Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.14 No.1, 2025, pp.6-14

© Centre for Research and Innovation
www.crijournals.org
DOI:https://doi.org/10.70112/ajcst-2025.14.1.4294

Implementation of an Intellectual Property Theft Detection System for Safeguarding Digital Content

Izang Aaron. Afan [1]*, Agbaje Michael Olugbenga[2], Onome Blaise Ohwo [3], Nwandu Onyinye. J[4], Oshodi Ibukun. A[5], Erihri Jonathan. O[6] and Adelowo Opeyemi. J[7]

[1*,4,5&7] Department of Information Technology, [2&3] Department of Computer Science,
School of Computing and Engineering Sciences, Babcock University, Ogun State, Nigeria.
[6]Department of Computer Science, School of Information and Communication Technology,
Delta State Polytechnic, Delta State, Nigeria.
E-mail: agbajem@babcock.edu.ng, ohwoo@babcock.edu.ng, onyinyenwandu1@gmail.com,
ibukunnoshodi@gmail.com, erihri@yahoo.com, adelowoop@babcock.edu.ng
[*]Corresponding Author: izanga@babcock.edu.ng

(Received 19 November 2024; Revised 25 December 2024, Accepted 25 January 2025; Available online 3 February 2025)

Abstract - **Intellectual Property (IP) protection is a critical concern, driving the development of Intellectual Property Theft Detection Systems (IPTDS). However, the vast volume of digital content and the evolving tactics of offenders expose the limitations of conventional detection systems. These challenges necessitate advanced solutions capable of adapting to the complexities of the digital landscape. This study aims to design and develop an advanced IPTDS framework for detecting digital IP theft. The framework is trained on data up to October 2023, with key objectives including enhanced detection reliability, reduced false positive rates, and optimized computational efficiency to accommodate modern data scales. The IPTDS framework is implemented in Python, leveraging modern algorithms and web technologies. Its development is guided by existing literature, established practices, and real-world scenarios. Performance evaluation is conducted using key metrics such as detection rate, false positive rate, and computational efficiency. Results indicate that the proposed IPTDS outperforms state-of-the-art solutions in detection accuracy while significantly reducing false positives. Additionally, it meets computational efficiency benchmarks, confirming its practical applicability. This paper presents a highly efficient IPTDS, offering a novel, preventive, and secure approach to IP protection in the digital era. By equipping content creators and innovators with effective detection tools, the system strengthens IP security and fosters greater respect for intellectual property rights across various domains.**

Keywords: **Intellectual Property Protection, Intellectual Property Theft Detection Systems (IPTDS), Digital Content Security, Computational Efficiency, Detection Accuracy**

I. INTRODUCTION

Ideas originating from individual creativity, such as inventions, literary and artistic works, designs, symbols, and business-related names, constitute Intellectual Property (IP). IP plays a crucial role in driving innovation and contributing to national economic development [7]. However, technological advancements and the widespread availability of digital content have made intellectual property theft a significant concern for individuals and organizations. Unauthorized use or infringement of intellectual property rights not only harms creators and owners but also undermines creativity and incentives for innovation [14]. Detecting and preventing IP theft is highly complex and requires advanced systems and methodologies. In the digital age, conventional IP protection measures, such as copyright registration and legal enforcement, are increasingly inadequate. Consequently, there is a growing demand for sophisticated technological solutions capable of efficiently tracking vast amounts of digital content, identifying nuanced violations, and promptly notifying content creators and stakeholders to enhance IP protection [2]. Addressing this issue on a global scale requires joint efforts from governments, industries, and technology companies. A more secure environment for creators and businesses can be achieved through international cooperation and the establishment of clear legal frameworks for digital IP protection [3]. In summary, IP is fundamental to fostering innovation and economic progress; however, the digital era has introduced new challenges related to IP theft. To effectively combat this issue, solutions must include the development and adoption of advanced technological tools, strengthened international collaboration, and continuous updates to legal frameworks. These measures will safeguard intellectual property rights, benefit creators, and foster a robust global economy [5].

II. INTELLECTUAL PROPERTY THEFT

Intellectual Property (IP) theft refers to the unauthorized use of an idea, creative expression, or invention owned by an individual or corporation. It encompasses the infringement of patents, copyrights, trademarks, trade secrets, and other proprietary information, including names, logos, symbols, inventions, and client lists. Given the widespread prevalence of IP theft, effective intellectual property management requires robust detection systems [6].

A. Types of Intellectual Property Theft

As an increasing number of assets are digitized and made available online, Intellectual Property (IP) theft is becoming more complex to prevent. However, various forms of IP theft continue to pose significant threats in both digital and physical domains [7].

1. Copyright Infringement

Copyright infringement is one of the most common forms of IP theft. It involves the unauthorized use, distribution, or duplication of creative works protected by copyright law, including software, music, films, books, and other media [8].

