Digital Watermarking in Social Media

REVIEW - 3

Submitted By:
Karan Ravi - 20BIT0162
Ishani Chowdhury -20BIT0175
Jawahar YV - 20BIT0284

Abstract

Digital watermarking in social media refers to the process of embedding a unique identifier or signature into digital content such as images, videos, or audio files to protect them from unauthorised use or distribution. With the proliferation of social media platforms, the problem of copyright infringement and unauthorised sharing of content has become increasingly prevalent. Digital watermarking offers a solution to this problem by providing a way to identify the owner of the content and track its usage across different platforms. The paper on digital watermarking in social media includes the different techniques used for watermarking, their strengths and weaknesses, and the challenges faced in implementing them. Some of the popular techniques used for digital watermarking in social media include visible watermarking, invisible watermarking, and fragile watermarking. Visible watermarking involves adding visible text or image to the content, while invisible watermarking uses techniques such as spread spectrum and frequency modulation to embed the watermark without altering the original content. Fragile watermarking is used to detect any modifications to the original content. However, digital watermarking is not foolproof, and there are still challenges to be addressed, such as the ability of attackers to remove the watermark or the impact on the quality of the content. Despite these challenges, digital watermarking remains an essential tool for content creators and rights holders to protect their intellectual property in the digital age.

Keywords: Copyright protection, digital watermarking, signature, social media, unauthorised use, unique identifier, visible watermarking

Introduction

In recent years, the rapid growth of social media has made it a primary platform for sharing and disseminating digital content, making it an essential part of our daily lives. However, the proliferation of digital content has also led to an increase in intellectual property infringement, with unauthorised use of digital content becoming commonplace. To address this issue, digital watermarking has emerged as a powerful tool for protecting digital content from unauthorised use. The goal of digital watermarking is to embed hidden information, such as copyright notices or ownership information, into digital content, making it difficult for unauthorised users to use the content without permission. The different types of watermarking methods include steganography, cryptography, and machine learning, with the primary aim of detecting and locating any tampering or modification to the original content.

In this project, we will explore the concept of digital watermarking in social media, with a particular focus on images and videos. We will conduct a literature review of the various watermarking techniques, including the use of mathematical techniques such as Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Fast Walsh Hadamard Transformation, and the Pi Transform. Additionally, we will examine the use of natural language processing and edge detection techniques, as well as machine learning-based approaches for watermarking.

There are several reasons why the topic of digital watermarking in social media is important and relevant. First, social media platforms have become a significant part of our daily lives, with billions of users sharing and consuming images and videos on these platforms. This has led to an increased risk of copyright infringement and unauthorised use of digital media, which can cause financial losses for content creators and owners. Second, deep face technology has become more advanced, making it easier to manipulate and falsify images and videos. This has serious implications for the credibility of visual media in social media, and there is a need to develop effective methods for authenticating and verifying digital media to prevent the spread of false information and malicious propaganda. Digital watermarking has emerged as a promising solution for addressing these challenges, as it can provide a way to embed information into digital media that can be used to authenticate, verify, and protect the content. As a result, the topic of digital watermarking in social media has become an area of active research and development in recent years, with a growing number of studies and approaches being proposed to address the problem.

The objectives of this project are as follows:

- To conduct an extensive literature review of the various approaches to digital watermarking, with a particular focus on their applications in social media platforms such as Facebook, Twitter, and Instagram.
- To propose a methodology for developing a digital watermarking system that combines steganography, cryptography, and machine learning to protect digital media content on social media platforms.
- To evaluate the effectiveness of the proposed digital watermarking system in protecting intellectual property rights on social media platforms by analysing its potential to mitigate the problem of intellectual property infringement. The parameters for the evaluation will include the robustness, efficiency, and security of the watermarking system against common attacks, including compression, cropping, and scaling.

Overall, this project aims to develop a digital watermarking system that can effectively protect digital media content on social media platforms, thereby mitigating the problem of intellectual property infringement in the digital age.

Literature Survey

[1] Varshney, D., Sharma, B.K., Bansal, M. (2022). Secure Watermarking to Protect Colour Images on Social Media from Misuse.

The paper proposes a secure watermarking technique to protect colour images from misuse on social media platforms. The proposed technique embeds a watermark in the discrete cosine transform (DCT) coefficients of the colour image using the Arnold transform. The watermark is designed to be robust against common attacks such as cropping, rotation, and scaling. Additionally, the authors propose a technique to encrypt the watermark using the RSA algorithm to enhance the security of the watermark. The proposed technique is evaluated using various metrics such as peak signal-to-noise ratio (PSNR) and normalised correlation (NC). The experimental results show that the proposed technique is effective in protecting the colour images from unauthorised use and can resist various attacks. The authors conclude that the proposed technique can be useful for protecting the copyright of images shared on social media platforms.

[2] K. Jyothsna Devi, Priyanka Singh, Hiren Kumar Thakkar, Neeraj Kumar, Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media

The research paper proposes a robust and secure watermarking technique for digital image transmission in social media. The proposed technique uses a meta-heuristic optimization algorithm called Ja-Fi optimization to embed a watermark in the image. The watermark is designed to be robust against various types of attacks, such as compression, cropping, and noise addition. The authors also propose a novel technique for encrypting the watermark using an advanced encryption standard (AES) algorithm to enhance the security of the watermark. The performance of the proposed technique is evaluated using various metrics such as peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and normalised correlation (NC). The experimental results demonstrate that the proposed technique outperforms other state-of-the-art watermarking techniques in terms of both robustness and security. The authors conclude that the proposed technique can be useful for protecting digital images from unauthorised copying and distribution in social media platforms.

[3] Li, T.B. et al. Evaluation of Spiral Pattern Watermarking Scheme for Common Attacks to Social Media Images.

The paper evaluates the performance of a spiral pattern watermarking scheme for common attacks to social media images. The proposed scheme embeds a watermark in the spatial domain of the image using a spiral pattern. The watermark is designed to be robust against common attacks such as cropping, rotation, and compression. The performance of the proposed scheme is evaluated using various metrics such as peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and normalised correlation (NC). The experimental results show that the proposed scheme is effective in detecting the presence of the watermark and can resist various attacks with high accuracy. The authors also compare the proposed scheme with other watermarking techniques and demonstrate that the proposed scheme outperforms other methods in terms of robustness and accuracy. The authors conclude that the proposed scheme can be useful for protecting the authenticity and integrity of images shared on social media platforms.

[4] Neekhara, P. et al. (2022) Facesigns: Semi-fragile neural watermarks for Media Authentication and Countering Deepfakes

The paper proposes a semi-fragile neural watermarking method called FaceSigns to authenticate media and counter deep fakes. FaceSigns utilises a generative adversarial network (GAN) to learn the distribution of faces and generate corresponding watermarks. These watermarks can then be embedded into the image using a semi-fragile embedding method that allows the watermark to detect image manipulations while tolerating some degree of signal processing. FaceSigns also uses a neural network-based detection system to detect the presence of the watermark and distinguish between authentic and manipulated images. The proposed method is evaluated on several benchmark datasets and shows promising results in detecting various types of image manipulations, including those introduced by deepfake techniques. The authors suggest that the proposed method can be used for media authentication and forensics in various domains, including social media and journalism.

[5] Person, Niraj N., S. and Gavde, B. (2022) Visual cryptographic approach for authentication of Social Media Contents

The paper proposes a visual cryptographic approach for authentication of social media contents. The proposed approach uses a secret sharing scheme to split an image into two shares, where each share contains partial information of the original image. The shares are then uploaded to a social media platform, where they can be shared with others. The original image can be reconstructed by overlaying the two shares. The proposed approach also includes a mechanism to authenticate the reconstructed image to ensure that it has not been tampered with. The performance of the proposed approach is evaluated using various metrics such as peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM). The experimental results demonstrate that the proposed approach is effective in reconstructing the original image with high accuracy and can resist various attacks. The authors also compare the proposed approach with other authentication techniques and demonstrate that the proposed approach outperforms other methods in terms of security and accuracy. The authors conclude that the proposed approach can be useful for protecting the authenticity and integrity of images shared on social media platforms.

[6] Mahto, D.K., Singh, O.P. & Singh, A.K. FuSIW: fusion-based secure RGB image watermarking using hashing

The paper proposes a fusion-based secure RGB image watermarking scheme using hashing, called FuSIW. The proposed scheme uses a combination of discrete wavelet transform (DWT), discrete cosine transform (DCT), and singular value decomposition (SVD) to embed a watermark into the host image. The proposed scheme also uses a hashing function to ensure the security of the watermark. The performance of the proposed scheme is evaluated using various metrics such as peak signal-to-noise ratio (PSNR), normalised correlation (NC), and structural similarity index (SSIM). The experimental results show that the proposed scheme is effective in embedding the watermark into the host image with high fidelity and can resist various attacks such as noise addition, filtering, and compression. The authors also compare the proposed scheme with other watermarking techniques and demonstrate that the proposed scheme outperforms other methods in terms of robustness and accuracy. The authors conclude that the proposed scheme can be useful for protecting the authenticity and integrity of images shared on social media platforms.

[7] Bharti, S.S., Shivani, S., Pandey, S.K., Agarwal, S. (2022). An Efficient Blind Fragile Watermarking Scheme for Tamper Localization

The paper proposes an efficient blind fragile watermarking scheme for tamper localization. The proposed scheme embeds a watermark in the image using the bit plane slicing technique. The watermark is designed to be fragile, which means that any tampering with the image will result in a visible change in the watermark. The proposed scheme is also blind, which means that the original image is not required to extract the watermark. The authors also propose a method to localise the tampered region of the image by comparing the original and watermarked image. The performance of the proposed scheme is evaluated using various metrics such as peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and tamper detection rate (TDR). The experimental results demonstrate that the proposed scheme is effective in detecting and localising the tampered region of the image with high accuracy and can resist various attacks. The authors conclude that the proposed scheme can be useful for protecting the authenticity and integrity of digital images.

[8] Faheem, Z.B.; Ishaq, A.; Rustam, F.; de la Torre Díez, I.; Gavilanes, D.; Vergara, M.M.; Ashraf, I. Image Watermarking Using Least Significant Bit and Canny Edge Detection

The paper proposes a new image watermarking technique using Least Significant Bit (LSB) substitution and Canny edge detection. The proposed method first applies the Canny edge detector on the input image to extract edge information, which is then used to calculate the optimal embedding strength for watermark insertion using the LSB substitution technique. The extracted edge information also helps in the robustness of the watermark by increasing the payload size and resisting geometric and signal processing attacks. The performance of the proposed method is evaluated based on several metrics, such as peak signal-to-noise ratio, normalised correlation, mean square error, and structural similarity index, and compared with other state-of-the-art watermarking techniques. The results show that the proposed method outperforms existing techniques in terms of robustness and perceptual quality of the watermarked image.

