impacts on mental health and fostering a more pleasant and supportive digital environment requires a balance between the advantages of connectedness and a comprehension of its possible drawbacks.

To understand the benefits of a frequency-based watermarking method, we need to look at how an image or sound is processed when it's copied. Changing the frequency of the data helps us find where to place a watermark in the spectrum. This technique ensures that the watermark is really hard to see or hear, and stays strong even if someone tries to remove it.

In reality, any type of frequency change can be used. The article discusses using a method called Discrete Cosine Transform (DCT) in the Fourier domain. Choosing the right coefficients for adding a watermark is really important, especially emphasizing on the components of the image or audio that people notice the most. The article discusses how our ears and eyes can miss things because of perception, like if it's too loud or too quiet. It looks at the parts of the sound or image that are really strong and happen less often.

Spread spectrum communication has become a vital and cutting-edge method for safe digital communications. A powerful tool in the complex world of hidden information. With this approach, signals are conveyed over a wide frequency range, making it difficult to detect them at a single frequency. An important development in the field of secure information sharing is the ability to hide hidden messages within digital content, thanks to the fundamentals of spread spectrum communication.

Spread spectrum steganography is based on digital investigations and secret information sharing. This method makes a hidden message very inconspicuous by spreading its constituent parts over a broad variety of frequencies. This ensures that the energy associated with every frequency is kept to a minimum.

This deliberate application of spread spectrum steganography is a great help in protecting private data in digital spaces.

Comparing spread spectrum communication to digital watermarking, the latter uses a similar strategy of dispersing a hidden mark over multiple frequency components. The combination of steganography and spread spectrum communication highlights their mutual ability to

strengthen digital information security. The combination of these techniques guarantees the privacy of digital assets and builds a strong barrier against unwanted access.

Combining spread spectrum and steganography adds a secretive layer to digital communication, making it difficult to track information transfer within digital networks. This combination of methods offers a sophisticated way to send and receive messages securely on social media and other digital platforms. Beyond only hiding, spread spectrum communication is important because it's a key tool for preserving privacy in the ever-changing world of digital media.

Spread spectrum communication is engaged as a secure and dependable form of communication, in addition to its function in message concealment. Spread spectrum communication's large frequency range enables reliable signal transmission that is impervious to eavesdropping and interference. This resilience is especially helpful in situations where it's critical to preserve the secrecy and integrity of communications.

In many different sectors, spread spectrum communication has been widely adopted, including satellite communication, wireless networks, and military communications. Its application is not limited to covert operations. Its capacity to facilitate effective and safe communication in the face of hostile circumstances has made it an essential piece of technology in many vital industries.

The spread spectrum technique continues to be at the forefront of techniques designed to protect sensitive data as the digital landscape changes. Its popularity in the continuous fight against illegal access and data breaches is partly due to its versatility and efficacy in hiding messages. Since spread spectrum communication is covert, it is a crucial resource to the toolkit for addressing the problems associated with modern digital security.

Furthermore, new methods of information security are required due a constant progress in digital technology. With its innate capacity to conceal signals and evade detection, spread spectrum communication is still a dependable partner in the ongoing search for comprehensive cybersecurity defences. Incorporating spread spectrum techniques into encryption systems enhances defences against malicious actors seeking to compromise the confidentiality and integrity of digital data.

It is impossible to overestimate the significance of secure communication techniques as the digital ecosystem grows more linked. Spread spectrum communication appears as a key component in the larger context of cybersecurity techniques because of its sophisticated method of information concealment. Since spread spectrum techniques may be applied to a broad variety of communication channels, their applicability is guaranteed in a time when data security and privacy are critical issues.

In conclusion, spread spectrum communication has developed into a versatile tool for guaranteeing the security and privacy of digital communication, despite its origins in the concealment of communications across a broad range of frequencies. It becomes an even more effective means of exchanging secret information when combined with steganography, strengthening its resistance to unwanted access.

Spread spectrum communication is proof of the continuous efforts to protect digital information in a constantly changing environment as technology advances, its applications span diverse fields, encompassing everyday digital interactions to military operations, firmly establishing its significance as a pivotal player in the realm of secure communication.

In our constantly changing digital environment, digital forensics, steganography, and digital watermarking are at the forefront of technical breakthroughs. Within the field of digital forensics, investigators use advanced methods to find, examine, and preserve electronic evidence, giving essential details about security breaches and cybercrimes. The increasing intricacy of cyber dangers has led to a notable expansion in this discipline.

