AuthentiScan: An AI-Powered Browser Extension for Real-Time Content Authenticity Detection

Under the guidance of
Dr. Naveen Kumar C
Professor & Head
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India

Chaitanya M
Department of Data Science
Aditya College of Engineering and Technology
Bangalore, India
chaitu3065@gmail.com

Muthaheera Firdos
Department of Data Science
Aditya College of Engineering and Technology
Bangalore, India
muthaheerafirdos65@gmail.com

Rishika MJ
Department of Data Science
Aditya College of Engineering and Technology
Bangalore, India
rishikamj72@gmail.com

Sejal S Bole
Department of Data Science
Aditya College of Engineering and Technology
Bangalore, India
sejalbole5@gmail.com

Abstract- AuthentiScan is an AI-powered browser extension designed to identify and detect potentially fake, manipulated, or misleading digital content in real time. The proposed system aims to improve online information reliability by helping users verify the authenticity of documents, images, and other digital content while browsing the internet. It uses Artificial Intelligence (AI), Machine Learning (ML), and Optical Character Recognition (OCR) techniques to analyze uploaded or selected content and identify suspicious patterns, alterations, and signs of forgery. The system processes the extracted information and evaluates its authenticity based on predefined verification methods and detection mechanisms. It provides users with clear results indicating whether the analyzed content appears authentic, suspicious, or potentially manipulated. AuthentiScan is designed with a simple and user-friendly interface that allows individuals to perform content verification without requiring advanced technical knowledge. By integrating intelligent detection techniques into a browser extension, the platform aims to make digital content verification more accessible, efficient, and convenient. The proposed system helps reduce the risks associated with fake documents, misleading information, and digitally manipulated content. It also promotes safer online interactions by encouraging users to verify information before trusting or sharing it. Overall, AuthentiScan provides an intelligent and practical approach to improving digital trust, strengthening content authenticity, and supporting reliable information sharing in the modern digital environment.

Keywords— AuthentiScan, Artificial Intelligence, Machine Learning, Browser Extension, Content Authenticity Detection, Digital Verification, Optical Character Recognition, Forgery Detection, Fake Content Identification, Online Security.

I. INTRODUCTION

The rapid growth of the internet and digital technologies has significantly changed the way people create, access, and share information. Online platforms have become important sources of documents, images, news, and other digital content. However, the increasing availability of digital editing tools and artificial intelligence technologies has also made it easier to create fake documents, manipulate images, and distribute misleading information. Such activities can affect the reliability of online information and create challenges in identifying genuine content. Therefore, developing an effective solution for detecting manipulated and unauthentic digital content has become increasingly important.

AuthentiScan is proposed as an AI-powered browser extension that aims to identify potentially fake, altered, or suspicious digital content in real time. The system focuses on improving digital content verification by combining Artificial Intelligence (AI), Machine Learning (ML), and Optical Character Recognition (OCR) techniques. It is designed to help users examine digital content and recognize possible signs of manipulation or forgery. By integrating verification capabilities into a browser extension, AuthentiScan provides a convenient approach to checking content while browsing the internet.

The proposed system incorporates intelligent content analysis techniques to examine the characteristics and patterns of digital information. OCR technology helps extract readable text from documents and images, while machine learning techniques support the identification of suspicious patterns and possible alterations. The system analyzes the available content and generates verification results that help users understand whether the content appears authentic, suspicious, or potentially manipulated. This approach reduces the need for users to depend entirely on manual verification methods.

The main objective of AuthentiScan is to develop a user-friendly and efficient browser extension that supports real-time content authenticity detection. The system aims to improve awareness of digital misinformation, assist in identifying forged documents, and provide users with a simple verification process. Its browser-based functionality makes content checking more accessible and convenient. The proposed platform can be useful in situations where users need to examine online information, verify digital documents, and make informed decisions before trusting or sharing content.

Another important objective of Smart Skill Hub is to improve career readiness by helping learners understand the relationship between their current capabilities and their desired professional roles. Regular progress tracking allows users to review their development and identify areas that require further attention. The framework can also be extended to include mentorship, certification opportunities, industry-oriented training, and collaboration with organizations. Such enhancements could create stronger connections between educational institutions, learners, and employers.

The remainder of this paper presents the proposed system architecture, the methodology used for skill assessment and learning recommendations, the implementation of the platform, and the testing and evaluation process. The final sections discuss the outcomes, limitations, and possible directions for future development.

II. LITERATURE SURVEY

The development of artificial intelligence and natural language processing has created new opportunities for identifying misleading, manipulated, and unreliable digital content. The increasing spread of misinformation, fake news, and AI-generated text has highlighted the need for automated content verification systems. AuthentiScan aims to address these challenges through an AI-powered browser extension that analyzes online content and provides real-time authenticity assessments.

