



INTELLIGENT SYSTEM FOR DETECTION OF COPYRIGHT-PROTECTED DATA FOR ENHANCED DATA SECURITY

Ndueso Udoetor¹, Godwin Ansa², Anietie Ekong³, and Anthony Edet⁴

¹Department of Computer Science, Akwa Ibom State University, Mkpato Enin, Nigeria.

Email: Udoetorndueso55@gmail.com

²Department of Computer Science, Akwa Ibom State University, Mkpato Enin, Nigeria.

Email: godwinansa@aksu.edu.ng

³Department of Computer Science, Akwa Ibom State University, Mkpato Enin, Nigeria.

Email: anietieekong@aksu.edu.ng

⁴Department of Computer Science, Akwa Ibom State University, Mkpato Enin, Nigeria.

Email: anthonyedet73@gmail.com

Cite this article:

Udoetor, N., Ansa, G., Ekong, A., Edet, A. (2024), Intelligent System for Detection of Copyright-Protected Data for Enhanced Data Security. British Journal of Computer, Networking and Information Technology 7(4), 58-80. DOI: 10.52589/BJCNIT-OQQNPPCJ

Manuscript History

Received: 11 Aug 2024

Accepted: 6 Oct 2024

Published: 17 Oct 2024

Copyright © 2024 The Author(s). This is an Open Access article distributed under the terms of Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0), which permits anyone to share, use, reproduce and redistribute in any medium, provided the original author and source are credited.

ABSTRACT: *In the digital era, the proliferation of digital content has intensified concerns over intellectual property rights infringement, highlighting the need for robust copyright protection solutions. This paper presents a software solution designed to address these challenges by combining advanced algorithms with intuitive user interfaces for effective copyright enforcement. Central to the software's functionality is the Most Significant Bit (MSB) embedding technique, which allows users to imperceptibly embed copyright or trademark information into digital images. This method modifies the MSB of pixel values to encode protection data while maintaining the visual integrity of the images. In the detection phase, the software employs Deep Convolutional Neural Networks (DCNN) to identify instances of unauthorized use or copyright infringement. By analyzing submitted images, the DCNNs use sophisticated pattern recognition algorithms to detect embedded copyright information or trademarks, promptly flagging infringements for further action. The software ensures a seamless user experience with an intuitive interface that guides users through image upload, copyright embedding, and infringement detection processes. This comprehensive approach provides a powerful tool for safeguarding intellectual property rights in the digital landscape, offering users an efficient means to protect and enforce copyright effectively.*

KEYWORDS: DCNN, MSB, Copyright, Data Security.



INTRODUCTION

In the digital age, the exponential growth of unstructured digital data has presented unprecedented challenges for protecting intellectual property and preventing copyright infringement (Basma et al., 2020). As individuals and organizations increasingly rely on digital platforms to create, share, and store diverse forms of content, the need for robust mechanisms to safeguard copyrights has become paramount. This research focuses on developing advanced techniques for the protection and detection of copyrights in unstructured digital data, aiming to enhance overall data security using a combined effort of Most Significant Bit (MSB) and Deep learning approaches. Traditional methods of copyright protection often fall short when applied to unstructured data, which includes images, videos, and textual content with varying formats and structures. The advent of deep learning, particularly Deep Convolutional Neural Networks (DCNN), offers a promising avenue for addressing these challenges. DCNNs have demonstrated remarkable capabilities in feature extraction and pattern recognition, making them well-suited for analyzing complex and diverse data types. By using the power of DCNNs, this research seeks to devise a sophisticated copyright protection system capable of identifying and validating copyrighted material across a wide range of digital formats. Deep learning is particularly effective in handling large datasets and is well-suited for scenarios involving multiple classes of data, making it a valuable addition to the proposed framework (Yingqian et al., 2023). Through the integration of DCNN and Most Significant Bit (MSB) technique, the research aims to create a comprehensive solution that not only enhances copyright protection but also contributes to the broader field of data security in the digital world (Li et al., 2017). The implications of successful implementation of the proposed copyright protection system extend beyond individual content creators and copyright holders. The safeguarding of intellectual property in unstructured digital data is crucial for fostering innovation, creativity, and fair compensation for content producers (Ansa et al., 2012). Additionally, as the digital space continues to evolve, the research outcomes are expected to contribute significantly to the ongoing discourse surrounding data security and the responsible use of digital content. Ultimately, the development of effective and efficient copyright protection mechanisms is essential for creating a sustainable and secure environment for the digital exchange of ideas and information (Hoyle et al., 2020). Copyright serves as the legal foundation for protecting the intellectual property rights of content creators, granting them exclusive rights to reproduce, distribute, and display their work. In unstructured digital data, which encompasses a vast array of multimedia content and text, enforcing copyright becomes increasingly complex due to the sheer volume and diverse nature of digital materials (Shen et al., 2019). Copyright infringement in this context involves unauthorized use, reproduction, or distribution of copyrighted content, posing a significant threat to the livelihoods of creators and the integrity of their work. As technology advances, so do the methods employed by infringers, necessitating innovative approaches to copyright protection that can adapt to the intricacies of unstructured digital data (Ekong et al., 2022). The proliferation of digital content and the ease of sharing information across online platforms have heightened concerns about data security in the context of copyright protection. Unauthorized access to copyrighted materials not only infringes on the rights of content creators but also poses risks to the confidentiality and integrity of sensitive information. The research at hand recognizes the intricate connection between copyright protection and data security, striving to develop a robust system that not only identifies and prevents copyright infringement but also fortifies the overall security of digital assets. By addressing these intertwined challenges, the research aims to contribute to the establishment of



a digital environment where creators can confidently share and disseminate their work without compromising the security of their intellectual property. In the era of big data, the sheer volume and diversity of unstructured digital data make traditional copyright enforcement methods inadequate. As copyright infringement increasingly occurs on a global scale through online platforms and peer-to-peer networks, the need for sophisticated technologies to detect and prevent such activities becomes imperative. The proposed use of Deep Convolutional Neural Networks and Most Significant Bit (MSB) signify a departure from conventional approaches, offering a more nuanced and adaptive solution to the multifaceted problem of copyright protection in unstructured digital data. By exploring the intersection of copyright, copyright infringement, and data security, this research endeavors to provide a comprehensive framework that not only safeguards the rights of content creators but also contributes to the broader discourse on responsible digital content dissemination and the protection of intellectual property in the digital age.

Research Problem

The escalating volume of unstructured digital data in contemporary society has given rise to a pressing problem concerning the protection of copyrights and the prevention of infringement. Traditional methods of copyright enforcement prove inadequate in the face of diverse multimedia content, such as images, videos, and text, which often lack a standardized structure. As a result, there is an urgent need for advanced technological solutions that can navigate the complexities of unstructured digital data to identify and mitigate copyright infringement effectively. This research addresses the overarching problem of safeguarding intellectual property in an era where the boundaries between legal and illegal digital content usage are becoming increasingly blurred. The challenge extends beyond the sheer scale of unstructured digital data; it encompasses the dynamic nature of copyright infringement mechanisms in the digital space. Rapid advancements in technology have enabled infringers to employ sophisticated techniques, necessitating a constant evolution in copyright protection methods. The statement of the problem recognizes the critical gap in existing approaches and emphasizes the urgency of developing a comprehensive solution that integrates Deep Convolutional Neural Networks and Steganograph techniques. The Most Significant Bit (MSB) technique will be used to protect the data, while deep learning does detection of the protected digital data.

LITERATURE/THEORETICAL UNDERPINNING

This section outlines the theoretical foundation of the research, providing a clear understanding of the underlying principles and concepts that support the study. It establishes the basis for the research framework by discussing key theories, models, and prior studies relevant to the topic, thereby contextualizing the research objectives and methodology. This theoretical groundwork enables a comprehensive grasp of how the research is built upon established knowledge and contributes to the existing body of literature.