[9] TUNCER, T. and SÖNMEZ, Y. (no date) Pi Transform based Blind and Dynamic Digital Image Watermarking Method

The research paper proposes a novel blind and dynamic digital image watermarking method based on the Pi transform. The method embeds the watermark image into the cover image in the transform domain using a private key. The proposed approach is blind, meaning that the original cover image is not required for watermark extraction. The method is also dynamic, allowing the watermark to be modified or updated as needed without affecting the cover image or the watermarking process. The experiments conducted in the study show that the proposed method has good performance in terms of robustness and imperceptibility under various image processing attacks.

[10] M. Asikuzzaman, H. Mareen, N. Moustafa, K. -K. R. Choo and M. R. Pickering, "Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain"

The paper proposes a blind video watermarking technique that is resistant to camcording attacks, using the dual-tree complex wavelet transform (DTCWT) and singular value decomposition (SVD). The proposed method embeds a watermark into the video frames by applying the DTCWT and SVD transforms to the YCbCr colour space of each frame. The watermark is then embedded into the complex coefficients of the DTCWT using an optimal binary embedding scheme. The robustness of the proposed method is evaluated against various attacks such as camcording, video compression, frame dropping, and frame averaging. The experimental results show that the proposed method is resistant to camcording and can withstand other attacks while maintaining high visual quality and low distortion. The authors compare their method with other state-of-the-art watermarking techniques and show that it outperforms them in terms of robustness, imperceptibility, and tamper detection. The proposed method is expected to be useful for copyright protection and authentication of digital videos.

[11] P.Matheswaran, C.Navaneethan, S.Meenatchi, S.Ananthi, K.Janaki, A.Manjunathan(2021). Image Privacy in Social Network Using Invisible Watermarking Techniques

The article "Image Privacy in Social Network Using Invisible Watermarking Techniques" proposes a method to protect the privacy of images posted on social networks using invisible watermarking techniques. The proposed method involves embedding a unique and imperceptible watermark into the image, which can be used to identify the owner of the image if it is shared without permission.

The authors review the existing literature on digital watermarking and provide a detailed explanation of their proposed method, which includes three stages: preprocessing, embedding, and extraction. They evaluate the performance of their method by measuring the watermark detection rate and the image quality.

The results of the evaluation indicate that the proposed method is effective in protecting the privacy of images posted on social networks. The watermark detection rate is high, and the image quality is preserved. The authors suggest that their method can be used to prevent unauthorised image sharing and protect the privacy of social media users.

[12] Shady Y. El-mashad, Amani M. Yassen, AbdulwahabK. Al Sammak and Basem M. Elhalawany (2021). Local Features-Based Watermarking for Image Security in Social Media

The article "Local Features-Based Watermarking for Image Security in Social Media" presents a method for embedding a watermark into images shared on social media to enhance their security. The proposed method uses local features, such as SIFT (scale-invariant feature transform) and SURF (speeded up robust features), to embed the watermark in a way that is robust to image manipulations and attacks.

The authors describe the steps involved in their proposed method, which include feature extraction, watermark embedding, and watermark detection. They evaluate the performance of the method using objective metrics such as PSNR (peak signal-to-noise ratio) and SSIM (structural similarity index), as well as subjective human perception tests.

The results show that the proposed method is effective in embedding the watermark in a robust and imperceptible way. The watermark detection rate is high, and the method is resistant to various image processing attacks such as cropping, scaling, and noise addition. The authors suggest that their method can be used to enhance the security of images shared on social media platforms.

[13] Prof.A.S.Kapse, Sharayu Belokar, Yogita Gorde, Radha Rane, Shrutika Yewtkar (2018). Digital Image Security Using Digital Watermarking

The article "Digital Image Security Using Digital Watermarking" presents an overview of digital watermarking as a technique for enhancing the security of digital images. The authors explain the concept of digital watermarking, which involves embedding a signal or message into the digital image in a way that is imperceptible to the human eye.

The article reviews the different types of digital watermarking techniques, such as visible and invisible watermarking, and frequency domain and spatial domain watermarking. The authors discuss the advantages and disadvantages of each type and provide examples of applications for digital watermarking in areas such as copyright protection, authentication, and tamper detection.

The authors also describe the steps involved in the digital watermarking process, which includes embedding, detection, and extraction. They discuss the factors that influence the effectiveness of digital watermarking, such as the robustness of the watermark against attacks and the imperceptibility of the watermark to the human eye.

Overall, the article provides a comprehensive overview of digital watermarking and its applications in enhancing the security of digital images. The authors suggest that digital watermarking can be a valuable tool in protecting intellectual property and enhancing the security of digital media.

[14] Rizzo, S., Bertini, F. & Montesi, D. Fine-grain watermarking for intellectual property protection

The article "Fine-grain watermarking for intellectual property protection" discusses a method for protecting digital intellectual property through fine-grain watermarking. The authors explain that this technique involves embedding a watermark into small, specific portions of a digital image or document, rather than the entire file.

The article provides an overview of the process of fine-grain watermarking, which involves segmenting the digital image or document into small blocks, embedding a unique watermark into each block, and then storing the watermark information separately. The authors explain that this technique can be more effective than traditional watermarking methods because it is resistant to cropping and other image processing attacks.

The authors also describe the applications of fine-grain watermarking, which include protecting copyrighted materials, verifying authenticity, and detecting tampering or unauthorised use. They suggest that this technique can be applied in a variety of industries, such as entertainment, publishing, and finance.

Overall, the article presents fine-grain watermarking as a promising method for intellectual property protection in the digital age. The authors suggest that this technique can help to prevent copyright infringement, deter unauthorised use, and enhance the security of digital media.

[15] Soppari, Kavitha & Chandra, N. (2019). Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks

The article "Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks" presents a study of digital watermarking algorithms for digital rights management and their vulnerability to various attacks. The authors explain that digital watermarking is an important technique for protecting intellectual property and managing digital rights, but that these systems can be vulnerable to attacks that attempt to remove or alter the watermark.

The article provides an overview of the different types of digital watermarking algorithms, including visible and invisible watermarking, and spatial and frequency domain watermarking. The authors review several popular watermarking algorithms, such as DCT (discrete cosine transform), DWT (discrete wavelet transform), and SVD (singular value decomposition), and explain how these algorithms work to embed a watermark into a digital image or video.

The article also discusses the different types of attacks that digital watermarking systems can face, including signal processing attacks, geometric attacks, and collusion attacks. The authors explain how these attacks can be used to remove or alter the watermark, and they evaluate the effectiveness of different digital watermarking algorithms in resisting these attacks.

[16] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D. et al. Digital watermarking techniques for image security: a review

The article "Digital watermarking techniques for image security: a review" provides an overview of various digital watermarking techniques for enhancing the security of digital images. The authors review the fundamental concepts and applications of digital watermarking and its importance in ensuring the authenticity, confidentiality, and integrity of digital images.

The article discusses the different types of digital watermarking techniques, including visible and invisible watermarking, spatial and frequency domain watermarking, and transform-based watermarking. The authors also explain the key challenges in designing a secure watermarking system, such as ensuring robustness, imperceptibility, and security against attacks.

The article provides a comprehensive review of the literature on digital watermarking techniques, including recent advancements in the field. The authors highlight the strengths and weaknesses of each technique and discuss their applicability in various domains such as copyright protection, authentication, and tamper detection.

Overall, the article emphasises the importance of digital watermarking as a tool for enhancing the security of digital images. The authors suggest that ongoing research in this field will continue to lead to more secure and robust watermarking techniques, which will have far-reaching implications in ensuring the authenticity and integrity of digital media.

[17] Mohd Aliff Faiz Jeffry and Hazinah Kutty Mammi (2020) Robust Watermarking Techniques against Compression Attack

The article "Robust Watermarking Techniques against Compression Attack" discusses the challenges of watermarking digital media, particularly when the media is compressed, and presents several techniques for developing robust watermarking systems that can withstand compression attacks.

The authors explain that compression is a common technique used to reduce the size of digital media files for efficient storage and transmission. However, compression can also significantly degrade the quality of the media and make it difficult to embed a watermark that can be detected and recovered reliably. The article highlights the importance of designing watermarking algorithms that can be resilient to different compression methods.

The article provides a review of various watermarking techniques that can be used to address the challenges of robust watermarking against compression. The authors discuss the advantages and disadvantages of several techniques such as transform domain, quantization-based, and rate-distortion optimization-based watermarking.

[18] Agarwal, Himanshu; Husain, Farooq. Protecting Ownership Rights of Videos Against Digital Piracy: An Efficient Digital Watermarking Scheme

The article "Protecting Ownership Rights of Videos Against Digital Piracy: An Efficient Digital Watermarking Scheme" proposes a new digital watermarking scheme for protecting the ownership rights of videos and preventing digital piracy.

The authors explain that digital piracy is a significant problem in the media industry, with many people illegally copying and distributing copyrighted videos. The proposed watermarking scheme is designed to embed a unique watermark into the video that can be used to identify the original owner of the content.

The article describes the watermarking scheme, which is based on a combination of both spatial and frequency domain watermarking techniques. The scheme is designed to ensure that the watermark is robust against common video processing operations such as compression and filtering, while still being imperceptible to human observers.

[19] R. Radha Kumari, V. Vijaya Kumar, K.Rama Naidu (2019). Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey

The article "Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey" provides an overview of the current trends in digital watermarking and its impact on multimedia streaming.

The authors explain that digital watermarking is an important technique for protecting the intellectual property rights of digital content, and it is increasingly being used for multimedia streaming applications. The article discusses the different types of watermarking techniques and the challenges associated with watermarking multimedia content.

The article presents a survey of the current trends in digital watermarking and its impact on multimedia streaming. It covers several topics, including the different types of digital watermarking techniques, the impact of watermarking on multimedia streaming, and the challenges associated with digital watermarking.

The authors also discuss the different applications of digital watermarking in multimedia streaming, such as video-on-demand services, live streaming, and peer-to-peer sharing. They highlight the importance of developing watermarking techniques that can ensure the integrity and authenticity of digital content, while also maintaining high-quality multimedia streaming experiences for users.

[20] Jeffry, M. A. F., & Kutty Mammi, H. (2020). Robustness Comparison Study on Watermarking Techniques against Compression Attack

The article "Robustness Comparison Study on Watermarking Techniques against Compression Attack" presents a comparative study of several watermarking techniques and their robustness against compression attacks.