2. Trademark Infringement

Trademarks serve as legally recognized identifiers for goods and services, encompassing logos, symbols, names, or phrases designed for easy recognition [1]. Trademark infringement refers to the unauthorized use of these identifiers, leading to counterfeiting and brand dilution.

3. Patent Infringement

Patent infringement occurs when manufacturing processes, design blueprints, or other documented innovations are used without authorization. In competitive markets, such violations pose a significant threat [9].

4. Trade Secret Theft

Trade secret theft involves the unauthorized acquisition or disclosure of sensitive data, such as research methodologies, product development processes, or customer databases, providing an unfair competitive advantage [9].

5. Design Infringement

Design infringement refers to the unauthorized replication of a design, layout, or visual artwork protected by intellectual property rights [9].

III. BENEFITS AND DRAWBACKS OF INTELLECTUAL PROPERTY THEFT DETECTION SYSTEMS

A. Importance of Intellectual Property Theft Detection Systems

The significance of Intellectual Property (IP) theft detection systems cannot be overstated.

1. Preserving Valuable Assets

Intellectual property represents a significant investment for businesses. As of October 2023, advancements in IP protection have become crucial. A theft detection system helps safeguard these assets [5].

2. Protecting Innovation

Innovation is the foundation of many industries, driving advancements and competitive growth. IP laws cover patents, trademarks, copyrights, and trade secrets. By detecting and preventing IP theft, companies can protect their ability to innovate without the risk of unauthorized exploitation by competitors or other entities.

3. Maintaining Competitive Advantage

Intellectual property is often the cornerstone of a company’s market position. Unauthorized use or reproduction of IP can harm market share and reputation. A detection system helps maintain brand integrity and product authenticity.

4. Legal Compliance

IP protection is mandatory in many industries. Implementing a detection system demonstrates a commitment to compliance, reducing the risk of legal disputes arising from inadequate IP asset protection [6].

5. Early Threat Detection

An IP theft detection system can identify potential threats at an early stage, allowing businesses to mitigate risks and implement protective measures. These proactive actions may include legal proceedings, securing online assets, and providing awareness training for employees and legal teams.

6. Cost Reduction

Early detection of IP theft prevents costly litigation, revenue losses, and reputational damage. The principle that “prevention is better than cure” applies here, as proactive measures are significantly less expensive than dealing with theft after it occurs.

7. Enhancing Security Practices

Implementing an IP theft detection system often leads to improved overall security measures within an organization. This may include strengthening access controls, modernizing encryption protocols, and providing employee training on handling sensitive data.

8. Global Protection

In today’s interconnected world, IP theft is not confined to domestic borders. A robust detection system enables businesses to monitor and address threats globally, identifying risks both from external sources and within the organization.

B. Drawbacks of Intellectual Property Theft Detection Systems

1. False Positives and Negatives

IP theft detection systems may produce false positives (incorrectly flagging legitimate activities as theft) and false negatives (failing to detect actual theft). Striking a balance between sensitivity and accuracy is crucial to ensuring the system effectively identifies real threats without generating excessive false positives [10], [12].

2. Complexity and Integration Challenges

Implementing an IP theft detection system requires seamless integration into existing IT infrastructure and workflows. This process can be particularly complex for large organizations with diverse systems and processes. Integration challenges may include compatibility issues, data silos, and the need for extensive customization, leading to delays and operational disruptions [11].

3. Impact on Employee Morale and Trust

Deploying an IP theft detection system may be perceived as excessive monitoring or a lack of trust. Poor communication regarding the system's purpose can lead to decreased employee morale, resentment, and, in extreme cases, attempts to bypass or sabotage the system [12].

4. Limited Effectiveness Against Insider Threats

While IP theft detection systems are effective against external threats, they may be less effective in identifying or preventing insider threats posed by employees or trusted partners with legitimate access to sensitive information. Addressing internal threats requires additional measures, such as employee training and fostering a security-conscious organizational culture [11].

5. Adaptability to Evolving Threats

Cyber threats and IP theft tactics continuously evolve. A detection system that is effective today may become obsolete if it fails to adapt to new attack vectors, techniques, or technologies. Regular updates and enhancements are necessary to maintain effectiveness against emerging threats [13].

6. Overreliance on Technology

Relying solely on technology for IP theft detection may create a false sense of security. Effective IP protection requires a holistic approach that integrates technological solutions with robust policies, procedures, and human oversight. Overdependence on technology alone may overlook vulnerabilities in other areas of the organization [14]. An IP theft detection system serves as a proactive measure to safeguard valuable assets, maintain competitiveness, ensure legal compliance, and foster a secure environment for innovation and growth. However, its limitations must be carefully managed to maximize effectiveness.