Copyright Protection in Digital Data

Copyright protection in the area of digital data is an increasingly critical concern in the wake of the digital revolution (Edet, et al., 2024). As the creation, distribution, and consumption of content transition to online platforms, safeguarding intellectual property has become



paramount. Copyright protection in digital data refers to the legal and technological measures implemented to ensure that creators' rights are respected and that unauthorized use or reproduction of digital content is prevented. This encompasses a wide range of digital assets, including text, images, audio, video, and software code, among others (Ekong et al., 2024). Historically, copyright laws have been established to protect creators by granting exclusive rights to reproduce, distribute, and display their work. However, the advent of the digital era has posed new challenges as the ease of copying and disseminating digital content has surged. In response, legal frameworks have evolved, adapting to the nuances of the online environment. Digital rights management (DRM) technologies have been developed to enforce copyright protection by restricting access to or usage of digital content through encryption, access controls, and other mechanisms. These measures aim to strike a balance between the rights of content creators and the public's need for access to information. Despite these advancements, copyright protection in digital data faces ongoing challenges (Edet et al., 2024). The borderless nature of the internet, coupled with the ease of replication and distribution, makes it challenging to enforce copyright laws globally. Additionally, emerging technologies such as artificial intelligence and deep learning introduce new complexities, requiring continuous adaptation of legal and technological frameworks. The ongoing discourse around copyright protection in digital data underscores the need for a dynamic and collaborative approach involving legal, technological, and ethical considerations to ensure the sustainable protection of intellectual property in the digital age. In the digital space, copyright protection plays a crucial role in fostering creativity and innovation by providing content creators with the assurance that their intellectual property will be acknowledged and fairly compensated (Ebong et al., 2024). Digital data, which encompasses a vast array of creative works, faces unique challenges due to its intangible and easily replicable nature. The ubiquity of online platforms, social media, and file-sharing services has amplified concerns about unauthorized use, piracy, and the potential dilution of creators' rights. Copyright protection in digital data involves not only legal mechanisms but also technological solutions that can adapt to the rapidly evolving digital environment (Ekong et al., 2024). Digital copyright protection involves the establishment of clear legal frameworks and international agreements that govern the rights and responsibilities of content creators, distributors, and consumers. These legal measures aim to strike a balance between protecting creators' rights and fostering the free exchange of ideas and information. The Digital Millennium Copyright Act (DMCA) in the United States and similar legislations worldwide exemplify attempts to adapt copyright laws to the digital era. Additionally, international organizations like the World Intellectual Property Organization (WIPO) work towards establishing standardized copyright protection measures on a global scale. Technologically, copyright protection employs a variety of methods to safeguard digital data (Uwah & Edet, 2024). Digital watermarks, encryption, and access controls are employed to embed ownership information and restrict unauthorized access or distribution. Digital Rights Management (DRM) systems, although contentious, are widely used to manage access to digital content. However, the effectiveness of these technologies is often debated, with concerns about their impact on user privacy and the potential for stifling legitimate usage. As the digital space continues to evolve, copyright protection in digital data remains a dynamic field that requires ongoing adaptation. Emerging technologies, such as blockchain, are being explored to create decentralized and tamper-proof systems for tracking and managing digital rights (Edet & Ansa, 2023). The conversation around copyright protection in digital data extends beyond legal and technological aspects, involving discussions on ethical considerations, fair use, and the balance between protecting creators' rights and ensuring access



to information for the broader public. In navigating these complexities, it is essential to foster a collaborative and multidisciplinary approach that addresses the challenges and opportunities presented by the digital age.

Related Literature

Shabou et al., 2020, proposed a work on Algorithmic methods to explore the automation of the appraisal of structured and unstructured digital data. They conducted an interdisciplinary and innovative research project in Switzerland at the Geneva School of Business Administration HES-SO, in collaboration with the State Archives of Neuchâtel (Office des archives de l'État de Neuchâtel, OAEN). The primary objective of the study was to address the classical challenge of extracting and discriminating relevant data from a vast and diverse range of data record formats and contents. The focus was on providing a framework and proof of concept for a software tool aimed at assisting in defensible decision-making regarding the retention and disposal of records and data at OAEN. The research was structured around two axes: the archival axis, which involved proposing archival metrics for the appraisal of structured and unstructured data, and the data mining axis, which aimed to provide algorithmic methods as complementary or additional metrics for the appraisal process.

In terms of methodology, the exploratory study designed and tested the feasibility of archival metrics paired with data mining metrics to advance the digital appraisal process systematically or even automatically. Under Axis 1, the authors undertook three key steps: conceptual framework design for records data appraisal with a detailed three-dimensional approach (trustworthiness, exploitability, representativeness); operationalization of proposed metrics in terms of variables supported by quantitative methods for measurement and scoring; and validation of the conceptual framework and metrics through feedback from experienced professionals. This process aimed to assess the relevance and feasibility of the proposed metrics, demonstrating their acceptability in real-life archival practice. Parallely, Axis 2 proposed functionalities covering both macro analysis for data and algorithmic methods to enable the computation of digital archival and data mining. The study thus represents a comprehensive and practical approach to enhancing the digital appraisal process for archival and data management purposes.

Haonan et al., 2023 proposed a work on Copyright Protection and Accountability of Generative AI: Attack, Watermarking and Attribution. This paper focuses on addressing the escalating concerns surrounding the protection of Intellectual Property Rights (IPR) in the context of Generative AI, particularly Generative Adversarial Networks (GANs). With the increasing popularity of Generative AI, the paper highlights the potential risks related to IPR, specifically in relation to images (toxic images) and models (poisoned models) generated by GANs. The authors propose an evaluation framework to comprehensively assess the current state of copyright protection measures for GANs. The evaluation encompasses a diverse range of GAN architectures and aims to identify factors influencing performance as well as suggest future research directions. The findings suggest that existing IPR protection methods for input images, model watermarking, and attribution networks are generally effective for a broad spectrum of GANs. However, the paper emphasizes the need for increased attention to protecting training sets, noting that current approaches lack robust IPR protection and provenance tracing for training data. Overall, the research provides valuable insights into the current state of copyright



protection in the realm of Generative AI, offering directions for improvement and emphasizing the importance of addressing potential vulnerabilities in training sets.

Cui et al., 2023, proposed a work on diffusion shield: a watermark for data copyright protection against generative diffusion models. The research presented in this work focuses on addressing copyright protection concerns arising from the prolific use of Generative Diffusion Models (GDMs) in generating images. As GDMs gain popularity for their remarkable image generation capabilities, concerns have emerged regarding the unauthorized replication of creative works by artists, such as painters and photographers. In response to these challenges, the authors introduce a novel watermarking scheme called Diffusion Shield. This scheme aims to protect images from copyright infringement by encoding ownership information into an imperceptible watermark, which is then injected into the images. The watermark is designed to be easily learned by GDMs and replicated in their generated images. The proposed method, Diffusion Shield, utilizes uniform watermarks and a joint optimization approach to ensure low distortion of the original image, high watermark detection performance, and the capacity to embed lengthy messages. Rigorous and comprehensive experiments are conducted to demonstrate the effectiveness of Diffusion Shield in defending against copyright infringement by GDMs, establishing its superiority over traditional watermarking methods. Overall, the research provides a practical solution to safeguarding intellectual property in the face of the evolving capabilities of Generative Diffusion Models.