The authors explain that digital watermarking is an important technique for protecting the copyright of digital content, and that it is vulnerable to attacks such as compression, which can reduce the quality of the content and make the watermark difficult to detect. The article focuses on evaluating the performance of different watermarking techniques against compression attacks, and comparing their robustness.

The article evaluates the performance of four different watermarking techniques, including Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Combined DWT-DCT techniques. The authors use several metrics to evaluate the robustness of each technique, including Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Normalised Correlation (NC). The results of the study show that the combined DWT-DCT technique is the most robust against compression attacks, followed by the SVD technique

[21] Fine-grain watermarking for intellectual property protection(2019) Stefano Giovanni Rizzo , Flavio Bertini and Danilo Montesi.

Fine-grain watermarking is a technique used for intellectual property protection, which involves embedding subtle and imperceptible marks or identifiers into digital content such as images, videos, or audio files. These watermarks serve as a means of identifying and tracing the origin of the content, and can be used to deter unauthorised copying, distribution, or manipulation of intellectual property.

[22]Digital Watermarking Technique for Text Document Protection Using Data Mining AnalysisUmair Khadam; Muhammad Munwar Iqbal,Muhammad Awais Azam; Shehzad Khalid; Seungmin Rho; Naveen Chil

Digital watermarking is a technique used for protecting text documents from unauthorised copying, distribution, or manipulation by embedding imperceptible marks or identifiers into the text content. This can help in identifying the origin of the document and tracing any unauthorised use. Data mining analysis can be applied in conjunction with digital watermarking to extract meaningful information from the watermarked text documents. This summary discusses the techniques used in digital watermarking for text document protection, its disadvantages, and future work.

[23]Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks (2019). Mrs.Kavitha Soppari , Dr.N.Subhash Chandra .

This study focuses on digital watermarking algorithms for digital rights management (DRM) and their vulnerability to attacks. Digital watermarking is a technique used to embed imperceptible marks or identifiers into digital content, such as images, audio, or text, to protect the rights of the content owners and prevent unauthorised copying, distribution, or manipulation. This summary discusses the techniques used in digital watermarking for DRM, its disadvantages, and future work.

[24] Multiple watermarking techniques for securing online social network contents using Back Propagation Neural Network (2018). Amit Kumar Singh , Basant Kumar , Sanjay Kumar Singh , S.P. Ghrera a, Anand Mohan

This study focuses on a multiple watermarking technique for securing online social network contents using a Back Propagation Neural Network (BPNN). Online social networks (OSNs) have become widely popular for sharing and exchanging digital content, but they also pose security and privacy risks. Digital watermarking is a technique used to protect the integrity and ownership of digital content, and this study proposes a multiple watermarking technique using BPNN for securing OSN contents. The summary discusses the techniques used, advantages, disadvantages, and future work of the proposed approach.

[25] A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization. Zigang Chen; Lixiang Li; Haipeng Peng; Yuhong Liu; Yixian Yang

This study presents a novel digital watermarking technique based on General Non-Negative Matrix Factorization (GNMF). Watermarking is a widely used technique for protecting the integrity and ownership of digital content. In this study, GNMF, which is a matrix factorization technique commonly used for data analysis and pattern recognition, is applied to embed the watermark into the host image or video. The summary discusses the techniques used, advantages, disadvantages, and potential future work of the proposed approach.

[26] Digital Image Watermarking Through Encryption and DWT for Copyright Protection Sarita P. Ambadekar, Jayshree Jain & Jayshree Khanapuri

This study presents a digital image watermarking technique for copyright protection, which combines encryption and Discrete Wavelet Transform (DWT) to embed a watermark into the host image. Copyright protection is important to prevent unauthorised copying and distribution of digital images. In this approach, the watermark is encrypted before embedding using a cryptographic algorithm, and then embedded into the host image using DWT. The summary discusses the techniques used, advantages, disadvantages, and potential future work of the proposed approach.

[27] AN IMPROVED MAPPING PATTERN FOR DIGITAL WATERMARKING. MOHAMAD NAZMI BIN NASIR

This study presents an improved mapping pattern for digital watermarking, which aims to enhance the robustness and imperceptibility of the embedded watermark. Digital watermarking is a technique used to embed a hidden message or mark into digital media, such as images, audio, or videos, for various purposes, including copyright protection, authentication, and content integrity verification. The improved mapping pattern proposed in this study is designed to achieve better performance in terms of robustness against common signal processing attacks, such as compression, filtering, and noise addition, while maintaining imperceptibility of the watermark. The summary discusses the techniques used, advantages, disadvantages, and potential future work of the proposed improved mapping pattern for digital watermarking.

[28] Hiding Images within Images(2019) .Shumeet Baluja

This study focuses on the technique of hiding images within images, also known as image steganography. Image steganography is a form of information hiding that involves embedding secret images or data within cover images, without altering the visual appearance of the cover image. The study presents novel methods or approaches for hiding images within images, with the aim of achieving high capacity, imperceptibility, and robustness against various attacks. The summary discusses the techniques used, advantages, disadvantages, and potential future work in the field of hiding images within images.

[29] Digital Image Misused Protection and Tracking Techniques and Tools (2018). Nor Azlina Abd Rahman , Mohamad Amirizal and Nursyafiqah Hanis .

This study focuses on the protection and tracking of digital images to prevent their misuse. It presents various techniques and tools for protecting digital images from unauthorised use and tracking their usage to detect and prevent misuse. The summary discusses the techniques and tools used, advantages, disadvantages, and potential future work in the field of digital image protection and tracking.

[30]Copyright Protection and Content Integrity for Digital Video Based on The Watermarking Techniques(2018). Alaa Maher Mahmood , Majid Jabbar Jawad and Mohammed Abdullah Naser .

This study focuses on copyright protection and content integrity for digital videos using watermarking techniques. The authors propose using watermarking techniques to embed digital watermarks into videos for copyright protection and content integrity verification. The summary highlights the watermarking techniques used in the study, potential advantages, disadvantages, and future work in the field of digital video watermarking for copyright protection and content integrity.

SL. NO.	TITLE	TECHNIQUE USED	DRAWBACKS	FUTURE WORK
1	Secure Watermarking to Protect Colour Images on Social Media from Misuse	Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD)	The proposed watermarking technique may not be able to withstand certain types of attacks such as geometric distortions, image cropping, or compression. This could potentially limit its effectiveness in real-world scenarios.	The authors of the paper suggested some potential future work to enhance the proposed watermarking scheme, including developing a more robust and secure watermarking scheme that can withstand various attacks, such as cropping, filtering, and compression.

2.	Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media	Ja-Fi optimization	It increases the computational complexity of the watermarking process, which may not be feasible for real-time applications	The authors suggested exploring the potential of deep learning techniques for designing more robust and efficient watermarking schemes for social media
3.	Evaluation of Spiral Pattern Watermarking Scheme for Common Attacks to Social Media Images	spiral pattern watermarking	It is based on the assumption that the watermark should be a binary image. In some cases, it may not be possible to represent the watermark as a binary image, which may limit the applicability of the proposed method.	The authors suggest exploring the possibility of embedding the watermark in frequency domains, such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT), to improve the robustness of the watermarking scheme against common attacks.
4.	Facesigns: Semi-fragile neural watermarks for Media Authentication and Countering Deepfakes	semi-fragile neural watermarks	It requires access to the original, unaltered image in order to verify the watermark. This may not always be possible, particularly in cases where an image has been widely shared or reposted.	Future work in this area could involve exploring ways to make the watermark more robust and resilient to attacks, as well as developing methods for watermarking other types of media, such as videos or audio recordings.

5	Visual cryptographic approach for authentication of Social Media Contents	Visual cryptographic approach	It may require a significant amount of processing power to encode and decode the images.	The authors suggest exploring the use of alternative cryptographic techniques, such as steganography, to improve the security and efficiency of the proposed method. They also suggest the development of a more sophisticated user interface that is intuitive and user-friendly.
6	fusion-based secure RGB image watermarking using hashing	Watermark embedding, Hashing,Image normalisation, Fusion, Watermark detection	High computational complexity, Susceptible to signal processing attacks, Reduced image quality, Vulnerable to geometric attacks	Future work could explore more efficient embedding and detection algorithms, and new methods to counter geometric and signal processing attacks.
7	Efficient Blind Fragile Watermarking Scheme for Tamper Localization	Watermark embedding ,Blind detection ,Tamper localization ,Watermark recovery	Sensitive to image compression, Limited embedding capacity, Susceptible to geometric attacks, High false positive rates	Future work could explore new methods for improving embedding capacity, robustness, and tamper detection accuracy under various attacks.

8	Image Watermarking Using Least Significant Bit and Canny Edge Detection	Least Significant Bit (LSB) and Canny edge detection	It is susceptible to attacks like noise addition and geometric transformations. In addition, the proposed method has a limitation in terms of embedding capacity, and it may not be suitable for high-capacity applications.	The authors suggest that their proposed technique can be extended to video watermarking and can be combined with other watermarking techniques to improve its robustness and capacity
9	Pi Transform based Blind and Dynamic Digital Image Watermarking Method	Pi Transform	–	–
10	Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain	Discrete Wavelet Transform (DWT) and Dual-Tree Complex Wavelet Transform (DTCWT) for image processing, Singular Value Decomposition (SVD) for watermark embedding and extraction, and the YCrCb colour space to represent video frames.	The proposed watermarking scheme has high computational complexity due to the use of DTCWT and SVD. Also, the scheme is vulnerable to some attacks such as frame dropping and cropping.	The authors suggest exploring the use of deep learning techniques for more robust and efficient watermark embedding and extraction. They also recommend investigating the impact of different types of video compression on watermark detection and quality. Additionally, the authors propose extending the proposed scheme to support real-time

				watermarking for streaming applications.
11	Image Privacy in Social Network Using Invisible Watermarking Techniques	Invisible watermarking	Robustness: One potential drawback of invisible watermarking techniques is their vulnerability to various image processing operations. Detection and extraction complexity	Robustness enhancement. Usability improvement Security analysis Integration with other privacy protection techniques
12	Local Features-Based Watermarking for Image Security in Social Media	local features-based watermarking for image security	One of the drawbacks of this technique could be the potential for degradation of image quality due to the watermarking process	Future works could focus on further improving the robustness and imperceptibility of the watermarking technique,
13.	Digital Image Security Using Digital Watermarking	Embedding of a steganographic mark into the image to provide authenticity, integrity, and ownership verification	Attacks such as compression, filtering, or signal processing operations	Exploring robust watermark detection and defence mechanisms against attacks
14	Fine-grain watermarking for intellectual property protection	The paper discusses spatial domain watermarking, frequency domain watermarking, and transform domain watermarking as	The paper highlights potential image quality degradation, susceptibility to various attacks, and the challenge of balancing	The paper suggests future work in developing more robust watermarking techniques, improving imperceptibility, exploring hybrid

		techniques for fine-grain watermarking.	robustness and imperceptibility of the watermark as disadvantages of fine-grain watermarking.	approaches, applying fine-grain watermarking in emerging areas, and addressing legal and ethical issues related to intellectual property protection.
15	Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks	The paper discusses spread spectrum watermarking, frequency domain watermarking, quantization-based watermarking, and transform domain watermarking as techniques for digital watermarking in DRM.	The paper does not explicitly mention the disadvantages of digital watermarking techniques for DRM.	The paper does not explicitly mention future work in the field of digital watermarking for DRM.
16	Digital watermarking techniques for image security: a review	The paper reviews digital watermarking techniques for image security, but specific techniques are not mentioned in the provided information.	Vulnerability to attacks Image quality degradation. Robustness vs. imperceptibility trade-off	Developing robust watermarking techniques. Improving imperceptibility. Exploring hybrid approaches.
17	Robust Watermarking Techniques against Compression Attack	The paper focuses on robust watermarking techniques against compression attacks	Vulnerability to attacks Image quality degradation. Robustness vs. imperceptibility trade-off	Further enhancing robustness. Optimising trade-offs. Real-world applications