A. AI-Based Content Authenticity Detection

Artificial Intelligence techniques play an important role in identifying whether digital content is genuine or potentially misleading. Machine learning models can examine textual patterns, writing styles, and contextual information to detect suspicious content. AuthentiScan uses AI-based analysis to help users evaluate the reliability of online information and make informed decisions.

B. Natural Language Processing (NLP)

Natural Language Processing enables computers to understand, interpret, and analyze human language. NLP techniques can identify unusual language patterns, misleading statements, and inconsistencies in written content. These techniques support AuthentiScan in examining webpage text and identifying information that may require further verification.

C. Fake News and Misinformation Detection

The rapid growth of social media and online publishing has increased the circulation of false and misleading information. Existing detection approaches use machine learning, linguistic analysis, and classification techniques to distinguish trustworthy information from potentially false content. AuthentiScan focuses on identifying suspicious online information and providing users with useful authenticity-related feedback.

D. Machine Learning-Based Classification

Machine learning algorithms are widely used to classify digital information based on previously learned patterns. These models can analyze textual features and predict whether content belongs to genuine or suspicious categories. AuthentiScan applies classification-based techniques to support automated content assessment and improve the efficiency of online verification.

E. Browser Extension-Based Verification Systems

Browser extensions provide convenient access to additional functionalities while users browse websites. They can analyze webpage information and display results without requiring users to visit separate applications. AuthentiScan follows this approach by integrating content authenticity detection into a browser extension, making verification more accessible and convenient.

F. AI-Generated Content Identification

Recent developments in generative AI have made it increasingly difficult to distinguish human-written content from machine-generated text. Different detection approaches examine writing patterns, linguistic characteristics, and statistical features to estimate the possibility of AI-generated content. AuthentiScan aims to incorporate intelligent text analysis to help users understand the nature and reliability of digital information.

G. Research Gap and Proposed Approach

Existing content verification approaches often focus on individual aspects, such as fake news detection, text classification, or AI-generated content identification. Some systems also require users to manually copy and paste information into separate platforms for verification. AuthentiScan addresses these limitations by proposing an integrated AI-powered browser extension that performs real-time content analysis and provides authenticity-related results directly while browsing. This approach aims to improve accessibility, reduce manual verification efforts, and promote safer consumption of online information.

III. METHODOLOGY

The proposed AuthentiScan follows a systematic methodology to identify potentially misleading, manipulated, and AI-generated online content. The development process involves requirement analysis, system architecture design, user interface development, content extraction, AI-based text analysis, authenticity classification, result generation, database management, testing, and deployment. The methodology aims to provide users with an efficient and accessible way to evaluate the authenticity of digital information while browsing the internet.

A. Requirement Analysis

The initial phase focuses on identifying the functional and technical requirements of the AuthentiScan system. The major requirements include webpage content extraction, text analysis, AI-based authenticity detection, suspicious content identification, and displaying analysis results. These requirements help determine the technologies, tools, and system components needed for implementation.

B. System Architecture

AuthentiScan follows a modular architecture in which different components work together to analyze online content. The browser extension provides the user interface and collects webpage text, while the backend processes the extracted information using AI-based analysis techniques.

The system evaluates the content and returns the results to the extension for display. This architecture supports efficient communication between the frontend, backend, and analysis modules.

C. User Interface Development

The user interface is designed to provide a simple and user-friendly experience. HTML, CSS, and JavaScript are used to develop the browser extension interface. The interface allows users to initiate content analysis and view the authenticity assessment. Appropriate visual indicators and result descriptions help users understand whether the analyzed content appears trustworthy, suspicious, or potentially AI-generated.

D. Webpage Content Extraction

This module is responsible for collecting textual information from the currently accessed webpage. The browser extension extracts relevant text while avoiding unnecessary elements such as advertisements, navigation menus, and unrelated page components wherever possible. The collected content is then prepared for further processing. This step provides the necessary input for the AI-based detection process.

E. Text Preprocessing Module

The extracted webpage content undergoes preprocessing before being submitted for analysis. This process may include removing unnecessary symbols, eliminating duplicate spaces, handling special characters, and organizing the text into a suitable format. Preprocessing improves the consistency of the input data and helps the analysis component examine the content more effectively.

F. AI-Based Content Analysis

The AI analysis module examines the extracted text using suitable artificial intelligence and natural language processing techniques. It evaluates linguistic patterns, sentence structure, contextual information, and other relevant textual characteristics. These techniques help identify unusual patterns and content that may require additional verification. The analysis results are used to support the authenticity assessment.