Liu et al. (2020) concluded several privacy issues of online image sharing. In this paper, the authors focused on the unawareness of privacy during image sharing. There are two main types of methods to deal with the risk of unawareness of privacy. The first type of method mainly adopts classification models to identify private images

Zerr, Siersdorfer, and Hare (2012) proposed a privacy-aware classifier based on vi

sual features like face and color histograms. Buschek et al. (2015) proposed a multi-modal method that assigns privacy labels to the images based on visual features and metadata like location and publication time. Tonge, Caragea, and Squicciarini (2018) utilized another kind of metadata, tag, and Tonge and Caragea (2019) further derived features of the object, scene, and tags for privacy-leaking image detection. Yang et al. (2020) extracted a knowledge graph from the images and identified private images based on object detection and graph neural networks.

The second type of method focuses on sensitive regions in the images, including approaches like object detection and semantic segmentation. Some detected private

attributes such as faces (Sun, Wu, and Hoi 2018), license plates (Zhou et al. 2012), and social relationship (Li et al. 2017a). Orekondy, Schiele, and Fritz (2017) defined a list of privacy attributes and detected them simultaneously. Some works attempted to protect privacy-leaking image based on blurring (Fan 2018), blocking (Li et al. 2017b), cartooning (Hasan et al. 2017), and perturbation (Oh, Fritz, and Schiele 2017). Shetty, Fritz, and Schiele (2018) removed private objects from the images based on a generative method. However, a person may be recognized even his face is not visible (Oh et al. 2016), and the redacted image may be recovered (Shen et al. 2019). As the usage of shared images is almost uncontrollable, it is better to prevent the risk from the beginning. Therefore, we follow the first type of method to solve the issue of privacy-leaking images by classification.



In exploring Machine Learning capabilities in prediction problems, (Odikwa, Ekong & Okpako, 2021) demonstrated the use of Fuzzy Logic in the design of Chat-bot Messenger for Home Intelligent System with Multiple Sensors. Also, (Ekong, James and & Edet, 2022) proposed a work on Supervised Machine Learning Model For Effective classification Of Patients With Covid-19 Symptoms-based On Bayesian Belief Network with a focus on the identification of patients with Covid-19 symptoms. Ekong et al., 2023, used machine learning algorithm, particularly, the Random Forest algorithm to address a cybersecurity problem. In another research, Ekong et al., 2023, proposed a work on Machine Learning based Model for the Prediction of Fasting Blood Sugar Level towards Cardiovascular Disease Control for the Enhancement of Public Health. In the research, Logistic Model was adopted for the prediction of fasting blood sugar level which enabled the control of Cardiovascular diseases which in turn enhanced public health. (Inyang & Umoren, 2023) proposed a work using NLP. This research employs a Framework-Based Method (FBM) to classify infectious diseases based on ecological risk factors, providing a structured and reproducible approach. Various machine learning models are utilized, including XGBoost, Random Forest (RF), Support Vector Machine (SVM), Artificial Neural Network (ANN), Linear Discriminant Analysis (LDA), Gradient Boosting Machine (GBM), k-Nearest Neighbors (KNN), and Decision Tree (DT). The results indicate varying levels of accuracy and Kappa statistics for each model. The study reveals the performance metrics for each model, with XGBoost and LDA achieving relatively high accuracy and Kappa values. Additionally, a Deep Learning model, BERT, is integrated with XGBoost to create an interactive interface for users, enhancing the practical application of machine learning and Natural Language Processing (NLP) in ecological disease classification. The research emphasizes the importance of considering ecological risk factors in infectious disease classification and explores the potential of machine learning techniques for this purpose. Ekong et al., 2023, proposed a work on Machine Learning Approach for Classification of Sickle Cell Anemia in Teenagers Based on Bayesian Network. In this study, a Bayesian network approach was employed for the classification of sickle cell anemia in teenagers based on diverse medical data. The research utilized probabilistic graphical models to represent relationships among various medical parameters, incorporating Bayesian principles for adaptive predictions. The Bayesian network demonstrated exceptional accuracy (99%) in classifying teenagers as either positive or negative for sickle cell anemia. Key features contributing to the classification were identified, offering valuable insights for early detection and intervention. The findings highlight the diagnostic significance of sickle cell anemia classification in teenagers, contributing to medical informatics and computational biology. The Bayesian network proves to be a reliable decision support system for clinicians, aiding in informed decisions and timely interventions. (Edet and Ansa, 2023), in this research, the authors proposed a Machine Learning Enabled System for Intelligent Classification of Host-based Intrusion Severity to effectively manage intrusion events, particularly those initiated by internal workers. The model comprises three phases: detecting intrusion severity, conducting source analysis, and providing security recommendations using counterfactual reasoning. The dataset was gathered from user interactions over time, captured in an activity log. Bayesian Network achieved an 82% accuracy in the intrusion severity classification. The system includes an API for scalability, aiming to assist IT firms in analyzing and managing the impact of intrusions effectively.

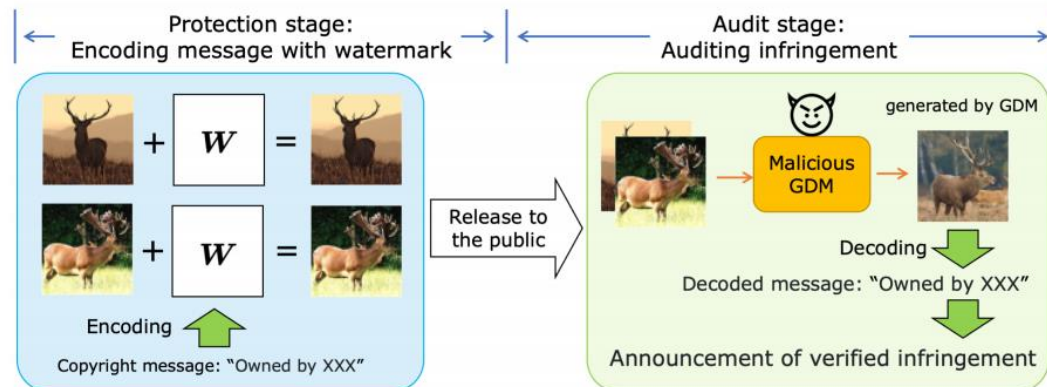


Fig. 1: Architecture of the Existing System (Yingqian et al., 2023)

Yingqian et al. in 2023, proposed a work on diffusion shield: a watermark for data copyright protection against generative diffusion models. The research presented in this work focuses on addressing copyright protection concerns arising from the prolific use of Generative Diffusion Models (GDMs) in generating images. As GDMs gain popularity for their remarkable image generation capabilities, concerns have emerged regarding the unauthorized replication of creative works by artists, such as painters and photographers. In response to these challenges, the authors introduce a novel watermarking scheme called Diffusion Shield. This scheme aims to protect images from copyright infringement by encoding ownership information into an imperceptible watermark, which is then injected into the images. The watermark is designed to be easily learned by GDMs and replicated in their generated images. The proposed method, Diffusion Shield, utilizes uniform watermarks and a joint optimization approach to ensure low distortion of the original image, high watermark detection performance, and the capacity to embed lengthy messages. Rigorous and comprehensive experiments are conducted to demonstrate the effectiveness of Diffusion Shield in defending against copyright infringement by GDMs, establishing its superiority over traditional watermarking methods. Overall, the research provides a practical solution to safeguarding intellectual property in the face of the evolving capabilities of Generative Diffusion Models. In the existing system, **Image + W = Copyrighted Image**. The initial phase of the system involves a crucial computation, taking place within its first segment. The underlying computational principle employed in this module is known as the Watermarking principle. This methodology, however, exhibits certain drawbacks, particularly in comparison to the more advanced machine learning approaches widely used in the field of data and information security. The Watermarking principle, although historically employed in the realm of security, is considered less reliable in the contemporary technological space. This is attributed to a number of weaknesses inherent in watermarking as an approach to enhancing security systems. Given the rapid evolution of tools designed for breaching security systems, relying solely on watermarking is no longer deemed sufficient for constructing robust security frameworks in today's technology-driven environment. The prevailing recommendation in the development of security systems is the incorporation of multiple algorithms or the adoption of a single, but exceptionally robust, algorithm. This