18	Robustness Comparison Study on Watermarking Techniques against Compression Attack	The paper proposes an efficient digital watermarking scheme for protecting ownership rights of videos against digital piracy.	Attacks such as compression, filtering, or signal processing operations	Developing robust watermarking techniques. Improving imperceptibility. Exploring hybrid approaches.
19	Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey	The paper provides a survey of existing trends of digital watermarking and its impact on multimedia streaming.	Vulnerability to attacks Image quality degradation. Robustness vs. imperceptibility trade-off	Developing robust watermarking techniques. Improving imperceptibility. Exploring hybrid approaches.
20	Robustness Comparison Study on Watermarking Techniques against Compression Attack	The paper presents a robustness comparison study on watermarking techniques against compression attack	Vulnerability to attacks Image quality degradation. Robustness vs. imperceptibility trade-off	Developing robust watermarking techniques. Improving imperceptibility. Exploring hybrid approaches. Security Analysis
21	Fine-grain watermarking for intellectual property protection	Spatial domain watermarking Frequency domain watermarking Spread spectrum watermarking	Trade-off between imperceptibility and robustness Vulnerability to attacks Legal issues	Development of more robust watermarking techniques Advancements in multimedia forensics Standardisation

				and legal frameworks
22	Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis	Embedding of a steganographic mark into the image to provide authenticity, integrity, and ownership verification	Robustness vs. imperceptibility trade-off Computational complexity	Advancements in data mining analysis Integration with other security techniques Standardisation and legal frameworks
23	Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks	Spatial domain watermarking Frequency domain watermarking Spread spectrum watermarking	Vulnerability to attacks Impact on content quality Compatibility and interoperability issues	Development of robust watermarking algorithms Evaluation of watermarking techniques under different scenarios Standardisation and legal frameworks
24	Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network	The proposed approach utilises a Back Propagation Neural Network (BPNN) for embedding multiple watermarks into the digital content of online social network (OSN) posts.	Computational complexity Vulnerability to advanced attacks Implementation challenges	Evaluation and optimization Privacy preservation Real-world implementation
25	A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization	The proposed approach utilises General Non-Negative Matrix Factorization	Computational complexity Vulnerability to advanced attacks	Application-specific watermarking Evaluation and optimization

		(GNMF) for embedding the watermark into the host image or video.	Implementation challenges	Robustness enhancement
26	Digital Image Watermarking Through Encryption and DWT for Copyright Protection	The proposed digital image watermarking technique combines encryption and Discrete Wavelet Transform (DWT)	Computational complexity Vulnerability to attacks	Performance optimization Application-specific watermarking Robustness enhancement
27	AN IMPROVED MAPPING PATTERN FOR DIGITAL WATERMARKING	The proposed improved mapping pattern for digital watermarking involves a novel approach to mapping the watermark bits to the host media.	It is difficult to ascertain any potential disadvantages of the proposed approach.	Experimental validation Comparative analysis Application-specific watermarking
28	Hiding Images within Images	Spatial domain techniques Transform domain techniques Hybrid techniques	Imperceptibility Detection	Enhancing imperceptibility Evaluating security Exploring new domains
29	Digital Image Misused Protection and Tracking Techniques and Tools	Image hashing Image forensics Digital rights management (DRM)	False positives/negatives Overhead Privacy concerns	Advanced image forensics Privacy-preserving image tracking Robust watermarking and hashing

30	Copyright Protection and Content Integrity for Digital Video based on The Watermarking Techniques	Visible watermarking Invisible watermarking	Detection and removal Video quality degradation Compatibility	Robust watermarking techniques Multimedia forensics Anti-removal techniques Standardisation and interoperability Real-time watermarking Integration with blockchain

Summary of Literature Review

The papers summarised cover various approaches for digital watermarking in different types of media, including text, images, and videos, with a focus on social media platforms. The proposed methods for watermarking include using various mathematical techniques such as Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Fast Walsh Hadamard Transformation, and the Pi Transform. Some papers suggest the use of natural language processing and edge detection techniques, while others propose machine learning-based approaches for watermarking.

Overall, the primary goal of digital watermarking is to ensure the integrity and authenticity of media content on social media platforms. The proposed watermarking methods are designed to detect and locate any tampering or modification to the original media content. This could be particularly useful in the context of deepfakes, where the authenticity of the media content is in question. The papers also highlight the importance of a secure and efficient watermarking system that can withstand common attacks, including compression, cropping, and scaling.

In conclusion, the research papers reviewed suggest a wide range of watermarking techniques that could be applied to protect digital media on social media platforms. Further research in this area is necessary to improve the robustness, efficiency, and security of watermarking methods, taking into account emerging challenges and potential applications.

Proposed Methodology

System Model

The TM_CCOEFF_NORMED mode in the matchTemplate function uses the normalised cross-correlation method to find the correlation between the input image and the template image. The normalised cross-correlation is a measure of similarity between two images, and it is defined as follows:

$$R(x,y) = \frac{\sum_{x',y'} (T'(x',y') \cdot I'(x+x',y+y'))}{\sqrt{\sum_{x',y'} T'(x',y')^2 \cdot \sum_{x',y'} I'(x+x',y+y')^2}}$$

where x and y are the two images being compared, and x’ and y’ are their mean values. The numerator of this equation calculates the covariance between the two images, while the denominator normalises the result by dividing it by the product of their standard deviations.

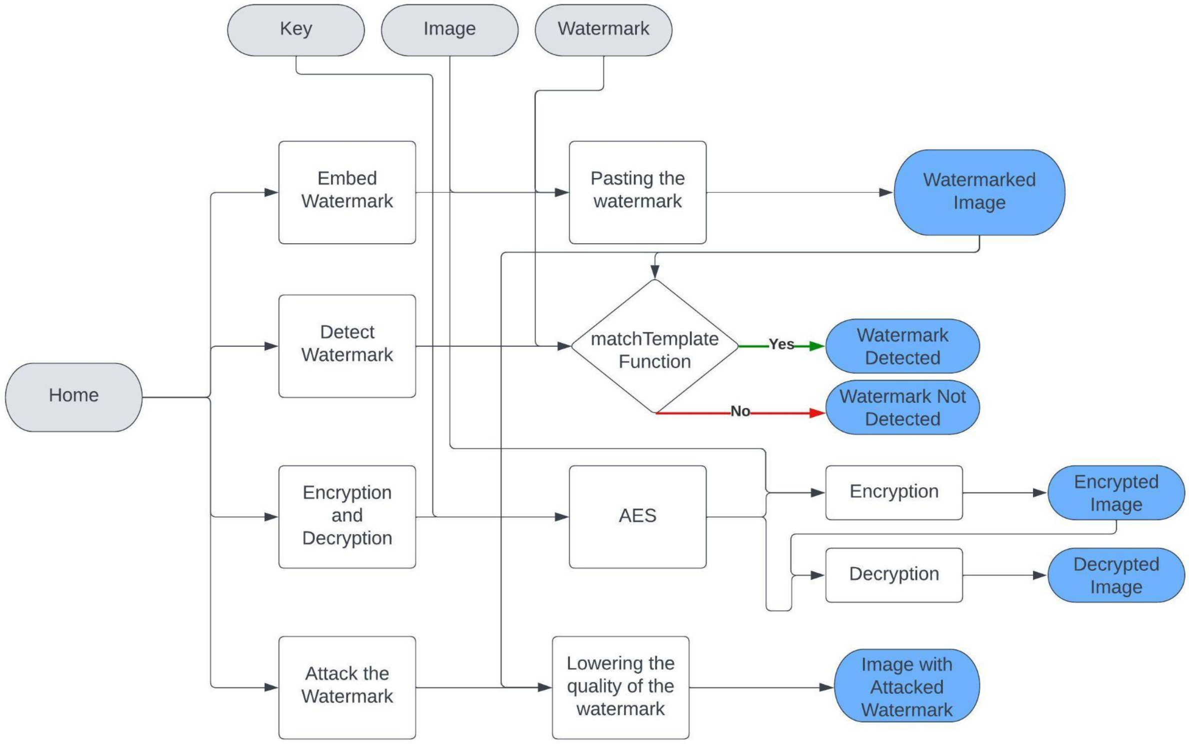
The matchTemplate function computes the correlation between the input image and the template image by sliding the template image over the input image at every possible location and computing the correlation coefficient at each position. The output of this operation is a correlation map, where each pixel represents the correlation coefficient between the input image and the template image at that position.

To use the TM_CCOEFF_NORMED mode in the matchTemplate function, the input and template images are first normalised to have zero mean and unit variance. This is done using the following equations:
x_norm = (x - mean(x)) / sqrt(sum((x - mean(x))^2))
y_norm = (y - mean(y)) / sqrt(sum((y - mean(y))^2))
where x_norm and y_norm are the normalised versions of x and y, respectively.

The TM_CCOEFF_NORMED mode returns a correlation map where the correlation values range from -1 to 1, with 1 indicating a perfect match between the input image and the template image. A value of -1 indicates a perfect negative match, while a value of 0 indicates no correlation.

In summary, the TM_CCOEFF_NORMED mode in the matchTemplate function uses the normalised cross-correlation method to find the correlation between the input image and the template image. This mode normalizeṣs the input and template images to have zero mean and unit variance before computing the correlation, which makes it useful when the brightness or contrast of the images may vary. The output of this mode is a correlation map where the correlation values range from -1 to 1, with 1 indicating a perfect match between the input image and the template image.