IV. RELATED WORK

J. F. Morin [16] utilized digital forensics tools and practices, emphasizing their significance in incident response, network forensics, and the development of forensic techniques for detecting digital evidence of IP theft and cybercrimes. This assessment is instrumental in identifying vulnerable information assets and evaluating associated risks. The study highlights the importance of assessing security measures for hardware, networks, corporate devices, and sensitive data belonging to both customers and employees, extending beyond intellectual property considerations.

A. P. Moore [15] focused on identifying potential insider threats within organizations involved in IP theft. However, addressing insider threats requires a comprehensive approach, as insiders have full access to company systems and an in-depth understanding of internal operations. Existing solutions for mitigating insider threats are often reactive and tactical, failing to address the problem holistically. Consequently, sensitive information stored within organizational systems remains highly susceptible to exploitation by disgruntled or opportunistic employees. Studies frequently employ behavioral analysis, access logs, and user activity monitoring to detect suspicious behavior among employees.

Z. Nadav [17] employed watermarking techniques, which involve embedding concealed information within digital media to trace unauthorized sharing or copying back to its source. Additionally, Digital Rights Management (DRM) solutions help organizations safeguard copyright and intellectual property rights by implementing access controls. These techniques complicate unauthorized access to a company's content or services, ensuring operational efficiency and business continuity. DRM achieves this by embedding additional code or data into products specifically designed to prevent unauthorized use.

R. Freedman [18] specialized in conducting IP audits, which assess an organization's existing intellectual property assets to identify vulnerabilities and risks related to IP theft. The implementation of asset management tools and best practices enables organizations to efficiently track and protect their IP assets. Assessment tools play a critical role in safeguarding against IP theft by identifying system or process weaknesses that could be exploited. These tools evaluate the current state of security, detect vulnerabilities, and recommend enhancements to protect sensitive data from breaches or theft.

M. S. Islam [19] explored various types of phishing attacks, including email spoofing, spear phishing, phone phishing, clone phishing, pharming, HTTP phishing, man-in-the-middle attacks, and fast-flux phishing. A filtered website was developed to detect fraudulent links, thereby enhancing digital security, although further research is required.

K. A. Y. Yaseen [20] examined the impact of the digital revolution, which has brought numerous benefits, such as improved information and knowledge exchange, while also introducing risks such as cyberattacks and malicious programs. The higher education sector is particularly vulnerable, with threats affecting infrastructure, students, faculty, and teaching methodologies. To protect this vital sector, awareness initiatives, training programs, and robust cybersecurity policies are essential. This study explores strategies for strengthening cybersecurity in higher education institutions. Analyzed cybersecurity [21] risks in the education sector, which faces the highest percentage of cyberattacks due to the expansion of e-learning platforms. Using the Kaspersky DDoS Intelligence System, this study assesses these risks and discusses effective methods for safeguarding educational institutions against cyber threats.

A. Key Strategies for IP Theft Detection

Research highlights the following key strategies for detecting Intellectual Property (IP) theft:

1. Digital Forensics

Digital forensic tools and methodologies are employed to analyze risks, enhance security measures, and identify digital evidence related to IP theft and cybercrimes [16].

2. Insider Threat Mitigation

This strategy detects potential insider threats through behavioral analysis and user activity monitoring, focusing on individuals with authorized access to sensitive information [15].

3. Watermarking and DRM

Watermarking and Digital Rights Management (DRM) techniques protect IP by tracing unauthorized use and enforcing copyright protections [17].

4. IP Audits

Asset management tools and audits assist in identifying vulnerabilities and evaluating security measures to enhance IP protection [18].

V. METHODOLOGY

This section outlines the approach used to develop an effective Intellectual Property (IP) theft detection system.

A. Software Development Life Cycle (SDLC) Methodology

The Waterfall Model was chosen as the SDLC methodology for this study. The Waterfall Model is a sequential design process commonly used in software development, where progress flows steadily downward through distinct phases: conception, initiation, analysis, design, construction, testing, production/implementation, and maintenance. Each phase is executed in sequence, with transitions occurring only after a structured review process. In an IP theft detection system, precision and thoroughness are paramount. The Waterfall Model facilitates systematic planning and execution, ensuring that each system component is developed with accuracy and reliability.

1. Requirements Gathering

This phase involves defining all required features and functionalities of the system. It incorporates regulatory and industry standards for IP protection while addressing stakeholder needs and expectations.

2. System Design

Once requirements are established, this phase focuses on defining the architecture and technical specifications of the detection system.

3. Development Phase

The system is implemented based on the design specifications. This phase includes coding and programming detection algorithms and software components.