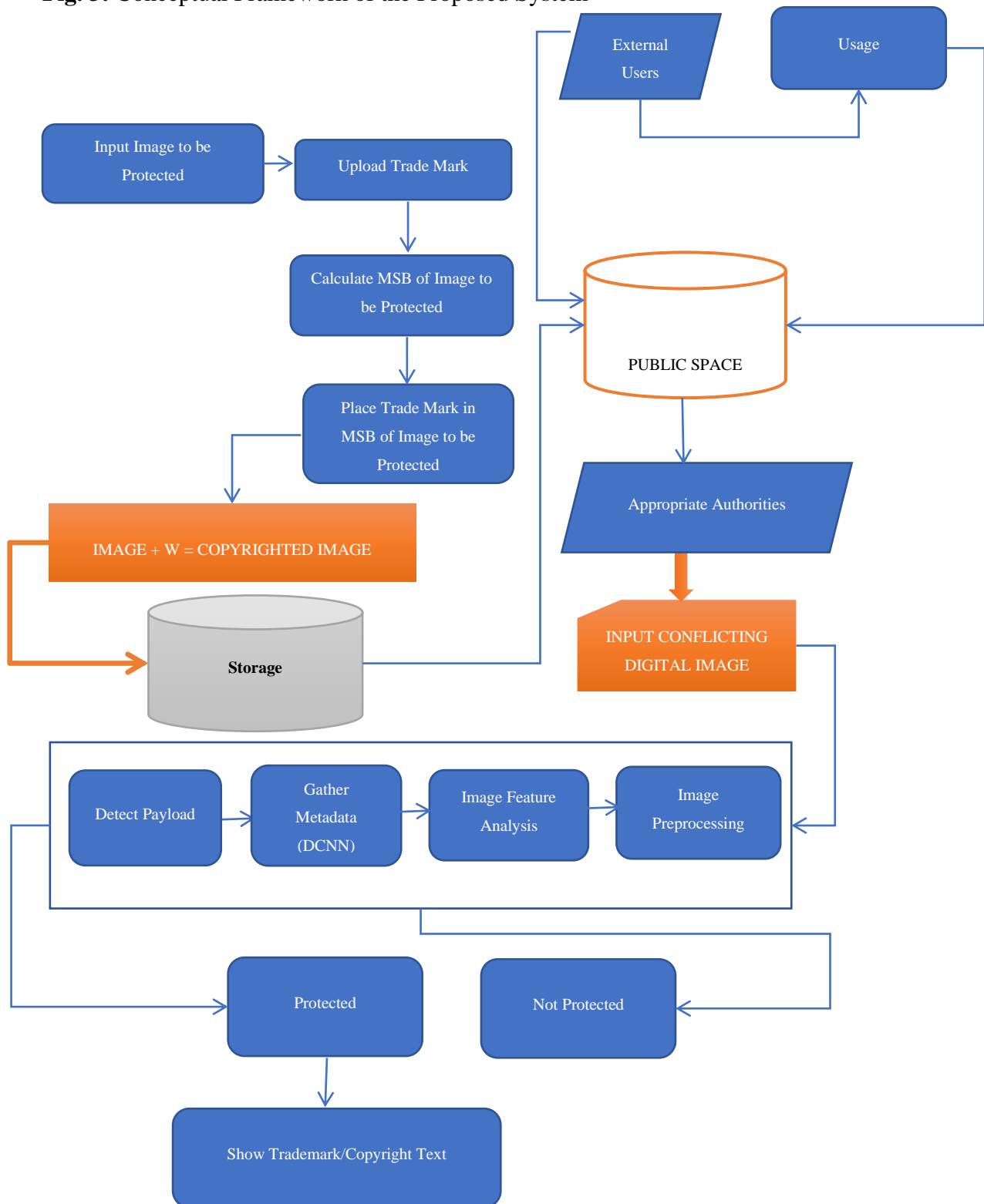


strategic combination enhances the overall resilience and effectiveness of the security system. In contrast, the existing system relies solely on the Watermarking principle, exposing it to potential vulnerabilities. For the system to remain viable and secure in today's dynamic technology space, a substantial improvement is imperative. The enhancement should involve the integration of advanced algorithms, capable of withstanding the sophisticated tools and techniques employed by malicious actors in attempting to compromise security systems. By embracing a more comprehensive and sophisticated approach, the system can better adapt to the evolving landscape of technological threats and ensure its functionality and reliability in safeguarding sensitive data and information.

Weaknesses of the Existing System

1. Watermarking (Diffusion shield) approach is not robust for copyrighting and protection of digital images as it relies on obfuscating or altering the image at the pixel level to protect it.
2. The security level of the existing system is weak and the file is vulnerable or susceptible to reverse engineering.
3. The process of embedding protective data or watermarks can degrade the quality of the original image, which might be unacceptable in high-quality or professional applications.
4. Diffusion shield techniques can introduce distortions or artifacts into the image, potentially affecting its quality or usability. This could be a concern in scenarios where image fidelity is important.

Fig. 3: Conceptual Framework of the Proposed System



This research focuses on digital image files and the potential risks associated with sharing unprotected images on the internet. The act of creating and disseminating images without implementing means of identification not visible to the human eye can jeopardize the rights to those images. Without proper protection, individuals may lose control over their images, emphasizing the need for robust security measures in the digital space. Building upon the work of Yingqian et al. in 2023, this study represents an advancement in image copyright protection and detection. While the previous work utilized a watermarking approach, a critical review of existing literature highlights the limitations of watermarking in providing the necessary security infrastructure for creators and organizations to implement copyright, safeguard, identify, or detect their digital images on the internet. Consequently, this research aims to extend and enhance the existing methodology