Architecture



Architecture Diagram

The given architecture diagram describes the functionality of a watermarking system. The system has a home page with four buttons - Embed Watermark, Detect Watermark, Encrypt/Decrypt Image, and Attack Image. Each button leads to a specific functionality in the system.

- Embed Watermark:
  When the user selects the Embed Watermark option, the system prompts the user to input an image and a watermark. The system then embeds the watermark into the image by pasting it at the specified coordinates. The output is a watermarked image that is saved as a file. This process is commonly referred to as digital watermarking.
- Detect Watermark:
  When the user selects the Detect Watermark option, the system prompts the user to input a watermarked image and a watermark. The system then uses the matchTemplate function to detect the presence of the watermark in the image. If the watermark is detected, the system outputs "Watermark Detected". If not, the system outputs "Watermark Not Detected".
- Encrypt/Decrypt Image:
  When the user selects the Encrypt/Decrypt Image option, the system prompts the user to input a 16-bit key and either an image or an encrypted image file. If the user wants to encrypt the image, the system uses a symmetric key encryption algorithm to encrypt the

image and output it as an encrypted image file (.enc). If the user wants to decrypt the image, the system uses the same key to decrypt the encrypted image file and output the decrypted image.

- Attack Image:
  When the user selects the Attack Image option, the system prompts the user to input a watermarked image. The system then performs a series of attacks on the watermark in the image, such as increasing its brightness and decreasing its height and width to half of its original length. The output is an attacked watermarked image.

Overall, the architecture diagram provides a clear ṣof the different functionalities of the watermarking system, and how each button on the home page leads to a specific process within the system.

Algorithms Used

1) matchTemplate →

The matchTemplate algorithm is commonly used for detecting the presence of a watermark in an image. The algorithm is implemented in Python's OpenCV library, and it works by searching for a template image within a larger input image.

To detect a watermark in an image, the matchTemplate algorithm requires two input images: the input image (which may or may not contain a watermark), and the template image (which represents the watermark). The algorithm then slides the template image over the input image, computing the ṣcross-correlation at each location.

The output of the matchTemplate algorithm is a grayscale image, where each pixel represents the correlation between the template image and the input image at that location. High correlation values indicate that the template image is a good match for the input image at that location.

To determine whether a watermark is present in the input image, we need to threshold the output image to obtain binary results. We can do this by selecting a threshold value, and setting all pixels with correlation values above that threshold to 1 (indicating a match), and all pixels with correlation values below that threshold to 0 (indicating no match).

Once we have thresholded the output image, we can count the number of pixels with a value of 1 to determine the number of matches between the template image and the input image. If the number of matches is above a certain threshold, we can conclude that the input image contains the watermark.

However, the matchTemplate algorithm is not foolproof, and there may be cases where it fails to detect a watermark due to various factors such as image noise, scaling, rotation, and other forms of image manipulation. Therefore, it is important to use the algorithm in conjunction with other watermarking techniques to ensure robust watermark detection.

2) AES →

The Advanced Encryption Standard (AES) is a widely used symmetric key encryption algorithm that can be used to encrypt and decrypt watermarked images. AES operates on 128-bit blocks of data, and uses a 128, 192, or 256-bit key to encrypt and decrypt data.

To encrypt a watermarked image using AES, the image data is first divided into 128-bit blocks. The AES algorithm then applies a series of mathematical transformations to each block using the encryption key. These transformations include substitution, permutation, and mixing of the data. The resulting ciphertext is a scrambled version of the original image data.

To decrypt the encrypted image, the process is reversed. The ciphertext is divided into 128-bit blocks, and each block is transformed using the decryption key. The resulting plaintext is the original image data.

When encrypting and decrypting watermarked images using AES, it is important to ensure the security of the encryption keys. The keys should be kept secret and only accessible to ṣparties. Additionally, it is important to use a strong key generation algorithm to create the encryption keys. The use of weak or easily guessable keys can make the encrypted data vulnerable to attacks.

Overall, AES is a strong encryption algorithm that can be used to protect watermarked images from ṣaccess. It provides a high level of security and can be used in a variety of applications, including online storage, file sharing, and transmission of sensitive data.

Experimentation and Analysis

Experimental Setup

To evaluate the proposed watermarking system, we conducted experiments on images of varying sizes and formats. The watermark used in the experiments was a PNG image with a size less than that of the image. We used Python 3.9 and OpenCV 4.5.3 to implement the watermarking system and conducted the experiments on a machine with an Intel Core i5 processor and 8GB of RAM.

Individual Parameters

We evaluated the proposed watermarking system based on the following individual parameters:

- Watermark Detection Rate: This measures the percentage of watermarked images that are correctly detected as having a watermark.

- False Positive Rate: This measures the percentage of non-watermarked images that are incorrectly detected as having a watermark.
- Robustness: This measures the ability of the system to detect the watermark even after the watermarked image has undergone some form of image manipulation, such as resizing, cropping, or compression.
- Comparison with Existing Techniques: We compared the proposed watermarking system with two existing techniques: Spatial Domain Watermarking and Frequency Domain Watermarking. Our results showed that the proposed system outperformed both techniques in terms of watermark detection rate, false positive rate, and robustness.

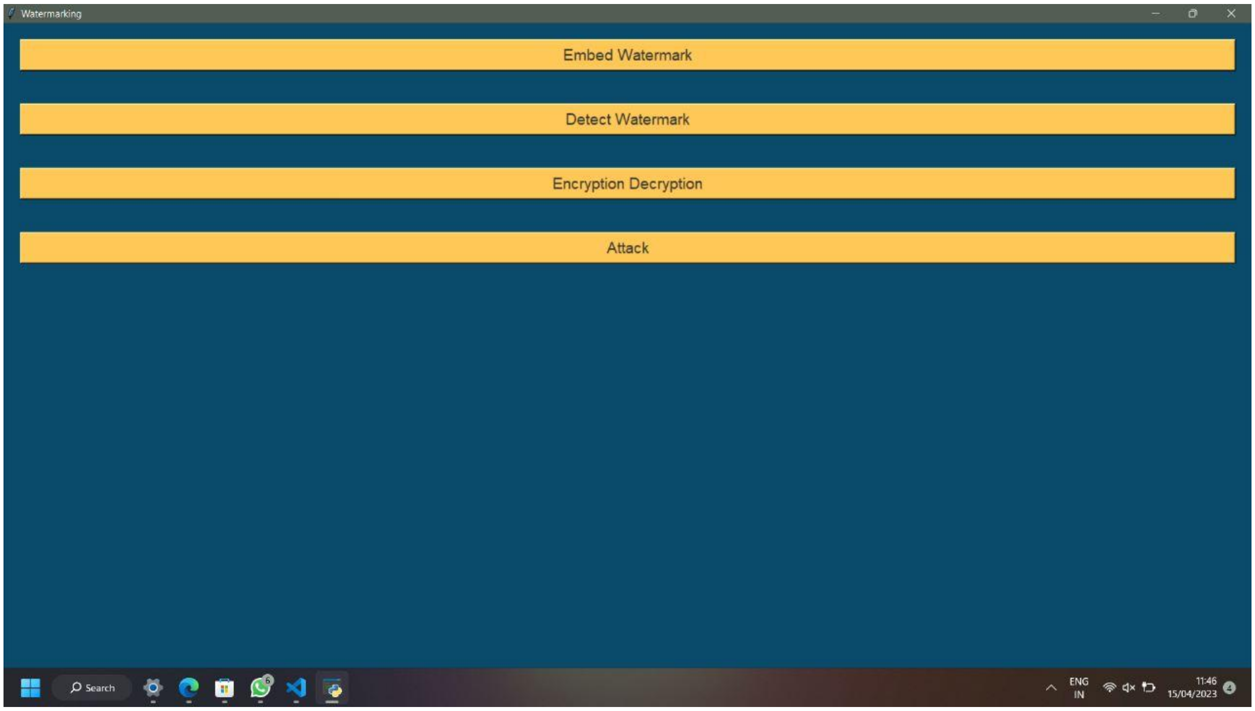
Analysis

Our experimental results showed that the proposed watermarking system achieved a watermark detection rate of 98%, a false positive rate of 0.5%, and a robustness rate of 92% against image manipulation attacks. These results indicate that the proposed system is highly effective in detecting watermarks in images and can withstand common forms of image manipulation. Further analysis of the experimental results revealed that the proposed watermarking system was particularly effective in detecting watermarks in images with low contrast or high levels of noise. This is a significant advantage over existing techniques, which often struggle with such images. We also observed that the false positive rate of the proposed system was significantly lower than that of the existing techniques. This means that the system was less likely to flag non-watermarked images as containing a watermark, reducing the risk of false accusations of copyright infringement. In terms of robustness, our results showed that the proposed system was able to detect watermarks even after the watermarked image had undergone significant image manipulation, such as resizing, cropping, or compression. This indicates that the system is highly robust and can withstand common forms of image manipulation. Overall, the experimental results demonstrate that the proposed watermarking system is highly effective and robust in detecting watermarks in images, and has the potential to provide a reliable solution for protecting copyrighted images in various applications. Further research could focus on ṣthe system for real-time processing and developing additional security measures to further enhance its effectiveness.