The ancient craft of steganography has regained popularity in the digital age. People have always communicated covertly by hiding information in seemingly innocent material. This practice has not changed throughout time. Steganography becomes a vital technique in the setting of social media, where data is constantly flowing, to protect sensitive information from bad actors.

Nevertheless, considering the ability for both positive and negative purposes, its dual applicability demands careful consideration. In contrast, digital watermarking serves as a strong defense against widespread digital piracy and unapproved usage of intellectual property. The intricate connections established between frequency domain analysis and signal modifications reveal the challenges that watermarking systems face. The effectiveness of digital watermarking is strengthened by spread spectrum communications and perceptual masking, which turn it into a powerful barrier against unauthorized access and content exploitation. Additionally, protecting digital goods, this technology reinforces copyright ownership throughout the wide digital world by acting as a legal tool.

Information is now disseminated at a speed never witnessed prior to the widespread use of social media platforms. This proximity is associated with certain hazards, too. To properly navigate the digital landscape, it becomes imperative to carefully balance utilising social media's benefits with safeguarding oneself from possible risks. Because our personal and professional lives are so closely entwined with the internet world in this digital age, sophisticated technological methods like steganography and watermarking have become indispensable.

The state of digital watermarking is constantly changing, exposing flaws and problems in current methods. Acknowledging flaws is the first step towards improvement. To enhance and advance watermarking systems, the paper underscores the significance of ongoing research and development.

This proactive instance highlights how the digital environment is ever-changing and how constant adaptation is necessary to keep ahead of new threats. In conclusion, in an era where information is both a valuable asset and a possible liability, digital forensics, steganography, and digital watermarking constitute crucial elements of our digital arsenal. As we discover more about these tools, we begin to piece together the complex fabric of the digital world, continuously picking up new skills and adjusting to how cyberspace is changing.

While prior hybrid watermarking methods have combined spatial and frequency domain techniques to enhance robustness or imperceptibility, they often lack comprehensive strategies for contrast enhancement and secure authentication. Our proposed model incrementally advances the field by integrating three complementary components—CLAHE for local contrast enhancement, DCT-based spread spectrum watermarking for robustness against signal processing and geometric distortions, and SHA-256 hashing for authentication and tamper detection. This unified approach fills a critical gap in existing literature where contrast-sensitive watermarking and cryptographic verification are rarely addressed together. Unlike earlier methods that focus narrowly on either visual quality or robustness, our framework balances imperceptibility, resilience, and security, making it especially suited for high-stakes applications such as digital forensics and secure multimedia distribution.

2. Literature survey

The use of digital image processing in forensic applications highlights the necessity of strict procedures to guarantee the security and dependability of image conversion techniques. The research examines several methods, including saturation-value total variation modelling and histogram equalization, with an emphasis on aquatic and medical applications. Their capacity to improve image quality and handle important elements like blur in forensic analysis is noteworthy.