G. Content Classification and Authenticity Detection

After analyzing the webpage content, the system applies classification techniques to categorize the identified information. Based on the implemented detection methods, the content can be classified into categories such as potentially genuine, suspicious, or AI-generated. The classification process helps users understand the possible reliability of the information. The system presents these results as automated assessments rather than absolute proof of authenticity.

H. Result Generation and Display

Once the analysis and classification processes are completed, AuthentiScan generates a summarized result for the user. The output includes the detected content category and relevant analysis information. Results are displayed directly through the browser extension interface, allowing users to understand the assessment without switching to another application. This improves accessibility and makes the verification process convenient.

I. Backend and Database Management

The backend manages communication between the browser extension and the AI analysis components. It receives extracted webpage content, processes analysis requests, and sends the corresponding results back to the extension. A database can be used to maintain relevant information such as user details, analysis history, and system records, depending on the implemented requirements. Proper data handling helps maintain system organization and reliability.

J. Testing and Evaluation

Testing is performed to verify the correctness and performance of the AuthentiScan system. Functional testing checks browser extension installation, webpage text extraction, content submission, AI analysis, classification, and result display. Integration testing ensures that the frontend, backend, and analysis modules communicate correctly. Performance and usability testing are also conducted to identify errors and improve the overall user experience.

K. Deployment and Maintenance

After successful testing, the AuthentiScan browser extension and its supporting backend components can be deployed in the intended environment. Maintenance activities include resolving technical issues, improving detection methods, updating system components, and enhancing the user interface. Regular updates help the application remain compatible with browser changes and evolving content analysis requirements.

L. Methodology Outcome

The proposed methodology provides a structured approach to developing AuthentiScan as an AI-powered browser extension for real-time content authenticity detection. By combining webpage text extraction, preprocessing, natural language processing, AI-based analysis, and content classification, the system aims to help users identify potentially misleading and AI-generated online information. Integrating these functions into a browser extension makes content assessment more accessible, convenient, and efficient.

IV. EXISTING SYSTEM

The existing system for content authenticity verification relies on various online tools and platforms to identify fake news, misleading information, and AI-generated content. These tools use different techniques, including manual fact-checking, text analysis, machine learning, and AI detection. However, users may need to access multiple websites and applications to verify the reliability of online information, which can make the process time-consuming.

A. Manual Fact-Checking Methods

Traditional fact-checking involves verifying online information by comparing it with trusted websites, official reports, and reliable sources. Although this approach helps identify incorrect information, it requires considerable time and manual effort from users.

B. Fake News Detection Platforms

Existing fake news detection platforms analyze news articles and online content to identify potentially false or misleading information. These platforms may use machine learning algorithms and language analysis techniques. However, their accuracy can depend on the available datasets and the quality of the information being analyzed.

C. AI-Generated Text Detection Tools

Several online applications are designed to identify content produced using artificial intelligence. They examine writing patterns, sentence structures, and linguistic characteristics to estimate whether a text may have been generated by AI. However, detection results are not always reliable, particularly when AI-generated text has been edited or rewritten.

D. Online Content Verification Tools

Content verification websites allow users to check the reliability of information by examining sources, references, and supporting evidence. These tools can help users identify questionable claims. However, users may need to manually copy content or search for related information across different platforms.

E. Machine Learning-Based Detection Systems

Existing detection systems apply machine learning and natural language processing techniques to classify text based on its characteristics. These approaches support automated identification of suspicious content. However, their performance may be affected by training data quality, changing writing patterns, and the complexity of online information.

F. Limitations of the Existing System

The major limitations of existing content verification approaches include:

- Users may need to visit multiple websites to verify online information.
- Manual fact-checking requires additional time and effort.
- AI-generated text detection tools may produce incorrect results.
- Some platforms require users to copy and paste content manually.
- Detection systems may not provide complete explanations for their results.
- Different verification tools often operate independently.
- Real-time content analysis may not be available in every platform.

G. Summary

Existing content verification systems provide useful facilities for detecting misleading information, checking online sources, and identifying potentially AI-generated text. However, many approaches require separate applications and manual verification. AuthentiScan aims to address these limitations through an integrated AI-powered browser extension that analyzes webpage content and provides real-time authenticity-related results in a single interface, making online content assessment more convenient and accessible.

V. PROPOSED SYSTEM

The proposed AuthentiScan is designed to help users identify potentially misleading, suspicious, and AI-generated online content. The system provides an integrated platform that analyzes webpage text using Artificial Intelligence (AI) and Natural Language Processing (NLP) techniques. It allows users to check the authenticity of online information directly through a browser extension without depending entirely on separate verification websites.