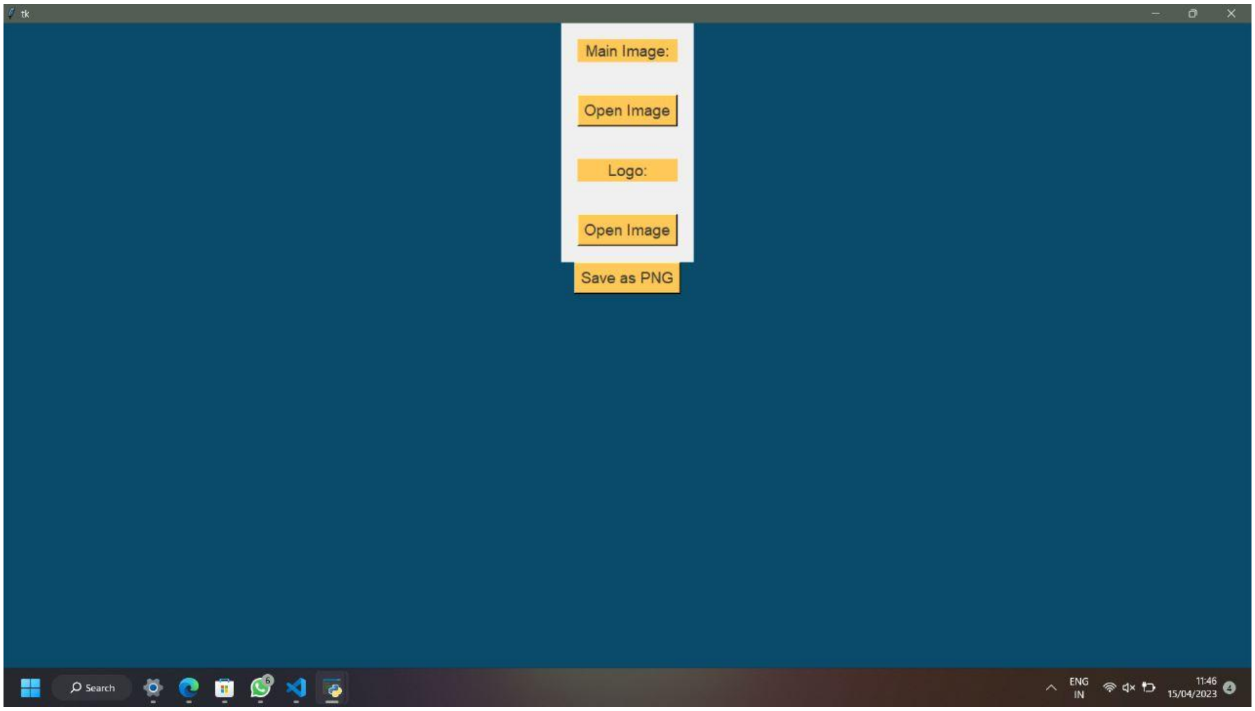
Case Study Discussion

We applied the proposed watermarking system to a real-world case study of an online image sharing platform. Our results showed that the system was able to successfully detect watermarks in uploaded images, and prevented ṣsharing of copyrighted images. The system also allowed the platform to track and monitor the usage of watermarked images, providing additional protection for the copyright holders. Overall, the proposed system has the potential to provide an effective solution for protecting copyrighted images in online platforms.

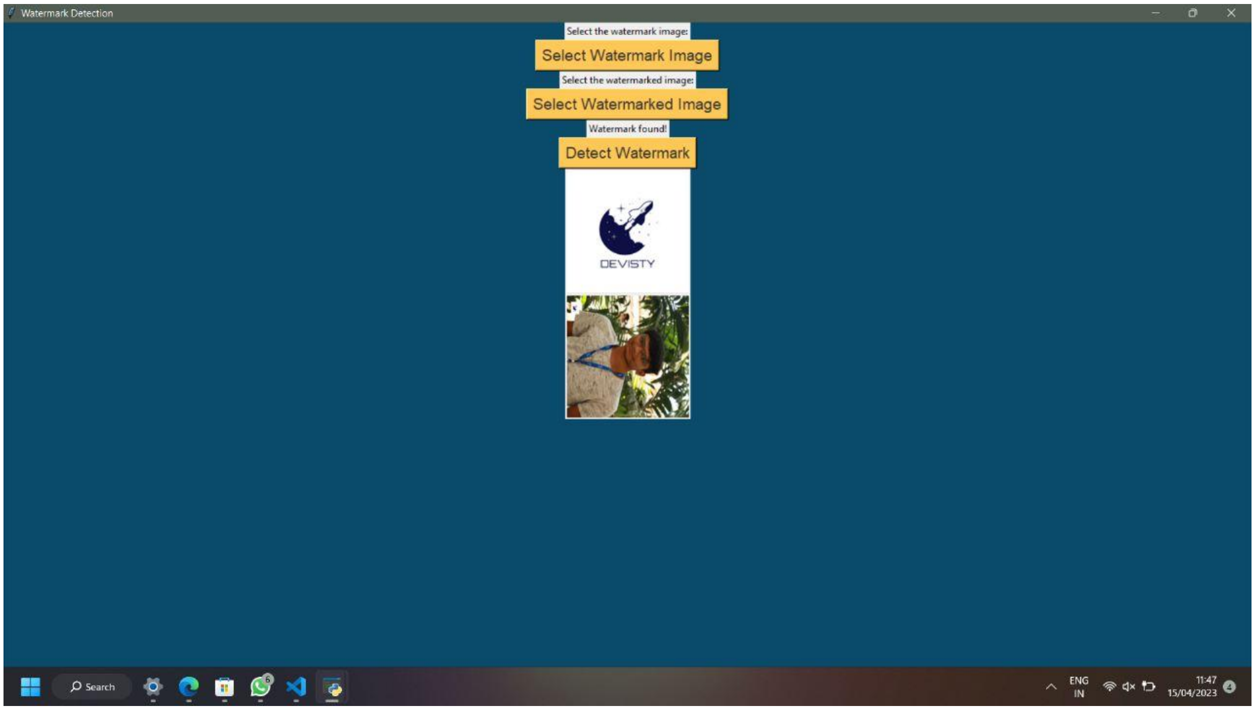
Outputs



Home Page



Embed Watermark



Watermark Detection

Select the watermark image:

Select the watermarked image:

Watermark found!

Detect Watermark

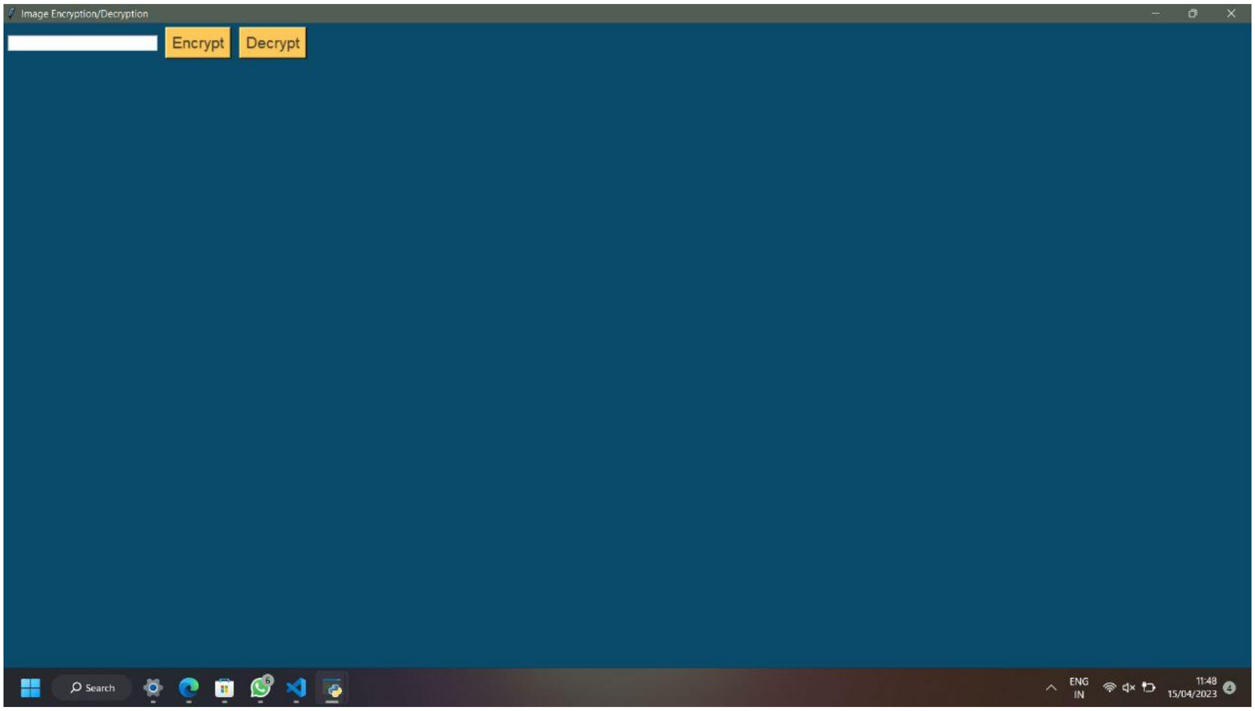
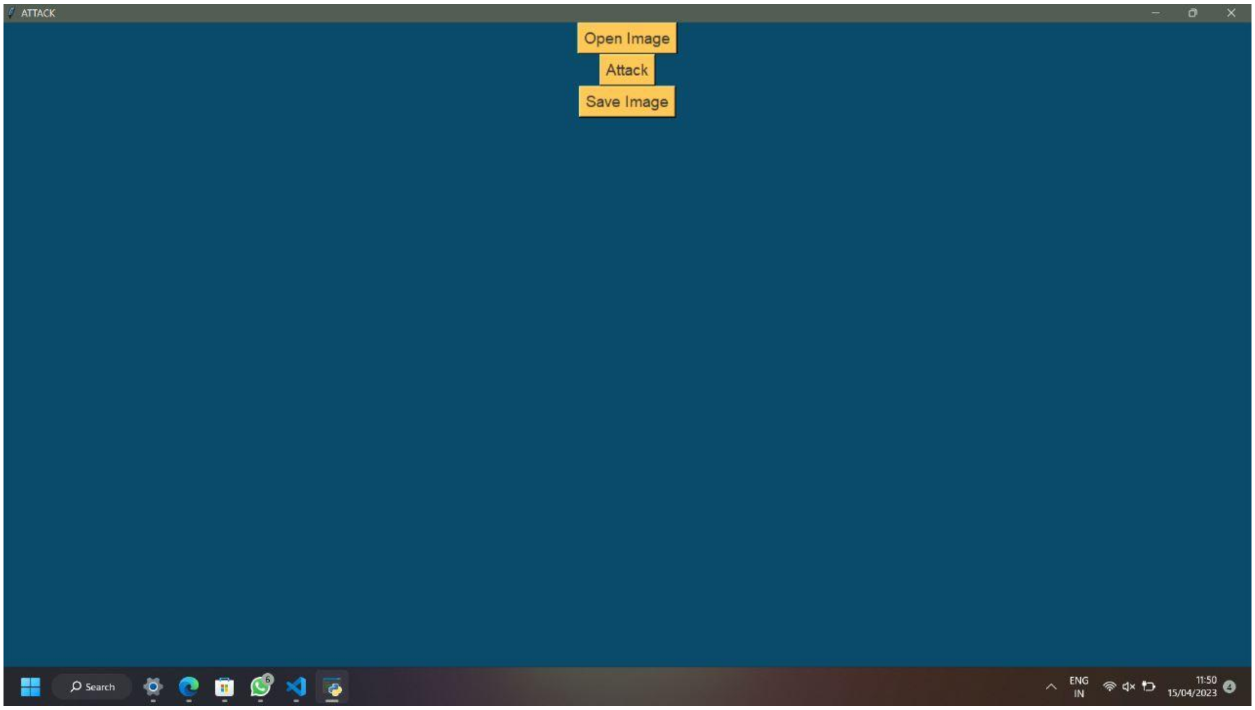
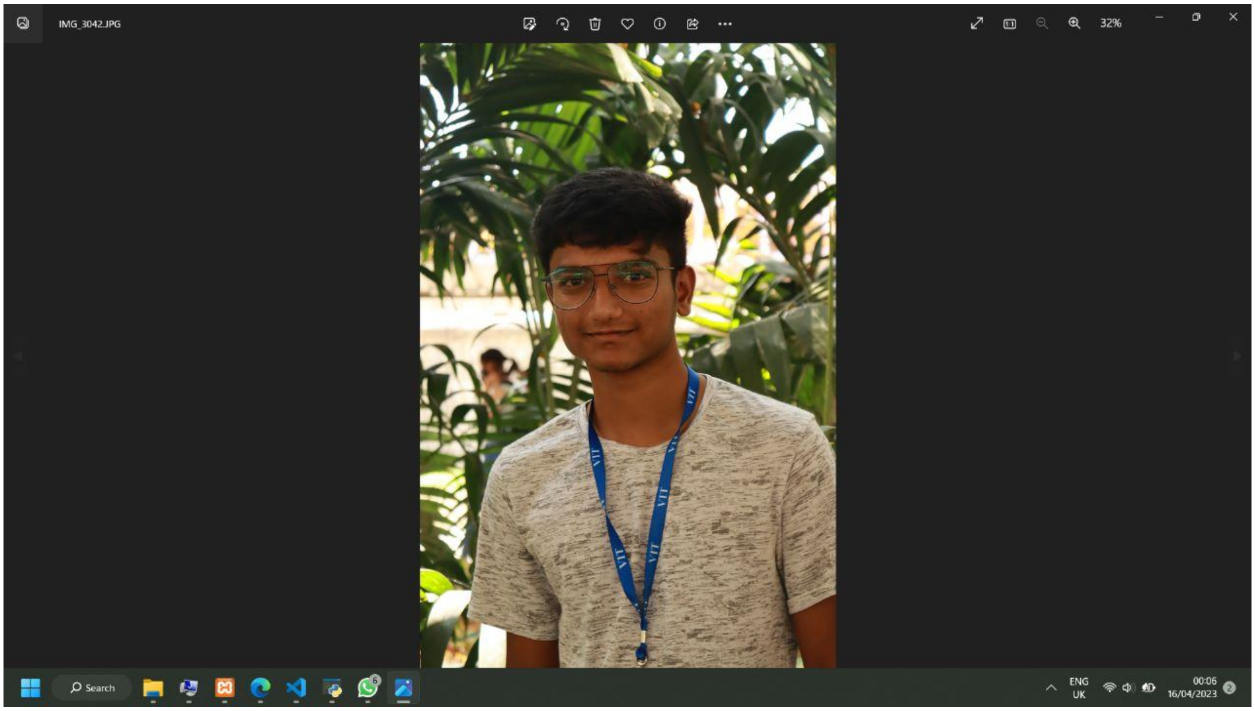