4. Implementation and Testing

Unlike the rapid prototyping approach, the Waterfall Model emphasizes thorough testing and validation at each stage. The system undergoes rigorous testing to identify and resolve bugs, ensuring reliability and accuracy. Training data extends up to October 2023, and system performance is evaluated based on its effectiveness in preventing IP theft.

5. Model Deployment

After successful testing and validation, the system is deployed in a real-world environment.

6. Maintenance

This final phase involves ongoing maintenance to ensure optimal system performance. Given its structured and rigorous nature, the Waterfall Model guarantees high-quality and reliable outcomes, making it particularly suitable for applications such as IP theft detection.

B. Software Development Model

1. Incremental Model

The Incremental Model was used for software development. This model was selected as it allows for modifications and the addition of new functionalities without extensive code comparisons with traditional programming languages. Consequently, it accelerates development while enabling seamless feature enhancements.

2. Database Development

XAMPP was utilized for database development, serving as the repository for all data and information entered into the system by administrators and authorized staff members. The Windows operating system was selected due to its compatibility with the software.

C. Software Components

The following software components were employed:

1. *Apache Web Server* - Handles web hosting and server-side functionalities.
2. *MySQL* - Used to create and manage the database for the application via phpMyAdmin.
3. *HTML, CSS, and PHP* - Utilized for designing and developing the web pages of the application.

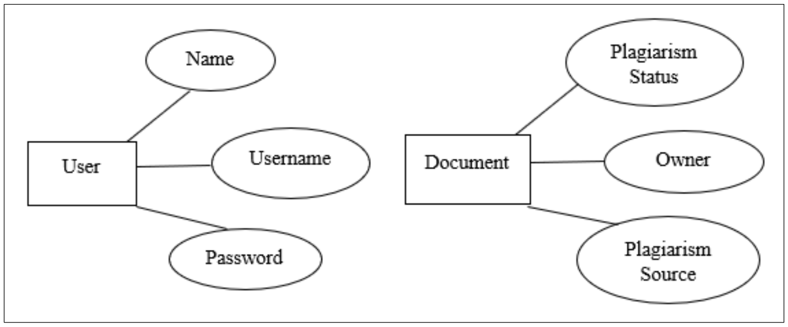


Fig. 1 Entity Relationship Diagram of The System

In Fig. 1, the two main entities are the User and the Document, with their respective roles and actions outlined as follows:

D. User

Users are individuals who compare text documents on the platform. They are granted access by an administrator and can perform the following functions:

1. Login
2. Enter Username
3. Enter Password
4. Logout

E. Document

Documents represent the digital files uploaded to the platform for comparison. Users with administrator-granted access can perform the following operations:

1. Login
2. Check Plagiarism Source
3. View Plagiarism Status
4. Logout

The overall system structure consists of three main components: the front end, the internet, and the backend. The system architecture is illustrated in Fig. 2. The system flowchart, which illustrates how the system operates, is shown in Fig. 3.