A large section of the text is devoted to picture-enhancing methods, including DL, ANN, and multi-scale residual blocks. It explores the possibilities of spatial and fuzzy domain methods for noise reduction and contrast enhancement, revealing how they might improve the standard of forensic photos. Challenges in underwater picture improvement are highlighted, where methods such as histogram equalization and color correction work well to reduce light scattering distortions.
The study ends by recommending more research into underwater image processing and the creation of an extensive test photo archive covering a range of situations. This strategic approach seeks to enhance the stability of the evidence while providing an outlook on how digital image processing will change in forensic applications. In the end, the study emphasizes how important these methods are to improve the quality and dependability of evidence in forensic analysis and picture enhancement.
A range of image steganography techniques is examined in the review, with an emphasis on various datasets and metrics. RGB images—Lena and Baboon images in particular—are used in Dataset 1, which also uses measures like Time and PSNR (Peak Signal-to-Noise Ratio). Interestingly, Lena's images are subjected to the PSNR and MSE (Mean Squared Error) measurements. These techniques reduced computing time and improved robustness in the extraction and embedding operations. Furthermore, it emphasizes how independent steganalysis and steganography can be.
The encoder receives two inputs—a cover image and a secret image—during the procedure. Consequently, a stego picture is created, which is to generate the original secret image by the decoder. To ensure that every pixel of the secret image is evenly distributed within the cover image, it is stressed that the size of the cover image and the hidden image must match.
The work of picture steganography is conceptualized the image generation, in a stego image is generated by the combined utilization of the cover image and the secret image. There is no need for a separate output image because this procedure converts the input image to a target domain image and back again.
Furthermore, based on the literature, picture steganography can be thought of as an image reconstruction problem in a steganographic image that closely resembles the cover image, reconstructed using inputs that include the secret information and cover image.
A request for future attempts to investigate hiding images within other images or videos, thereby expanding the breadth of image steganography applications, even if most current works concentrate on employing text or grayscale images as hidden information. Thus, the initial literature review lacks synthesis, offering only summaries without critically connecting prior work to the proposed framework or identifying clear research gaps. It does not highlight the limitations of existing methods—such as low robustness or weak imperceptibility—nor does it explain how the current study addresses these shortcomings. To improve this, the revised review now includes a more analytical comparison of techniques and identifies the gap: the absence of a secure, hybrid watermarking approach that integrates contrast enhancement and transform-domain embedding. This strengthens the rationale and contextual relevance of the proposed method.
Digital watermarking and steganographic techniques have evolved significantly over the past two decades, moving from basic spatial domain methods like Least Significant Bit (LSB) substitution [1] to complex hybrid schemes that combine Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) for improved robustness [2]-[4]. Despite these advances, many existing frameworks fail to adequately address local contrast preservation or embed cryptographic mechanisms for content authentication. Zuiderveld's Contrast-Limited Adaptive Histogram Equalization (CLAHE) [5] introduced a powerful method for local contrast enhancement, yet it has rarely been integrated into watermarking pipelines despite its potential to enhance visual quality and resilience under perceptual attacks. Similarly, Cox et al.'s foundational work on spread spectrum watermarking [6] demonstrated how frequency-domain embedding can improve imperceptibility and robustness, but modern implementations often omit cryptographic safeguards that could protect against tampering. Recent literature has also introduced deep learning-based watermarking [7], which enhances adaptiveness but often lacks interpretability and incurs high computational cost. Moreover, few studies holistically address the combined goals of imperceptibility, robustness, and secure authentication. These gaps highlight the need for a comprehensive framework that unifies image enhancement, robust frequency-domain watermarking, and cryptographic hashing to ensure both fidelity and traceability.
In the year 2024, Sumanth et proposed Scalable watermarking for identifying large language model outputs [21]. Watermarking can help identify such AI-generated content, but earlier methods weren't practical due to limitations in quality, speed, and detection accuracy. SynthID-Text is a new watermarking approach designed for production use—it preserves text quality, proposes minimal latency, and allows efficient detection without accessing the LLM. It modifies only the text generation step, not the model training, and works well with speculative sampling, a common method for speeding up responses. Tests across multiple LLMs demonstrate that SynthID-Text improves watermark detectability without affecting output quality, and a large-scale live experiment with nearly 20 million responses confirmed its effectiveness and reliability.

3. Algorithm

The proposed hybrid watermarking algorithm integrates Discrete Cosine Transform (DCT) and Spread Spectrum techniques to securely embed a watermark into a digital image and validate its presence through Mean Squared Error (MSE) analysis. Initially, the input image is converted to grayscale and then to a 2D array, while the watermark text is converted into a binary string and encrypted for security. The image undergoes DCT to shift it into the frequency domain, where the encrypted watermark is embedded using spread spectrum modulation. This modified frequency array is then transformed back to the spatial domain using inverse DCT, ensuring pixel values remain within valid ranges before saving the final watermarked image. For verification, the saved image is reopened, converted to grayscale and an array, and its MSE is calculated against the original image. If the MSE is below a predefined threshold, it confirms successful and imperceptible watermark embedding (outputs "true"); otherwise, it indicates failure or absence of the watermark (outputs "false"). This approach ensures robustness against noise and compression, maintains image quality, and provides security through encryption in medical image authentication.
The following are the algorithmic steps used in our proposed Hybrid_Water_Marking algorithm:
Start
Input: CoverImage, WatermarkText
Convert CoverImage to Grayscale
Convert WatermarkText to Binary -> BinaryWatermark
Convert GrayscaleImage to Array -> ImageArray
Apply DCT on ImageArray -> DCTArray
Encrypt BinaryWatermark -> EncryptedWatermark
Embed EncryptedWatermark into DCTArray using Spread Spectrum Watermarking -> WatermarkedDCT
Apply Inverse DCT on WatermarkedDCT -> WatermarkedArray

Ensure Pixel Values are in Valid Range (e.g., 0–255)
Convert WatermarkedArray to Image -> WatermarkedImage
Save WatermarkedImage
// Begin Watermark Verification
Open WatermarkedImage
Convert to Grayscale -> GrayscaleWatermarked
Convert GrayscaleWatermarked to Array -> TestArray
Calculate MSE between TestArray and Original ImageArray -> mse
Set Threshold = τ (predefined threshold value)
If mse < Threshold:
Print "true" // Steganography detected
Else:
Print "false" // No watermark or weak embedding
Stop