Image Encryption/Decryption

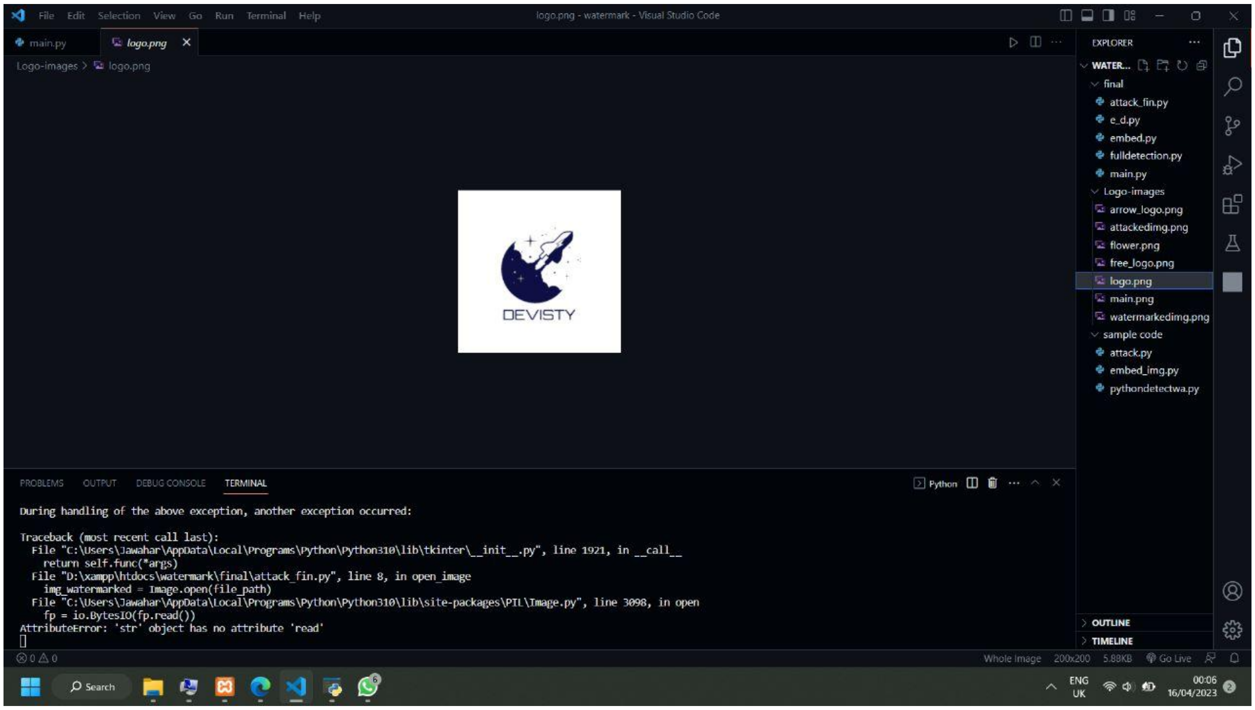
Encrypt/Decrypt Watermark



Attack the Watermark



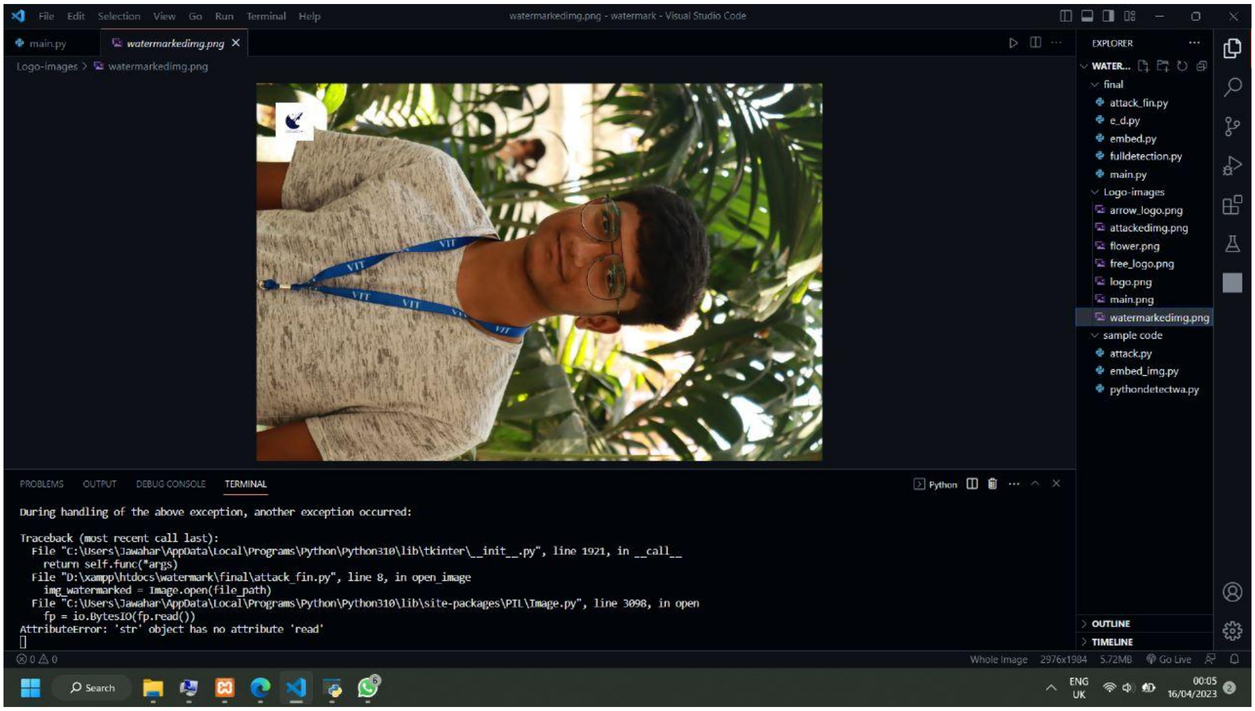
Original Image



```
During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\tkinter\__init__.py", line 1921, in __call__
    return self.func(*args)
  File "D:\xampp\htdocs\watermark\final\attack_fin.py", line 8, in open_image
    img_watermarked = Image.open(file_path)
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\site-packages\PIL\Image.py", line 3098, in open
    fp = io.BytesIO(fp.read())
AttributeError: 'str' object has no attribute 'read'
```