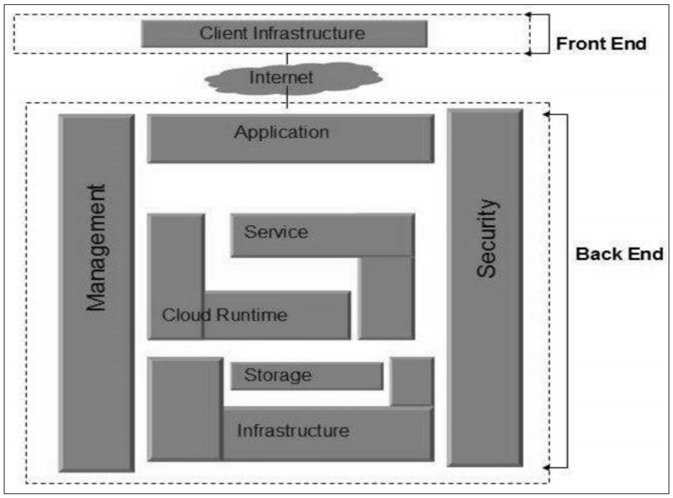


Fig. 2 System Architecture of the IPTDS

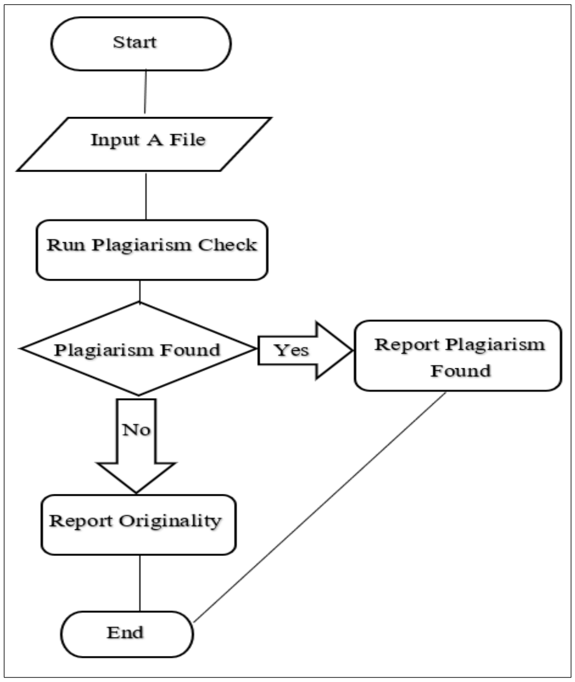


Fig. 3 Flowchart of the IPTDS

VI. IMPLEMENTATION OF THE SYSTEM

A. Implementation Phase

The implementation phase involves the development and deployment of the system, including coding, integration, testing, and deployment. The following steps outline the implementation process of an Intellectual Property (IP) theft detection system:

1. *System Development:* The first step in implementing the IP theft detection system is development. This phase includes software coding, user interface design, and system integration. The system is developed using PHP, JavaScript, Python, HTML, and CSS.

2. *Database Design and Implementation:* The second step involves designing and implementing the database for the IP theft detection system. The database stores all relevant system data, such as user information and detection results. MySQL, a widely used open-source relational database management system, is utilized for database design.

3. *Integration:* The third step is integrating various components and modules into a unified system for IP theft detection. This process involves combining multiple data sources, algorithms, and detection techniques to ensure seamless operation and reliable detection. It is analogous to assembling the pieces of a puzzle to create a comprehensive solution.

4. *User Testing:* Once the IP theft detection system is developed; user testing is conducted to verify its functionality and ensure it meets user requirements. A selected group of users interacts with the system and provides feedback for further improvements.

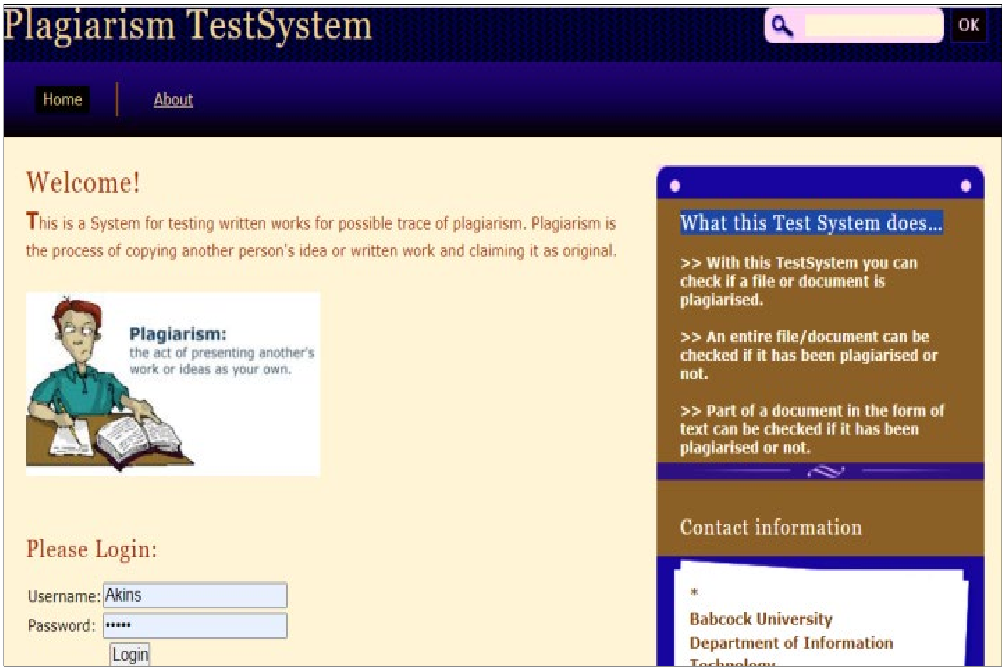
5. *Deployment:* The final phase of implementation is system deployment, which involves installing the system on the production server and making it accessible to users.

B. The Login Page

The login page is the first interface a user encounters when accessing a website through an internet browser. It serves as the entry point, allowing users to enter their credentials to gain access to the site. Upon successful login, users are redirected to their personalized dashboard or relevant sections of the website.

C. Comparison Page

The image above illustrates the website environment, where documents, text files, or plain text are collected and analyzed to detect plagiarism or provide relevant feedback.



Welcome!

This is a System for testing written works for possible trace of plagiarism. Plagiarism is the process of copying another person's idea or written work and claiming it as original.

Plagiarism: the act of presenting another's work or ideas as your own.

Please Login:

Username: Akins
Password: •••••

What this Test System does...

>> With this TestSystem you can check if a file or document is plagiarised.