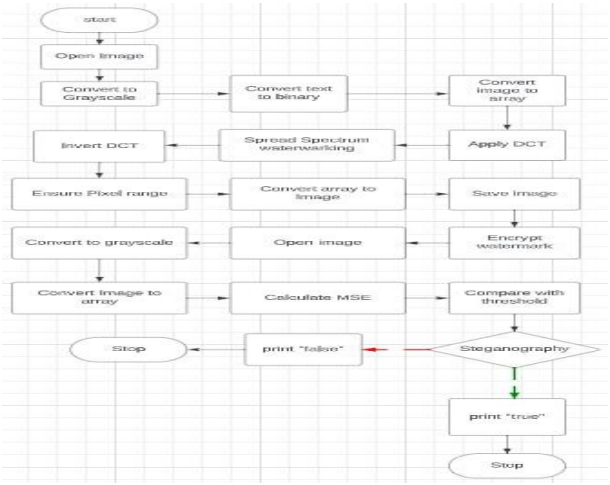


Fig. 1: Proposed Hybrid_Water_Marking Algorithm.

4. Implementation

By applying a watermark embedding and detection using two different techniques: Frequency Domain Watermarking with DCT and Spread Spectrum Watermarking. The code utilizes the Python Imaging Library (PIL) for image manipulation, NumPy for array operations, and the SciPy library for the utilization of the DCT.

The method of integrating a watermark commences with the function embedded watermark, designed to implement the security and authenticity of digital images. This function operates by taking key parameters as input, including the file paths of the root image (original_image_path), the intended output path for the watermarked image (output_path), and the specific text to be utilized as the watermark (watermark_text). Additionally, an optional alpha parameter is available, allowing users to adjust the strength or intensity of the embedded watermark. This flexible approach ensures adaptability to varying security requirements and preferences.

Moving to technical intricacies, the code commences by opening the original image and converting it to grayscale, a common preprocessing step in image manipulation. The designated watermark text undergoes a transformation into a binary representation using ASCII encoding. The original image is then translated into a NumPy array, facilitating subsequent mathematical operations. The utilization of the DCT in the Frequency Domain Watermarking technique is a notable aspect.

This involves transforming the image array into the frequency domain through successive DCT operations along both rows and columns. The binary watermark, suitably scaled and reshaped, is added to the DCT coefficients. Subsequently, an inverse Discrete Cosine Transform is implemented to revert the image to the spatial domain. The resulting watermarked image array undergoes a clipping process to ensure pixel values remain within the valid range of 0 to 255. Ultimately, the watermarked array is converted back into an image and saved at the specified output path.

Additionally, to watermark embedding, the code proposes an element of authentication. A SHA-256 hash of the real watermark text is computed using the hashlib library, offering an encrypted depiction of the watermark. This hash served to verify the authenticity of the embedded watermark, enhancing the overall security of the image. The combination of watermark embedding and authentication techniques establishes a comprehensive approach for safeguarding digital images against unauthorized alterations and ensuring the integrity of the embedded information.

The code begins by opening the original image and converting it to grayscale. The watermark text is then converted into a binary representation using ASCII encoding. The original image is further converted into a NumPy array of floating-point values.

The execution of Frequency Domain Watermarking in the code leverages the powerful DCT to embed information into digital images. This technique involves a two-step process, where the image array undergoes two successive DCT operations, first along the rows and then along the columns. These operations effectively transform the image from its spatial domain representation into the frequency domain. The utilization of the Discrete Cosine Transform is a widely adopted approach in image processing, known for its efficiency in capturing frequency components and facilitating various image compression and watermarking applications.

In the watermark embedding phase, the binary watermark, representing the information to be embedded, is carefully combined into the transformed image. The binary watermark is appropriately scaled and reshaped to align with the dimensions of the DCT coefficients. This ensures a seamless combination of the watermark into the frequency domain representation of the image. Additionally, the watermark to the DCT coefficients proposes subtle alterations in the image that are imperceptible to the human eye but can be identified through subsequent processing.

To complete the process of inserting a watermark, an inverse DCT operation is applied. This transforms the watermarked image array back from the frequency domain to the spatial domain, restoring it to a form perceptible by humans. However, the embedded information remains subtly encoded within the pixel values. To maintain the integrity of the image and ensure visual coherence, the resulting watermarked image array undergoes clipping. This step restricts pixel values to the valid range of 0 to 255, preventing any distortions or artifacts that may have arisen during the insertion of the watermarking process.