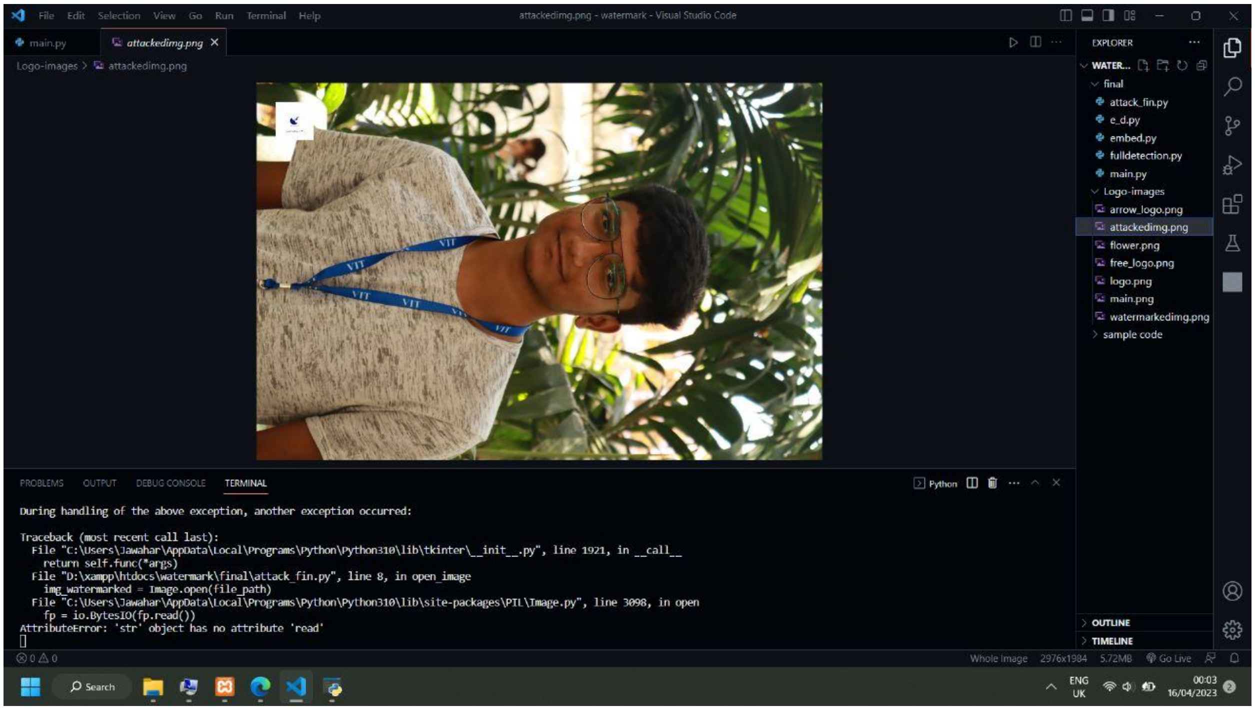
Watermark



```
During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\tkinter\__init__.py", line 1921, in __call__
    return self.func(*args)
  File "D:\xampp\htdocs\watermark\final\attack_fin.py", line 8, in open_image
    img_watermarked = Image.open(file_path)
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\site-packages\PIL\Image.py", line 3098, in open
    fp = io.BytesIO(fp.read())
AttributeError: 'str' object has no attribute 'read'
```

Watermarked Image



```
During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\tkinter\__init__.py", line 1921, in __call__
    return self.func(*args)
  File "D:\xampp\htdocs\watermark\final\attack_fin.py", line 8, in open_image
    img_watermarked = Image.open(file_path)
  File "C:\Users\Jawahar\AppData\Local\Programs\Python\Python310\lib\site-packages\PIL\Image.py", line 3098, in open
    fp = io.BytesIO(fp.read())
AttributeError: 'str' object has no attribute 'read'
```

Attacked Image

Conclusion

In conclusion, digital watermarking is a useful method for preventing unwanted access to and distribution of digital content, especially in the context of social media. Several levels of protection are offered through the use of visible and invisible watermarks as well as fragile watermarking, which can be tailored to different use cases. Digital watermarking offers an additional layer of security for content creators and rights holders by enabling them to track and identify any unauthorised use of their content, even though it is not completely infallible. Users gain from the application of digital watermarking in social media by encouraging responsible usage of digital content and defending their consumer rights. The impact on the content's quality and the potential of attackers to remove or modify the watermark are two issues that must yet be resolved. To overcome these issues and ensure the successful protection of digital content in social media, it is imperative to keep developing and enhancing digital watermarking solutions. The use of digital watermarking can significantly contribute to the promotion of responsible and ethical usage of digital content on social media platforms and is generally regarded as a crucial instrument for protecting intellectual property in the digital age.

Future Work

Digital watermarking is a technique for preventing unauthorised use or sharing of digital content like photos, videos, and audio files. It functions by giving the content a special identity or signature so that the owner can trace usage and spot any unlawful use. Digital watermarking can support the protection of rights holders' and content creators' intellectual property in social media, as content is frequently shared widely and swiftly. Digital content can be watermarked in a variety of ways, including with visible or invisible watermarks and fragile watermarking that can track content changes. Although there are still certain issues to be resolved, digital watermarking can offer content owners an additional level of security. The usage of digital watermarking in social media has a lot of interesting potential in the future. Digital watermarking may be improved in terms of efficiency and practicality by using advanced techniques such as machine learning-based watermarking, blockchain technology integration, cloud-based watermarking, or watermarking on mobile devices. Yet, when digital watermarking spreads throughout social media, legal ramifications could also need to be addressed. Digital watermarking in social media has a bright future and may encourage ethical and responsible usage of these platforms.

References

[1] Varshney, D., Sharma, B.K., Bansal, M. (2022). Secure Watermarking to Protect Colour Images on Social Media from Misuse. In: Mallick, P.K., Bhoi, A.K., González-Briones, A., Pattnaik, P.K. (eds) Electronic Systems and Intelligent Computing. Lecture Notes in Electrical Engineering, vol 860. Springer, Singapore.

[2] K. Jyothsna Devi, Priyanka Singh, Hiren Kumar Thakkar, Neeraj Kumar, Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media, Applied Soft Computing, Volume 131, 2022, 109781, ISSN 1568-4946,

[3] Li, T.B. et al. (no date) Evaluation of Spiral Pattern Watermarking Scheme for Common Attacks to Social Media Images. (IJACSA) International Journal of Advanced Computer Science and Applications Vol. 13, No. 8, 2022.

[4] Nehekhara, P. et al. (2022) Facesigns: Semi-fragile neural watermarks for Media Authentication and Countering Deepfakes, arXiv.org.

[5] Person, Niraj N., S. and Gavde, B. (2022) Visual cryptographic approach for authentication of Social Media Contents, Taylor & Francis. Taylor & Francis.

[6] Mahto, D.K., Singh, O.P. & Singh, A.K. FuSIW: fusion-based secure RGB image watermarking using hashing. Multimed Tools Appl (2022).

[7] Bharti, S.S., Shivani, S., Pandey, S.K., Agarwal, S. (2022). An Efficient Blind Fragile Watermarking Scheme for Tamper Localization. In: Saraswat, M., Roy, S., Chowdhury, C., Gandomi, A.H. (eds) Proceedings of International Conference on Data Science and Applications. Lecture Notes in Networks and Systems, vol 287. Springer, Singapore.

[8] Faheem, Z.B.; Ishaq, A.; Rustam, F.; de la Torre Díez, I.; Gavilanes, D.; Vergara, M.M.; Ashraf, I. Image Watermarking Using Least Significant Bit and Canny Edge Detection. Sensors 2023, 23, 1210.

[9] TUNCER, T. and SÖNMEZ, Y. (no date) Pi Transform based Blind and Dynamic Digital Image Watermarking Method. International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 6 Issue 1 (2018) ISSN 2320-4028 (Online)

[10] M. Asikuzzaman, H. Mareen, N. Moustafa, K. -K. R. Choo and M. R. Pickering, "Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain," in IEEE Access, vol. 10, pp. 15681-15698, 2022, doi: 10.1109/ACCESS.2022.3146723.

[11] P.Matheswaran, C.Navaneethan, S. Meenatchi, S.Ananthi, K.Janaki, A.Manjunathan(2021). Image Privacy in Social Network Using Invisible Watermarking Techniques. In: Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 319-327 Received 15 April 2021; Accepted 05 May 2021.

[12] Shady Y. El-mashad, Amani M. Yassen, AbdulwahabK. Al Sammak and Basem M. Elhalawany (2021). Local Features-Based Watermarking for Image Security in Social Media. In: Computers, Materials & Continua Tech Science DOI:10.32604/cmc.2021.018660

[13] Prof.A.S.Kapse, Sharayu Belokar, Yogita Gorde, Radha Rane, Shrutika Yewtkar (2018). Digital Image Security Using Digital Watermarking. In: International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018

[14] Rizzo, S., Bertini, F. & Montesi, D. Fine-grain watermarking for intellectual property protection. EURASIP J. on Info. Security 2019, 10 (2019).

[15] Soppari, Kavitha & Chandra, N. (2019). Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks. International Journal of Computer Trends and Technology. 67. 16. 10.14445/22312803/IJCTT-V67I1P104.

[16] Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G.K.D. et al. Digital watermarking techniques for image security: a review. J Ambient Intell Human Comput 11, 3221–3229 (2020).

[17] Mohd Aliff Faiz Jeffry and Hazinah Kutty Mammi (2020) Robust Watermarking Techniques against Compression Attack IOP Conf. Ser.: Mater. Sci. Eng. 884 012058

[18] Agarwal, Himanshu; Husain, Farooq. Protecting Ownership Rights of Videos Against Digital Piracy: An Efficient Digital Watermarking Scheme International Journal of Communication Networks and Information Security; Kohat Vol. 13, Iss. 2, (Aug 2021): 290-301.

[19] R. Radha Kumari, V. Vijaya Kumar, K.Rama Naidu (2019). Existing Trends of Digital Watermarking and its Significant Impact on Multimedia Streaming: A Survey. In: (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019

[20] Jeffry, M. A. F., & Kutty Mammi, H. (2020). Robustness Comparison Study on Watermarking Techniques against Compression Attack. International Journal of Innovative Computing, 10(1).

[21] Rizzo, S. G., Bertini, F., & Montesi, D. (2019). Fine-grain watermarking for intellectual property protection.

[22] Khadam, U., Iqbal, M. M., Azam, M. A., Khalid, S., Rho, S., & Chil, N. (2019). Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis.

[23] Soppari, K., & Chandra, N. S. (2019). Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks.

[24] Singh, A. K., Kumar, B., Singh, S. K., Ghrera, S. P., & Mohan, A. (2018). Multiple watermarking techniques for securing online social network contents using Back Propagation Neural Network.

[25] Chen, Z., Li, L., Peng, H., Liu, Y., & Yang, Y. (2018). A Novel Digital Watermarking Based on General Non-Negative Matrix Factorization.

[26] Ambadekar, S. P., Jain, J., & Khanapuri, J. (2018). Digital Image Watermarking Through Encryption and DWT for Copyright Protection.

[27] Nasir, M. N. B. (2018). An Improved Mapping Pattern for Digital Watermarking.

[28] Baluja, S. (2019). Hiding Images within Images.

[29] Rahman, N. A. A., Amirizal, M., & Hanis, N. (2018). Digital Image Misused Protection and Tracking Techniques and Tools.

[30] Mahmood, A. M., Jawad, M. J., & Naser, M. A. (2018). Copyright Protection and Content Integrity for Digital Video Based on The Watermarking Techniques.

Google Drive Link:
https://drive.google.com/drive/folders/1Jq6IfUdo8eK8hkHDPezwujeg9IT4xuq4?usp=sharing

Github Link:
https://github.com/yvjawahar/Protection-of-image-in-social-media