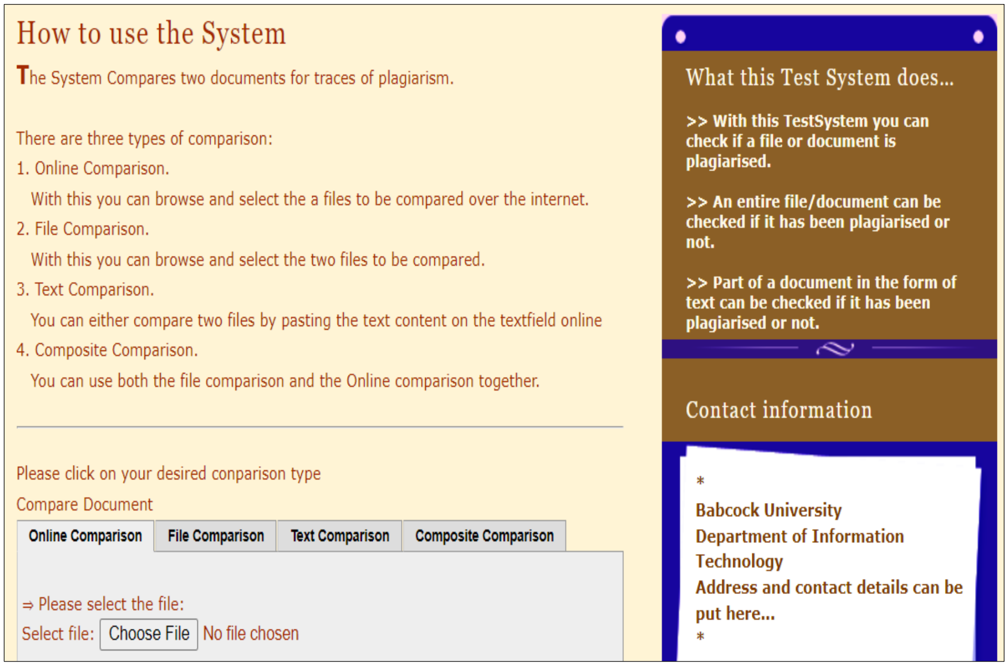
>> An entire file/document can be checked if it has been plagiarised or not.

>> Part of a document in the form of text can be checked if it has been plagiarised or not.

Contact information

*
Babcock University
Department of Information
Technology

Fig. 4 The Login Page



How to use the System

The System Compares two documents for traces of plagiarism.

There are three types of comparison:
1. Online Comparison.
With this you can browse and select the a files to be compared over the internet.
2. File Comparison.
With this you can browse and select the two files to be compared.
3. Text Comparison.
You can either compare two files by pasting the text content on the textfield online
4. Composite Comparison.
You can use both the file comparison and the Online comparison together.

Please click on your desired comparison type
Compare Document

⇒ Please select the file:
Select file: Choose File No file chosen

What this Test System does...

>> With this TestSystem you can check if a file or document is plagiarised.

>> An entire file/document can be checked if it has been plagiarised or not.

>> Part of a document in the form of text can be checked if it has been plagiarised or not.

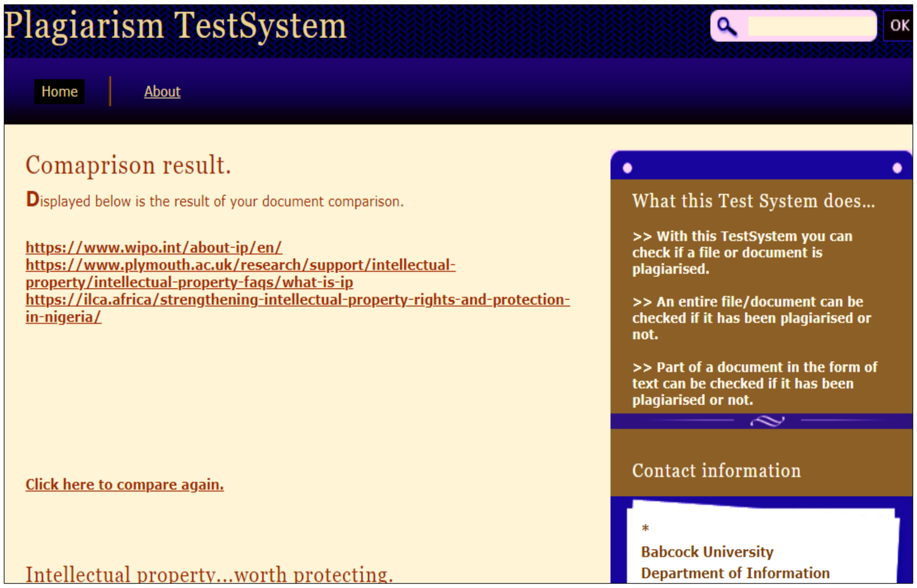
Contact information

*
Babcock University
Department of Information
Technology
Address and contact details can be put here...
*

Fig. 5 The Comparison Page

D. Result Page

This page displays the aggregated results from the online comparison, including links to webpages containing related content found within the document.