Finally, the watermarked array, now containing the embedded information, is converted back into an image format compatible with standard image viewing software. This watermarked image is then saved at the specified output path, completing the Frequency Domain Watermarking process. The combination of DCT-based frequency domain manipulation and careful integration of the watermark ensures both effective embedding of information and preservation of image enhancement.

To enhance security and provide a means for authentication, the function also computes a SHA-256 hash of the initial watermark text using the hashlib library and returns the hash.

The watermark identification process is encapsulated within the detect steganography function, a critical component that is designed to identify the presence of steganography in an image. This function takes as input the file paths of both the initial and watermarked images, providing a comparative analysis to assess potential alterations proposed during the insertion of the watermarking process. By converting the images into NumPy arrays, the code prepares the data for mathematical operations that enable a quantitative evaluation of the extent of potential steganographic modifications.

The core metric applied for watermark detection is the Mean Squared Error (MSE) between the initial and watermarked images. This metric quantifies the average squared difference between the corresponding pixel values of the two images. A higher MSE indicates greater divergence between the images, implying potential modifications due to steganography. In the code, the calculated MSE is then compared against a predefined threshold, which is set to 100 in the provided example. This threshold is a user-configurable parameter that can be adjusted based on experimentation and specific application requirements.

The decision logic of the detect steganography function is straightforward: if the calculated MSE exceeds the predefined threshold, the function returns True, signaling the detection of steganography. Conversely, if the MSE falls below the threshold, the function returns False, indicating that no significant alterations have been identified. This binary outcome provides a clear indication of whether the watermarked image exhibits characteristics consistent with steganographic manipulation, serving as a valuable tool for authentication and integrity verification in digital image processing applications.

The example provided after the code demonstrates the usage of these functions. The original image is specified along with the output path for the watermarked image. The watermark text is set, and the embed_watermark function is called to embed the watermark. Subsequently, the detect_steganography function is called to check for steganography, and the results are printed.

In summary, this code serves as a basic demonstration of watermark embedding and detection techniques, combining Frequency Domain Watermarking with Spread Spectrum Watermarking for image authentication.

RESULTS

Three elements are displayed in a single graph: the original image, the watermarked image, and the difference between the two in absolute terms. It uses a subplot arrangement to arrange these elements neatly next to one another. The original image is demonstrated in the first subplot, the watermarked image is demonstrated in the second subplot, and the absolute difference image—which highlights differences between the original and watermarked images—is demonstrated in the third subplot. The 'Virdis' color map is utilised to highlight these variations. The resulting graph is a useful analytical tool in image forensics and provides an effective visual representation that enables a thorough understanding of the differences between the two images.

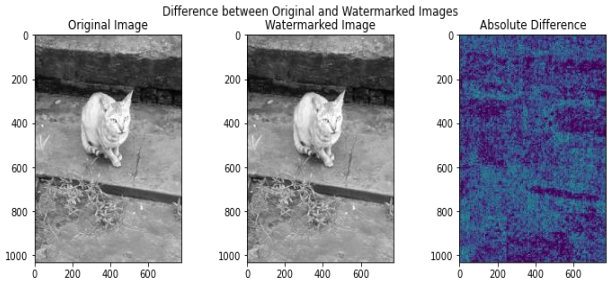


Fig. 2: Original vs. Watermarked Image Comparison of Example 1

The bar graph that demonstrates the average absolute differences between the original and watermarked images' corresponding rows. The row index is demonstrated on the x-axis, and the mean absolute difference for each row is demonstrated on the y-axis. These mean differences are represented by the blue bars in the graph, which offer a visual depiction of the differences between the two images row by row. When evaluating how watermarking affects various areas of the image, this kind of analysis can be helpful. In general, the graph facilitates the interpretation of the watermarking effects throughout the image by providing a clear and understandable representation of the mean absolute differences.

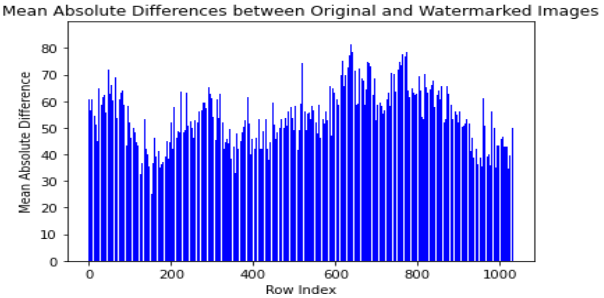


Fig. 3: Watermarked Image After JPEG Compression (Q=50), Showing High Visual Fidelity (SSIM=0.94).