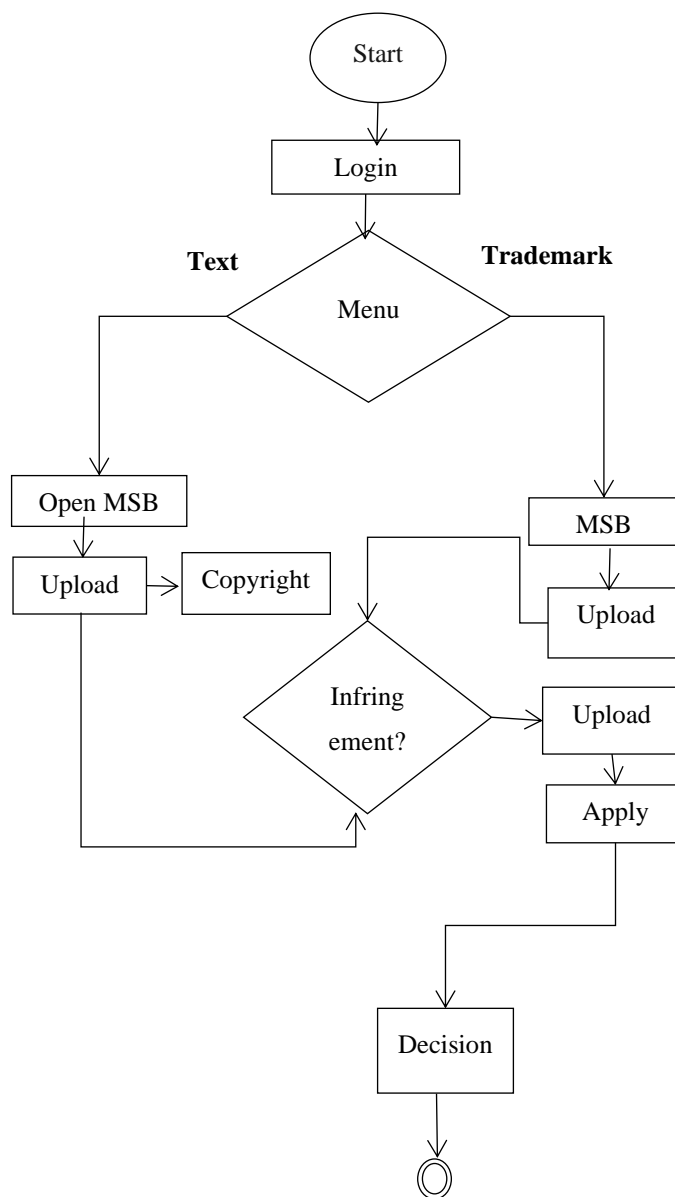


Fig. 2: Flowchart of the Conceptual System



In this new approach, Deep Learning and Most Significant Bit (MSB) are employed to fortify digital information by embedding copyright details. This ensures that the original owner can assert their rights to the image without encountering conflicts. The main system comprises three distinct modules: the copyright protection module handled by Most Significant Bit (MSB), copyright detection module handled by machine learning, and file summary module to further help in the analysis of the image. The file summary module serves as a pivotal point displaying digital image metadata upon uploading to the main system.

METHODOLOGY

In the proposed system, the Deep Convolutional Neural Network (DCNN) plays a pivotal role in the development of the copyright protection and detection system. DCNN, renowned for its effectiveness in image processing and recognition tasks, is harnessed to enhance the system's capabilities in safeguarding digital images (Ekong et al., 2023). Through its sophisticated architecture, DCNN is adept at learning hierarchical spatial features from input data, making it a valuable tool for tasks related to image identification and protection. This approach ensures that the system benefits from the strengths of DCNN, leveraging it for image-related tasks and for effective copyrighted image classification. The integration of deep learning enhances the system's capacity to detect and protect copyrighted material, thereby providing a well-rounded solution for digital content security. Most Significant Bit (MSB) is a data security technique that hides one data in another data allowing it to be hidden from the eyes and perception of the general public.

1. Deep Convolutional Neural Networks (DCNN)

Deep Convolutional Neural Networks (DCNNs) are a type of artificial neural network designed for tasks involving visual data, such as image recognition and computer vision. The mathematical representation of a DCNN involves several components, including convolutional layers, pooling layers, fully connected layers, and activation functions. Below is a basic outline of the mathematical operations commonly used in a DCNN:

1. Convolutional Operation:

Input Volume: (I) (Image or Feature Map)

Convolutional Filter (Kernel): (K)

Convolution Operation (with Stride (S)):

$$[(I * K)_{i,j}] = \sum_m \sum_n I_{(i \cdot S + m), (j \cdot S + n)} K_{m,n}$$

Output Feature Map: (O)

$$[O_{i,j}] = (\sum_m \sum_n I_{(i \cdot S + m), (j \cdot S + n)} K_{m,n} + b)$$

where (f) is an activation function (e.g., ReLU), and (b) is the bias term.



2. Pooling Operation:

Max Pooling:

$$[\{ \text{MaxPooling} \} (I)_{i,j} = \max_{\{m,n\}} I_{\{i \cdot S + m, j \cdot S + n\}}]$$

Average Pooling:

$$[\{ \text{AvgPooling} \} (I)_{i,j} = \{ 1 \} / \{ m \cdot n \} \sum_{\{m,n\}} I_{\{i \cdot S + m, j \cdot S + n\}}]$$

3. Fully Connected Layer:

Input Vector: (X) (flattened output from previous layers)

Weight Matrix: (W)

Bias Vector: (b)

Output Vector: (Y)

$$[Y = f(WX + b)]$$

4. Activation Function:

Commonly used activation functions include ReLU (Rectified Linear Unit):

$$[\{ \text{ReLU} \} (x) = \max(0, x)]$$

and Sigmoid:

$$[\{ \text{Sigmoid} \} (x) = \{ 1 \} / \{ 1 + e^{-x} \}] \text{ (Ekong et al., 2022) }$$

These mathematical operations are applied across the layers of a DCNN to progressively learn hierarchical features from the input data (Edet et al., 2024). The network is trained using backpropagation and optimization algorithms to minimize a defined loss function, ensuring that the network's output aligns with the ground truth labels for the training data.

2. MSB Algorithm

The Most Significant Bit (MSB) algorithm is a straightforward technique used for data embedding in digital images. Below is a simple algorithm outlining the steps involved in the MSB embedding process:

Input:

- Original digital image (represented as a matrix of pixel values)
- Copyright or trademark information to be embedded (binary data)

Output:

- Payload digital image



Steps:

1. Convert Copyright Information to Binary:

Convert the copyright or trademark information into binary format. Each character in the copyright information is represented by its corresponding binary value using ASCII or Unicode encoding.

2. Iterate Through Image Pixels:

Iterate through each pixel in the digital image, row by row and column by column.

3. Embed Copyright Information:

For each pixel, retrieve the grayscale value or color channels (e.g., RGB values). Since the MSB is the highest-order bit, it has the least effect on the pixel's intensity or color perception. Therefore, overwrite the MSB of each pixel's binary representation with the bits of the copyright information. Repeat this process for each bit of the copyright information until all bits are embedded.

4. Update Pixel Values:

Update the pixel values in the image matrix with the modified binary representations containing the embedded copyright information.

5. Output Payload Image:

The resulting image now contains the embedded copyright or trademark information in its MSB. This image is the output of the MSB embedding algorithm.

3. Strength of MSB and DCNN over the Existing Approach

In this section, we state five potential advantages of using the MSB and DCNN methods over traditional watermarking techniques for copyright protection in digital images, intellectual property, trademarks, etc.:

1. Higher Capacity for Data Embedding:

The MSB and DCNN methods can embed more information compared to traditional watermarking techniques that often use the least significant bits (LSBs). By leveraging the most significant bits and DCNN, the methods allows for embedding and checking a larger amount of data without significantly affecting the image quality.

2. Enhanced Robustness:

The MSB and DCNN methods are generally more robust against various types of attacks, such as compression, noise addition, and other common image processing operations. Since data is embedded in the more critical parts of the data, it is less likely to be destroyed by such operations.

3. Improved Security:

By embedding data in the most significant bits, the MSB method can offer enhanced security against unauthorized removal or tampering. Modifying or removing the embedded data without noticeably altering the image quality can be more challenging for attackers.

4. Better Visual Quality:

The MSB method can maintain better visual quality, especially when the data is spread over multiple MSBs in a controlled manner. This can result in less noticeable changes compared to some traditional watermarking methods that may introduce visible distortions.

5. Easier Detection and Verification:

Data embedded using the MSB method can be more easily detected and verified, as it is less susceptible to loss or degradation during common image processing. This simplifies the process of verifying copyright and ownership, making it faster and more reliable.

RESULTS/FINDINGS

In this section, the output of the system is presented. Below are the output of the copyright protection and detection system.



Fig. 3: Application Loading Screen

As the application initiates, it undergoes a meticulous loading process, systematically gathering essential files and resources vital for its seamless operation. Beginning from index 0 and progressing sequentially to 100, each file is meticulously retrieved and integrated into the application's runtime environment. This loading phase ensures that all requisite components, including libraries, configuration files, and data sets, are efficiently accessed and initialized, laying a robust foundation for the subsequent execution of the application's functionalities. During the loading sequence, the application meticulously verifies the integrity and completeness of each file, performing validation checks to ascertain their authenticity and

compatibility with the runtime environment. This rigorous validation process helps mitigate potential errors or inconsistencies that may arise during runtime, fostering stability and reliability in the application's execution. Additionally, the loading phase serves as a critical preparatory stage, setting the stage for the application to deliver optimal performance and functionality while adhering to established quality standards and best practices.