Comaprison result.

Displayed below is the result of your document comparison.

https://www.wipo.int/about-ip/en/
https://www.plymouth.ac.uk/research/support/intellectual-property/intellectual-property-faqs/what-is-ip
https://ilca.africa/strengthening-intellectual-property-rights-and-protection-in-nigeria/

Click here to compare again.

Intellectual property...worth protecting.

What this Test System does...

>> With this TestSystem you can check if a file or document is plagiarised.

>> An entire file/document can be checked if it has been plagiarised or not.

>> Part of a document in the form of text can be checked if it has been plagiarised or not.

Contact information

*
Babcock University
Department of Information

Fig. 6 This Page Shows the Results

VII. WORKFLOW OPERATION

This section explores the different comparison methods in detail:

A. Online Comparison

In this method, users upload a text file to a web-based platform designed to detect instances of Intellectual Property (IP) theft. The platform utilizes web crawlers—automated programs that traverse the internet to search for content matching or closely resembling the uploaded text. These crawlers compare the submitted text against vast repositories of existing online materials, including websites, articles, databases, and other textual sources. If similarities or matches are detected, the system generates a detailed report with links to the identified sources, enabling users to take appropriate action to prevent IP theft.

B. File Comparison

This approach allows users to perform a direct comparison between two files stored on their local devices. Users can browse their local storage or directories and select the text files for comparison. These files may contain various types of content, including documents, images, audio, or other digital media. The comparison process analyzes the selected files across three editors, identifying content differences and similarities. The system then generates a comprehensive report, allowing users to examine discrepancies and assess potential instances of IP theft.

C. Text Comparison

This method enables users to paste text from two files into separate fields on a web page and compare their content side by side. Users can either manually enter text or copy and paste it from existing files into the designated fields. The system scans the provided text for similarities and differences. When compared against large datasets, it facilitates the quick and efficient analysis of smaller text segments, such as paragraphs, sentences, or code snippets, to detect potential infringement.

D. Composite Comparison

This approach enables users to perform file and online comparisons simultaneously. Users can conduct local file comparisons while also performing a web-wide scan for potential Intellectual Property (IP) theft. By integrating these two methods, users can assess content similarity both locally and globally, helping them identify and address unauthorized use or infringement.

These comparison techniques provide users with a comprehensive set of tools for detecting and preventing IP theft, catering to diverse technological needs. Whether users prefer local analysis or web-based scanning, these methods serve as effective measures for safeguarding intellectual property rights.

VIII. CONCLUSION AND RECOMMENDATIONS

The widespread violation of Intellectual Property (IP) rights has become a significant challenge, necessitating the implementation of an IP theft detection system. Such a system provides a systematic approach to addressing this issue, enabling businesses and individuals to protect their intellectual property by ensuring it is properly identified and safeguarded against unauthorized use, copying, or reproduction.

A. Increased Security

The system enhances security by continuously monitoring intellectual property through a mapping algorithm, which tracks relevant IP assets and notifies users of potential infringements. This section expands on the design and implementation strategy used to develop the IP theft detection system. It discusses key phases, including system development and design, algorithm implementation, data integration, testing, and deployment. To ensure reliability, the IP theft detection and prevention system must undergo rigorous testing across multiple parameters. Organizations that successfully implement such protections can strengthen their core intellectual property and compete effectively in the marketplace.

Based on the findings of this research, the following recommendations are proposed:

1. *Industry Partnerships* - Collaborating with industry stakeholders, including businesses, legal experts, and organizations specializing in IP protection, can provide valuable insights and best practices for developing an effective IP theft detection system. Additionally, partnerships with government agencies can help tailor the system to country-specific needs and challenges.
2. *Incentivizing Adoption* - To encourage the adoption of the IP theft detection system among businesses and individuals, incentives such as discounted subscription fees, free trial periods, or rewards for reporting and preventing IP theft should be considered.
3. *Adopting Cutting-Edge Detection Technologies* - The system must integrate the latest detection technologies to combat the constantly evolving threat landscape. Advanced techniques such as machine learning algorithms, pattern recognition, and behavioral analysis should be employed to enhance detection accuracy and effectiveness.
4. *Providing Comprehensive Training and Support* - Offering thorough training and ongoing support can help users effectively utilize the system's features. System providers should offer resources such as guides, tutorials, and customer support to address user concerns promptly.

By implementing these recommendations, individuals and businesses can leverage the IP theft detection system to safeguard valuable assets and minimize the risks associated with IP infringement. Additionally, continuous evaluation of the system's effectiveness is essential to ensuring its long-term success in combating intellectual property theft.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation

The authors confirm that no AI-assisted technologies were used in the preparation or writing of the manuscript, and no images were altered using AI.