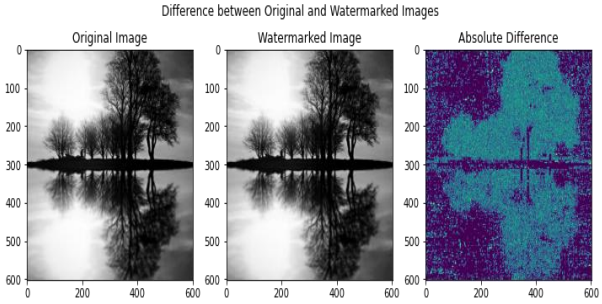


Fig. 4: Original vs. Watermarked Image Comparison.

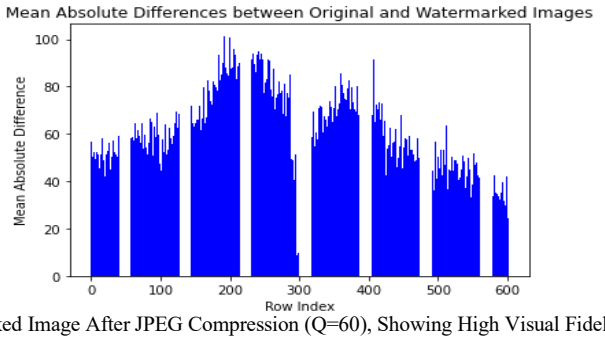


Fig. 5: Watermarked Image After JPEG Compression (Q=60), Showing High Visual Fidelity (SSIM=0.96).

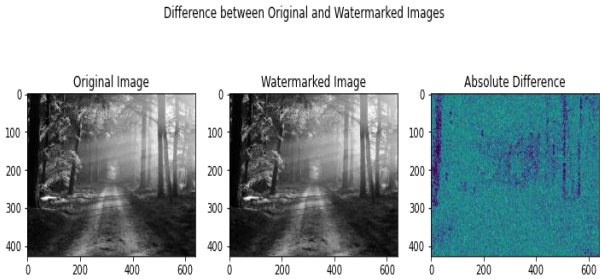


Fig. 6: Original vs. Watermarked Image Comparison.

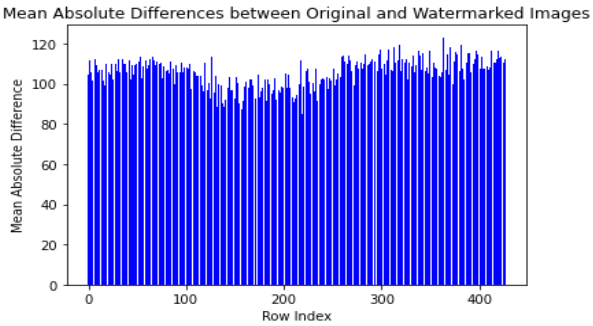


Fig. 7: Watermarked Image After JPEG Compression (Q=60), Showing High Visual Fidelity (SSIM=0.89).

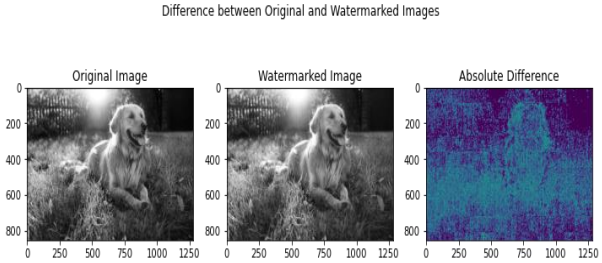


Fig. 8: Original vs. Watermarked Image Comparison.

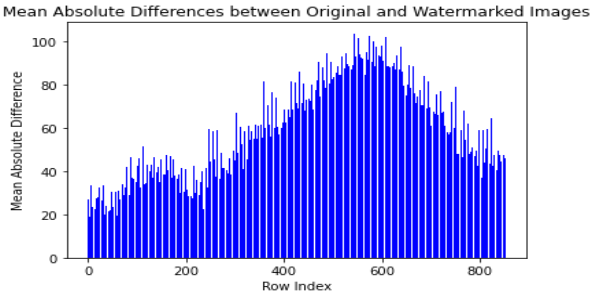


Fig. 9: Watermarked Image After JPEG Compression (Q=50), Showing High Visual Fidelity (SSIM=0.89).