Fig. 5: Login Screen

The login screen serves as the gateway to the application's functionalities, ensuring secure access through robust authentication mechanisms. Upon accessing the login screen, users are prompted to input their credentials, including a username and password. The system meticulously validates these credentials against predefined criteria, verifying the correctness of the provided username and password combination. Only upon successful validation of the credentials does the login screen grant access to authorized users, enabling them to proceed to utilize the application's features and functionalities, while maintaining the integrity and confidentiality of the system.

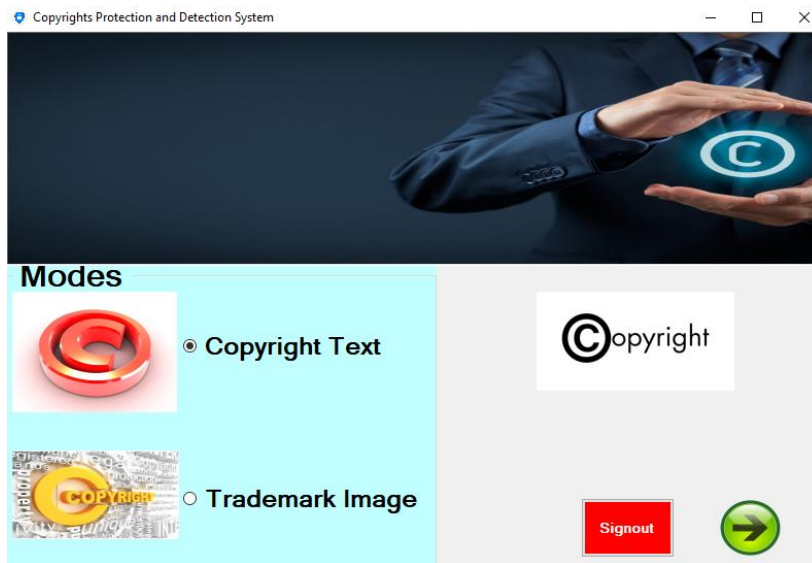


Fig. 6: Menu Screen

The menu screen presents users with a pivotal choice, offering two distinct options to tailor their interaction with the application's functionalities. Users are empowered to select between protecting and detecting digital images embedded with textual copyright information or those embedded with trademark images. This clear and intuitive interface design provides users with flexibility, allowing them to align their actions with their specific copyright protection and detection needs. Whether opting to safeguard textual content or visual trademarks, users can seamlessly navigate through the application's features, ensuring comprehensive protection and detection of their digital assets. By offering these distinct pathways, the menu screen enhances user engagement and efficiency, enabling users to make informed decisions that align with their copyright management objectives.

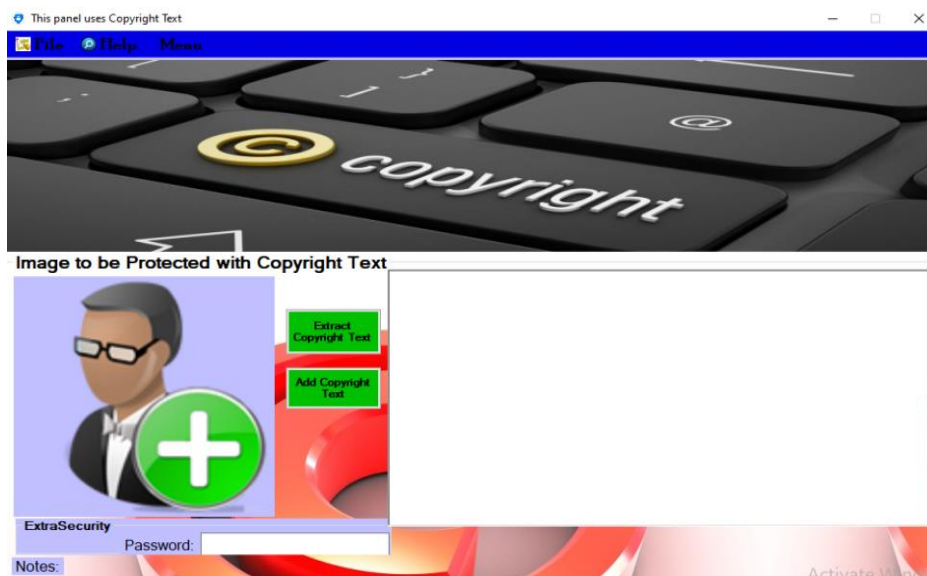


Fig. 7: Screen for Protection of Digital Data with Copyright Text Information

The screen dedicated to the protection of digital data with copyright text information provides users with a streamlined interface tailored for seamless integration of copyright information into their digital assets. Upon accessing this screen, users are prompted to upload the image they intend to safeguard, facilitating a straightforward process for embedding copyright text for enhanced protection. Additionally, users are prompted to input a password, bolstering security measures to ensure authorized access to the embedding process. Once the image and password are provided, the MSB algorithm seamlessly embeds the copyright text into the digital image, leveraging imperceptible alterations to preserve visual integrity. Following the embedding process, the image is securely saved as a payload carrying the copyright information, effectively encapsulating the copyright text within the image's metadata. This encapsulation ensures that the copyright information remains seamlessly integrated with the image, serving as a robust identifier in the event of conflict or infringement. By equipping digital assets with embedded copyright text, users fortify their ability to assert ownership and defend against unauthorized usage or reproduction. The interface's user-centric design prioritizes simplicity and efficacy, empowering users to safeguard their intellectual property with confidence and ease.

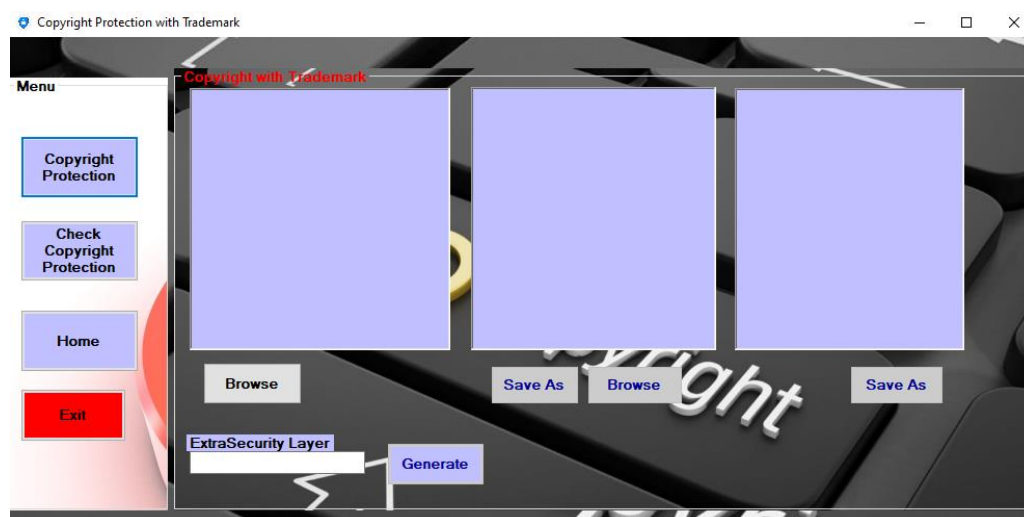


Fig. 8: Protection of Digital Data with Trademark Information

The protection of digital data with trademark information follows a meticulous process, blending the efficiency of the Most Significant Bit (MSB) method with the advanced capabilities of Deep Convolutional Neural Networks (DCNN) for detection. Users engaging in this protection process are guided through an interface optimized for seamless integration of trademark information into their digital assets. With an intuitive design, users are prompted to upload the image intended for protection, initiating a process where the MSB algorithm delicately embeds the trademark information into the image's binary data. This embedding process is conducted with precision, ensuring that the trademark remains discreetly integrated while maintaining the image's visual fidelity. Upon completion of the embedding process, the image is fortified with trademark information, serving as a distinct identifier for the protected asset. During the subsequent detection phase, powered by DCNN, the system rigorously scans digital content to identify instances of trademark infringement or unauthorized usage. Leveraging the robust pattern recognition capabilities of DCNN, the system efficiently identifies trademarked elements within digital assets, providing users with invaluable insights

into potential copyright violations. By integrating the MSB embedding method with DCNN-based detection, users can effectively safeguard their digital assets, preemptively detecting and addressing instances of trademark infringement with precision and confidence. This harmonious fusion of algorithms empowers users to assert ownership rights over their intellectual property in the digital landscape, ensuring comprehensive protection and enforcement capabilities.