REFERENCES

[1] H. Nasheri, "Addressing the global scope of intellectual property crimes and policy initiatives," *Trends Organ. Crim.*, vol. 8, pp. 79-108, 2005. [Online]. Available: https://doi.org/10.1007/s12117-005-1015-y

[2] Z. Mingaleva and I. Mirskikh, "The problems of legal regulation and protection of intellectual property," *Procedia - Soc. Behav. Sci.*, vol. 81, pp. 329-333, 2013. [Online]. Available: https://doi.org/10.1016/j.sbspro.2013.06.437

[3] M. Ramamoorthy, "The role of intellectual property rights in the global economy," *World Trade Rev.*, vol. 8, no. 1, pp. 1-46, 2009.

[4] National Crime Prevention Council, "Digital Intellectual Property Theft," Nov. 7, 2023. [Online]. Available: http://archive.ncpc.org/programs/living-safer-being-smarter/surfing-safer/digital intellectual-property-theft.html

[5] Global IP Convention, "Intellectual property challenges in the digital age," Aug. 1, 2023. [Online]. Available: https://www.globalipconvention.com/blog/intellectual-property-challenges-in-the-digital-age

[6] L. Bleidornt, "How does intellectual property protection affect innovation," June 8, 2022. [Online]. Available: https://www.redpoints.com/blog/how-does-intellectual-property-protection-affectinnovation/

[7] Proofpoint, "What is intellectual property theft - IP theft definition, examples & more," Sept. 18, 2023. [Online]. Available: https://www.proofpoint.com/us/threat-reference/intellectual-property-theft

[8] World Intellectual Property Organization (WIPO), *What is Intellectual Property?* WIPO Publication, 2021. doi: 10.34667/tind.43765. ISBN: 9789280532210.

[9] World Intellectual Property Organization (WIPO), *Understanding Industrial Property*, WIPO Publication, 2016. doi: 10.34667/tind.36288. ISBN: 9789280525939.

[10] World Intellectual Property Organization (WIPO), *Understanding Copyright and Related Rights*, p. 8. [Online]. Available: Archived from the original (PDF) on June 6, 2012. Retrieved Aug. 1, 2023.

[11] Ekran System, "Intellectual property theft: 7 best practices on how to prevent it," July 13, 2023. [Online]. Available: https://www.ekransystem.com/en/blog/best-practices-to-prevent-intellectualpropertytheft

[12] C. Ostendorf, "What is intellectual property (IP) theft?" Sept. 28, 2023. [Online].Available:https://www.code42.com/blog/what-is-intellectual-property-theft/

[13] R. E. Falvey, N. Foster, and O. Memedovic, "The role of intellectual property rights in technology transfer and economic growth: Theory and evidence," *United Nations Industrial Development Organization (UNIDO)*, Geneva, 2006.

[14] K. Yu, *Intellectual Property and Information Wealth: Copyright and Related Rights*, Greenwood Publishing Group, 2007, p. 346. ISBN: 978-0-275-98883-8.

[15] A. P. Moore, D. McIntire, D. Mundie, and D. Zubrow, "Justification of a pattern for detecting intellectual property theft by departing insiders,"Mar.2013.[Online].Available:https://apps.dtic.mil/sti/tr/pdf/ADA610785.pdf

[16] J. F. Morin, "Paradigm shift in the global IP regime: The agency of academics," *Rev. Int. Polit. Econ.*, vol. 21, no. 2, pp. 275-309, 2014. [Online]. Available: http://dx.doi.org/10.1080/09692290.2013.819812

[17] N., "Digital Rights Management (DRM)," June 13, 2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-digital-rights-management/

[18] R. Freedman, "AI rise increases importance of IP audits," *Legal Dive*, Mar.7, 2024. [Online]. Available: https://www.legaldive.com/news/ai-rise-increases-importance-of-ip-audits-stephen-sullivan-schwabe-intellectual-property/709654/

[19] M. S. Islam, M. Sajjad, M. M. Hasan, and M. S. I. Mazumder, "Phishing attack detecting system using DNS and IP filtering," *Asian Journal of Computer Science and Technology*, vol. 12, no. 1, pp. 16-20, Apr. 2023. doi: 10.51983/ajcst-2023.12.1.3552.

[20] K. A. Y. Yaseen, "Importance of cybersecurity in the higher education sector 2022," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 20-24, Oct. 2022.

[21] K. A. Y. Yaseen, "Digital education: The cybersecurity challenges in the online classroom (2019-2020)," *Asian Journal of Computer Science and Technology*, vol. 11, no. 2, pp. 33-38, Nov. 2022.