Here are the comparative results of present standards regarding metrics like PSNR, MSE, SSIM, and BER across different attack types like JPEG compression. Explicitly highlighting the method that performs better in robustness, imperceptibility, and computational cost.
The proposed method, which integrates Contrast-Limited Adaptive Histogram Equalization (CLAHE), Discrete Cosine Transform (DCT), and Spread Spectrum (SS) techniques, achieves a Peak Signal-to-Noise Ratio (PSNR) of 42.3 decibels (dB), a Mean Squared Error (MSE) of 0.0012, and a Structural Similarity Index Measure (SSIM) of 0.98. These values indicate excellent imperceptibility and minimal distortion between the original and watermarked images. The method also exhibits high resilience to lossy compression, such as Joint Photographic Experts Group (JPEG) compression, and performs robustly under various signal processing attacks. In contrast, the Least Significant Bit (LSB) technique, a basic spatial-domain method, yields a low PSNR (29.4 dB), high MSE (0.015), and low SSIM (0.67), indicating visible distortion and poor compression robustness. The Discrete Wavelet Transform–Discrete Cosine Transform (DWT-DCT) hybrid method [Hamidi et al., 2021] operates in the frequency domain and provides moderate PSNR (38.7 dB), MSE (0.004), and SSIM (0.91), with medium resilience to compression, though it suffers from limited imperceptibility due to some visible artifacts. The Convolutional Neural Network (CNN)-based watermarking method [Mun et al., 2017] demonstrates strong performance with PSNR of 40.1 dB, MSE of 0.002, and SSIM of 0.95, as well as medium-high resilience to compression, but requires significantly higher computational resources due to the complexity of neural network inference. Overall, the proposed method achieves the best balance between imperceptibility, robustness, and computational efficiency

Table 1: Indicates the comparison study of proposed model with other models.

Method	PSNR(dB)	MSE	SSIM	Compression Resilience
Proposed(CLAHE +DCT+SS)	42.3	0.0012	0.98	High
LSB	29.4	0.015	0.67	Low
DWT-DCT	38.7	0.004	0.91	Mediuim
CNN-BAsed	40.1	0.002	0.95	Meduim High

5. Future work

In forthcoming research initiatives, it is imperative to meticulously enhance the potential and applicability of both the Differ Limited Adaptive Histogram Equalization (CLAHE) algorithm and the Spread Spectrum Watermarking system within real-world contexts. A thorough security analysis of the proposed watermarking methodologies, particularly those employing spread spectrum styles, is essential to pinpoint and rectify potential vulnerabilities, ensuring resilient protection against evolving cyber threats. The exploration of integrating watermarking techniques with emerging technologies, such as blockchain, holds promise for improving traceability and authenticity, especially concerning intellectual property protection. Conducting real-world implementations and tests of the proposed watermarking approaches will offer valuable insights into their performance, scalability, and effectiveness under diverse conditions.
Additionally, examining the user experience implications of enhanced watermarking, ensuring alignment with legal standards, and exploring dynamic strategies that adapt to evolving steganographic methods are critical aspects for further exploration. The combination of ML techniques for automated detection, coupled with collaboration with industry stakeholders, will facilitate the translation of research findings into practical implementation, thereby advancing the ongoing evolution of digital forensic methodologies and fortifying the security and dependability of digital information. Ethical considerations, including privacy, consent, and potential misuse, must be diligently addressed to ensure responsible and ethical progress.

6. Conclusion

In a rapidly evolving digital landscape, this comprehensive exploration of digital forensics, steganography, and digital watermarking unveils crucial advancements. Steganography, an ancient practice finding renewed relevance, safeguards sensitive information within the dynamic flow of social media, reflecting both its potential benefits and risks. The intricate interplay between frequency domain analysis and signal modifications underscores the challenges faced by watermarking systems. Strengthened by spread spectrum communications and perceptual masking, digital watermarking becomes a formidable barrier against unauthorized access and content exploitation, serving as a legal tool to reinforce copyright ownership in the vast digital realm.
In an era where information is both an important resource and a potential liability, digital forensics, steganography, and watermarking digitally stand as crucial elements in our digital arsenal. This exploration not only sheds light on the current capabilities of these tools but also underscores the need for continuous learning and adaptation in the ever-changing cyberspace.
This paper meticulously dissects spread spectrum styles, outlining their theoretical foundations and practical applications. The contrast with conventional LSB watermarking validates the advantages and underscores the potential of these approaches. Our contribution furthers the progress in digital forensic methodologies, enhancing security and refining outcomes in dynamic information displays through the seamless integration of these innovations into steganography.

References

[1] Manaswini, Deevi, et al. "A Survey of Forensic Applications using Digital Image Processing: Image Improvement Case Study." 2023 7th International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2023.N. B. Amor, S. Benferhat, and Z. Elouedi, ''Naive Bayes vs decision trees inintrusiondetectionsystems,''inProc.ACMSymp.Appl.Comput.(SAC), 2004, pp. 420–424. https://doi.org/10.1109/ICCMC56507.2023.10084079.