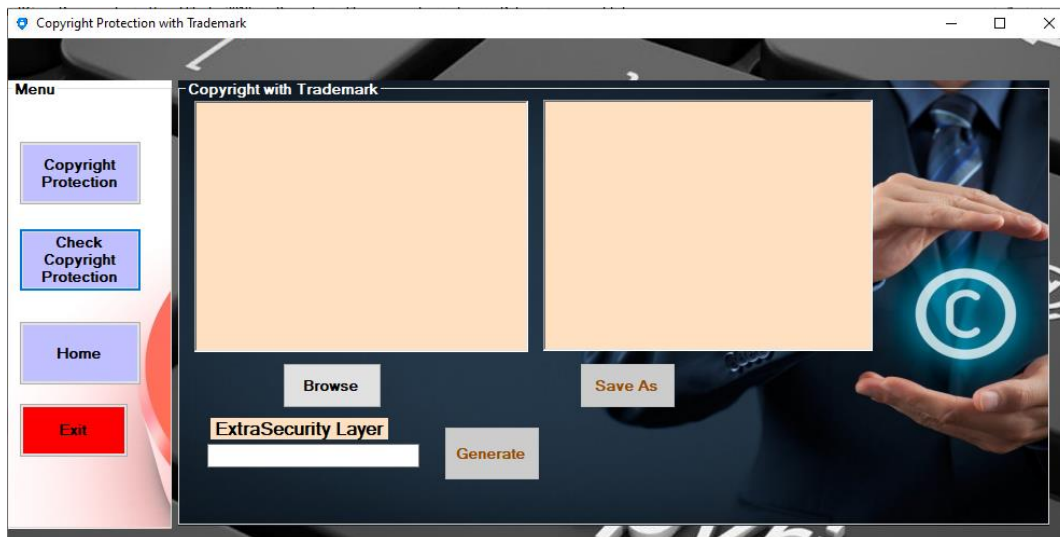


Fig. 9: Detection of Copyright infringement using DCNN

The Detection of Copyright Infringement using Deep Convolutional Neural Networks (DCNN) screen provides users with a swift and reliable means to ascertain the copyright status of digital images, enabling proactive identification of potential infringement or conflicts. Through an intuitive interface, users can effortlessly upload images for analysis, leveraging the powerful capabilities of DCNN for copyright detection. Upon submission, the system rigorously analyzes the uploaded images, employing sophisticated pattern recognition algorithms to identify copyrighted elements or trademarks embedded within the digital content. This comprehensive analysis enables users to swiftly determine the copyright status of images, empowering them to take appropriate action in cases of infringement or conflict. With its user-friendly design and efficient processing capabilities, the DCNN-based detection screen serves as a valuable tool for safeguarding intellectual property rights in the digital domain, facilitating proactive enforcement and protection measures with ease.



Name	Date modified	Type	Size
Form1.Designer.cs	5/9/2024 1:23 PM	C# Source File	27 KB
Form1.resx	5/9/2024 1:23 PM	Microsoft .NET M...	640 KB
Form2.cs	5/9/2024 1:23 PM	C# Source File	2 KB
Form2.Designer.cs	5/9/2024 1:23 PM	C# Source File	12 KB
Form2.resx	5/9/2024 1:23 PM	Microsoft .NET M...	572 KB
Form4.cs	5/9/2024 1:23 PM	C# Source File	2 KB
Form4.Designer.cs	5/9/2024 1:23 PM	C# Source File	11 KB
Form4.resx	5/9/2024 1:23 PM	Microsoft .NET M...	793 KB
Form5.cs	5/9/2024 2:45 PM	C# Source File	2 KB
Form5.Designer.cs	5/9/2024 2:45 PM	C# Source File	4 KB
Form5.resx	5/9/2024 2:45 PM	Microsoft .NET M...	381 KB
icon.ico	8/15/2013 2:54 AM	Icon File	51 KB
NduesoCopyrightsSystem.cs	5/9/2024 2:45 PM	C# Source File	14 KB
NduesoCopyrightsSystem.Designer.cs	5/9/2024 1:23 PM	C# Source File	42 KB
NduesoCopyrightsSystem.resx	5/9/2024 1:23 PM	Microsoft .NET M...	654 KB
Program.cs	11/28/2019 3:30 PM	C# Source File	1 KB
ResizeBilinear.cs	10/10/2019 5:09 PM	C# Source File	1 KB

Fig. 10: Program files from folder

The program files necessary for system programming are meticulously organized within designated folders, ensuring efficient development and maintenance workflows. These folders house a comprehensive array of files essential for the system's functionality, including source code, libraries, configuration files, and documentation.

IMPLICATION TO RESEARCH AND PRACTICE

The implications of this research to practice are significant, as it offers a practical framework for enhancing copyright protection and detection in the digital domain. By integrating advanced algorithms like the Most Significant Bit (MSB) embedding technique and Deep Convolutional Neural Networks (DCNNs), the software provides a robust solution for safeguarding intellectual property rights against unauthorized use. Practitioners can utilize this technology to efficiently embed copyright information into digital images and detect potential infringements, thus streamlining enforcement processes and reducing the risk of intellectual property theft. This practical application empowers individuals and organizations to better protect their digital assets and uphold their rights, contributing to a more secure and equitable digital environment.



CONCLUSION

In conclusion, this research has developed and evaluated a software solution designed to address the growing concerns of copyright infringement in the digital landscape. The software employs a dual-faceted approach: during the protection phase, it utilizes the Most Significant Bit (MSB) embedding technique to subtly integrate copyright or trademark information into digital images, ensuring that this data is not perceptible while maintaining the image's visual quality. During the detection phase, the software leverages Deep Convolutional Neural Networks (DCNNs) to rigorously analyze images for signs of unauthorized use or copyright violations. This methodology combines advanced image processing with sophisticated pattern recognition to offer a comprehensive tool for protecting and enforcing intellectual property rights. The results of this research demonstrate the effectiveness of the proposed solution in both embedding copyright information and detecting infringement. The MSB embedding technique proved to be efficient in encoding protection data without compromising image integrity, while the DCNN-based detection algorithm successfully identified instances of copyright violations with high accuracy. This combination of methodologies not only enhances the capability to safeguard digital assets but also streamlines the enforcement process for users. The software's intuitive interface ensures that users can navigate these functionalities with ease, making it a valuable asset for individuals and organizations seeking to protect their intellectual property in an increasingly digital world.

FUTURE RESEARCH

Future research should explore integrating additional machine learning models and encryption techniques to further enhance the robustness and adaptability of copyright protection and detection mechanisms .

REFERENCES

- Anietie Ekong, Blessing Ekong and Anthony Edet (2022), Supervised Machine Learning Model for Effective Classification of Patients with Covid-19 Symptoms Based on Bayesian Belief Network, *Researchers Journal of Science and Technology*(2022),2, pp-27-33.
- Ansa, G., Cruickshank, H., & Sun, Z. (2012). An Energy-Efficient Technique to Combat DOS Attacks in Delay Tolerant Networks. *EAI Endorsed Transactions on Ubiquitous Environments*, 1, (1),.
- Basma, M. S., Julien, Tièche, J. K. & Arnaud, G. (2020). Algorithmic methods to explore the automation of the appraisal of structured and unstructured digital data, *Records Management Journal*,30(2), 175-200.
- Buschek, D., Bader, M., von Zezschwitz, E., & Luca, A. (2015). Automatic privacy classification of personal photos. *In IFIP Conference on Human-Computer Interaction*, 428–435.
- Ebong, O., Edet, A., Uwah, A., & Udoetor, N. (2024). Comprehensive Impact Assessment of Intrusion Detection and Mitigation Strategies Using Support Vector Machine Classification. *Research Journal of Pure Science and Technology*, 7,(2), 50-69.



- Edet, A. E. and Ansa, G. O. (2023). Machine learning enabled system for intelligent classification of host-based intrusion severity. *Global Journal of Engineering and Technology Advances*,16(03), 041–050.
- Edet, A., Ekong, B. and Attih, I. (2024). Machine Learning Enabled System for Health Impact Assessment of Soft Drink Consumption Using Ensemble Learning Technique. *International Journal Of Computer Science And Mathematical Theory*,10(1):79-101, DOI: 10.56201/ijcsmt.v10.no1.2024.pg79.101
- Edet, A., Silas, A., Ekaetor, E., Ebong, O., Isaac, E., & Udoetor, N. (2024). DATA-DRIVEN FRAMEWORK FOR CLASSIFICATION AND MANAGEMENT OF START-UP RISK FOR HIGH INVESTMENT RETURNS. *Advanced Journal of Science, Technology and Engineering*, 4,(2),81-102.
- Edet, A., Udonna, U., Attih, I., and Uwah, A. (2024). Security Framework for Detection of Denial of Service (DoS) Attack on Virtual Private Networks for Efficient Data Transmission. *Research Journal of Pure Science and Technology*, 7(1),71-81. DOI: 10.56201/rjpst.v7.no1.2024.pg71.81
- Ekong, A., James, G., Ekpe, G., Edet, A., & Dominic, E. A (2024). Model For The Classification Of Bladder State Based On Bayesian Network. *International Journal of Engineering and Artificial Intelligence*, 5 ,(2) 33–47
- Ekong, B., Edet, A., Udonna, U., Uwah, A.,and Udoetor, N. (2024), Machine Learning Model for Adverse Drug Reaction Detection Based on Naive Bayes and XGBoost Algorithm. *British Journal of Computer, Networking and Information Technology* 7(2), 97-114.DOI: 10.52589/BJCNIT-35MFFBC6
- Ekong, B., Ekong, O., Silas, A., Edet, A., & William, B. (2023). Machine Learning Approach for Classification of Sickle Cell Anemia in Teenagers Based on Bayesian Network. *Journal of Information Systems and Informatics*, 5(4), 1793-1808. <https://doi.org/10.51519/journalisi.v5i4.629>.
- Haonan, Z. , Jiamin, C., Ziyue, Y., Tingmin, W., Pathum, C. M. A. , Chehara, P., & Minhui, X. (2023). Copyright Protection and Accountability of Generative AI: Attack, Watermarking and Attribution. University of New South Wales, Australia.
- Hasan, R., Shaffer, P., Crandall, D., Apu Kapadia, E. T., et al. (2017). Cartooning for enhanced privacy in lifelogging and streaming videos. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 29–38.
- Henry, O., Ekong, A., Okpako, E. (2021). A Fuzzy-Based Chat-bot Messenger for Home Intelligent System with Multiple Sensors. *International Journal of Advanced Trends in Computer Science and Engineering*,10,(2),1026-1038.
- Hoyle, R., Stark, L., Ismail, Q., Crandall, D., Kapadia, A., and Anthony, D. (2020). Privacy Norms and Preferences for Photos Posted Online. *ACM Transactions on Computer Human Interaction*, 27(4): 1–27.
- Li, J., Wong, Y., Zhao, Q., and Kankanhalli, M. S. (2017a). Dual-glance model for deciphering social relationships. In *Proceedings of the IEEE International Conference on Computer Vision*, 2650–2659.
- Liu, C., Zhu, T., Zhang, J., and Zhou, W. (2020). Privacy Intelligence: A Survey on Image Sharing on Online Social Networks. *arXiv preprint arXiv:2008.12199*.
- Oh, S. J., Benenson, R., Fritz, M., & Schiele, B. (2016). Faceless person recognition: Privacy implications in social media. In *European Conference on Computer Vision*, 19– 35.



- Oh, S. J., Fritz, M., & Schiele, B. (2017). Adversarial image perturbation for privacy protection a game theory perspective. In *Proceedings of the IEEE International Conference on Computer Vision*, 1491–1500.
- Orekondy, T., Schiele, B., and Fritz, M. (2017). Towards a visual privacy advisor: Understanding and predicting privacy risks in images. In *Proceedings of the IEEE International Conference on Computer Vision*, 3686–3695.
- Shabou, B., Tièche, J., Knafou, J., Gaudinat, A. (2020). Algorithmic methods to explore the automation of the appraisal of structured and unstructured digital data. *Records Management Journal*. DOI: [10.1108/RMJ-09-2019-0049](https://doi.org/10.1108/RMJ-09-2019-0049)
- Shen, L., Hong, R., Zhang, H., Zhang, H., and Wang, M. (2019). Single-shot Semantic Image Inpainting with Densely Connected Generative Networks. In *Proceedings of the 27th ACM International Conference on Multimedia*, 1861–1869.
- Shetty, R. R., Fritz, M., and Schiele, B. (2018). Adversarial scene editing: Automatic object removal from weak supervision. In *Advances in Neural Information Processing Systems*, 7706–7716.
- Sun, X., Wu, P., and Hoi, S. C. (2018). Face detection using deep learning: An improved faster RCNN approach. *Neurocomputing*, 299: 42–50.
- Tonge, A., and Caragea, C. (2019). Dynamic deep multimodal fusion for image privacy prediction. In *The World Wide Web Conference*, 1829–1840.
- Tonge, A., Caragea, C., and Squicciarini, A. (2018). Uncovering scene context for predicting privacy of online shared images. In *Proceedings of the 32nd AAAI Conference on Artificial Intelligence*, 8167–8168.
- Uwah, A. and Edet, A. (2024). Customized Web Application for Addressing Language Model Misalignment through Reinforcement Learning from Human Feedback. *World Journal of Innovation And Modern Technology*, 8,(1), 62-71. DOI: 10.56201/wjimt.v8.no1.2024.pg62.71.
- Yang, G., Cao, G., Chen, Z., Guo, J., & Li, J. (2020). Graph-based neural networks for explainable image privacy inference, *Pattern Recognition*, Volume 105, <https://doi.org/10.1016/j.patcog.2020.107360>.
- Yingqian, C., Jie, R., Han, X., Pengfei, H., Hui, L., Lichao, S., Yue, X., Jiliang, T. (2023). Diffusionshield: a Watermark For Data CopyRight Protection Against Generative Diffusion Models.
- Yingqian, C., Jie, R., Han, X., Pengfei, H., Hui, L., Lichao, S., Yue, X., Jiliang, T. (2023). Diffusionshield: a Watermark For Data CopyRight Protection Against Generative Diffusion Models.
- Zerr, S., Siersdorfer, S., Hare, J., and Demidova, E. (2012). Privacy-aware image classification and search. In *Proceedings of the 35th International ACM SIGIR Conference on Research and Development in Information Retrieval*, 35–44.
- Zhou, W., Li, H., Lu, Y., and Tian, Q. (2012). Principal visual word discovery for automatic license plate detection. *IEEE Transactions on Image Processing*, 21(9): 4269–4279.