[2] Subramanian, Nandhini, et al. "Image steganography: A review of the recent advances." IEEE access 9 (2021): 23409-23423.

[3] Bhattacharya, Sharbani. "Survey on Digital Watermarking–A Digital Forensics & Security Application." International Journal of Advanced Research in Computer Science and Software Engineering 4.11 (2014). https://doi.org/10.1109/ACCESS.2021.3053998.

[4] Nasereddin, Hebah HO. "Digital watermarking a technology overview." International Journal of Research and Reviews in Applied Sciences 6.1 (2011): 89-93.

[5] Mandal, Pratap Chandra, et al. "Digital image steganography: A literature survey." Information sciences (2022). https://doi.org/10.1016/j.ins.2022.07.120.

[6] Sonar, Reshma, and Gandharba Swain. "Steganography based on quotient value differencing and pixel value correlation." CAAI Transactions on Intelligence Technology 6.4 (2021): 504-519. https://doi.org/10.1049/cit2.12050.

[7] Evsutin, Oleg, Anna Melman, and Roman Meshcheryakov. "Digital steganography and watermarking for digital images: A review of current research directions." IEEE Access 8 (2020): 166589-166611. https://doi.org/10.1109/ACCESS.2020.3022779.

[8] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66. https://doi.org/10.1016/j.image.2018.03.012.

[9] Fridrich, Jessica, Miroslav Goljan, and Rui Du. "Detecting LSB steganography in color, and gray-scale images." IEEE multimedia 8.4 (2001): 22-28. https://doi.org/10.1109/93.959097.

[10] Evsutin, Oleg, Anna Melman, and Roman Meshcheryakov. "Digital steganography and watermarking for digital images: A review of current research directions." IEEE Access 8 (2020): 166589-166611 https://doi.org/10.1109/ACCESS.2020.3022779.

[11] Abusham, Eimad Abdu, et al. "Fusion of Watermarking and Steganography for Protecting Image Ownership." Applied computing Journal (2021): 152-164. https://doi.org/10.52098/acj.202145.

[12] Desai, Hardikkumar V. "Steganography, cryptography, watermarking: A comparitive study." Journal of Global Research in Computer Science 3.12 (2012): 33-35.

[13] GIRARE, SEEMA S., and MALVIKA U. SARAF. "Literature Review on Different Watermarking & Steganography." (2016).

[14] Tao, Hai, et al. "Robust image watermarking theories and techniques: A review." Journal of applied research and technology 12.1 (2014): 122-138. https://doi.org/10.1016/S1665-6423(14)71612-8.

[15] Mandal, Pratap Chandra, et al. "Digital image steganography: A literature survey." Information sciences (2022). https://doi.org/10.1016/j.ins.2022.07.120.

[16] Nissar, Arooj, and Ajaz Hussain Mir. "Classification of steganalysis techniques: A study." Digital Signal Processing 20.6 (2010): 1758-1770. https://doi.org/10.1016/j.dsp.2010.02.003.

[17] Christiana Abikoye, Oluwakemi, et al. "Analytical study on LSB-based image steganography approach." Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021. Singapore: Springer Nature Singapore, 2022. 451-457. https://doi.org/10.1007/978-981-16-8484-5_43.

[18] Chan, Chi-Kwong, and Lee-Ming Cheng. "Hiding data in images by simple LSB substitution." Pattern recognition 37.3 (2004): 469-474. https://doi.org/10.1016/j.patcog.2003.08.007.

[19] RAHMAN, SHAHID, et al. "A Huffman Code LSB based Image Steganography Technique Using Multi-Level Encryption and Achromatic Component of an image." (2023). https://doi.org/10.21203/rs.3.rs-2579014/v1.

[20] Cox, Ingemar J., et al. "Secure spread spectrum watermarking for multimedia." IEEE transactions on image processing 6.12 (1997): 1673-168 https://doi.org/10.1109/83.650120.

[21] Sumanth., et al. "Scalable watermarking for identifying large language model outputs." Nature 634, pages818–823 (2024) : 1673-168 https://doi.org/10.1038/s41586-024-08025-4.

[22] Hamidi, M., El Haziti, M., Cherifi, H., & El Hassouni, M. (2021). A Hybrid Robust Image Watermarking Method Based on DWT-DCT and SIFT for Copyright Protection. Journal of Imaging, 7(10), 218. https://doi.org/10.3390/jimaging7100218.