A. Key Components

1. **Browser Extension:** Provides an interface through which users can initiate content analysis while browsing websites.
2. **Webpage Content Extraction:** Collects relevant textual information from the currently opened webpage for further examination.
3. **Text Preprocessing:** Removes unnecessary characters, spaces, and irrelevant elements to prepare the extracted text for analysis.
4. **AI-Based Content Analysis:** Examines textual patterns, sentence structure, and linguistic characteristics using suitable AI techniques.
5. **Fake Content Detection:** Identifies potentially misleading or suspicious information by analyzing the available textual features.
6. **AI-Generated Text Detection:** Evaluates writing patterns to estimate whether the analyzed content may have been generated using artificial intelligence.
7. **Result Generation:** Displays the analysis outcome through the extension interface with suitable classifications and feedback.

B. AI-Driven Features

- **Automated Content Analysis:** Examines webpage information automatically and reduces the need for manual checking.
- **Natural Language Processing:** Uses language-processing techniques to understand and evaluate textual content.
- **Authenticity Classification:** Categorizes analyzed content according to the detection methods implemented in the system.
- **Suspicious Pattern Identification:** Highlights unusual textual characteristics that may require additional verification.
- **Real-Time Feedback:** Provides analysis results directly through the browser extension after processing the selected webpage content.
- **Content Assessment:** Helps users understand the possible reliability of information through summarized analysis results.

C. System Benefits

- **Easy Accessibility:** Allows users to analyze online content directly through a browser extension.
- **Time Efficiency:** Reduces the effort involved in manually checking information across multiple platforms.
- **Automated Verification Support:** Uses AI techniques to assist in identifying potentially misleading content.
- **User-Friendly Interface:** Presents analysis results in a simple and understandable format.
- **Improved Awareness:** Helps users become more cautious when accessing questionable online information.
- **Future Scalability:** Supports the addition of improved detection algorithms and new verification features.

D. Summary

AuthentiScan aims to provide a convenient and intelligent solution for analyzing the authenticity of digital content. Its main components combine webpage text extraction, preprocessing, AI-based analysis, and content classification within a single browser extension. By providing accessible and timely feedback, the proposed system helps users identify potentially misleading and AI-generated information and encourages responsible consumption of online content.

VI. ADVANTAGES

The AuthentiScan system offers the following advantages:

1. **Real-Time Content Analysis:** Examines webpage content directly through a browser extension and provides analysis results.
2. **Easy Accessibility:** Allows users to check online information without frequently switching between different applications.
3. **Automated Detection:** Uses AI-based techniques to identify potentially misleading and suspicious digital content.
4. **AI-Generated Content Identification:** Helps estimate whether the analyzed text may have been produced using artificial intelligence.
5. **Time Saving:** Reduces the time and effort required for manually examining online information.
6. **User-Friendly Interface:** Provides a simple and organized interface for accessing content analysis features.
7. **Improved Information Awareness:** Helps users recognize questionable content and encourages careful evaluation of online information.
8. **NLP-Based Analysis:** Examines linguistic patterns and textual characteristics to support content authenticity assessment.
9. **Quick Result Generation:** Presents summarized analysis results through the browser extension for convenient access.
10. **Future Enhancement:** Provides opportunities to integrate advanced AI models, improved detection techniques, and additional verification features.

VII. CONCLUSION

The AuthentiScan project provides an AI-based approach to identifying potentially AI-generated and manipulated digital content. The system focuses on analyzing images and videos to recognize patterns and features that may indicate whether the content has been artificially created or altered. By applying artificial intelligence and machine learning techniques, the platform aims to support users in assessing the authenticity of digital media and improving awareness of synthetic content.

The proposed system offers a user-friendly approach to digital content verification by bringing media analysis and authenticity assessment together in a single platform. It aims to help users make more informed decisions when viewing and sharing digital information. The system also highlights the importance of identifying misleading or manipulated content in areas such as social media, journalism, cybersecurity, and online communication.

Future enhancements may include improving detection accuracy, supporting additional media formats, integrating advanced deep learning models, and providing detailed analysis reports. Further testing using diverse datasets, performance evaluation, and user feedback will help improve the system's reliability and effectiveness. Overall, AuthentiScan provides a foundation for promoting digital media authenticity, reducing the spread of misleading content, and creating a more trustworthy digital environment.

VIII. REFERENCES

[1] [1] F. Mira, "Deep Learning Technique for Recognition of Deep Fake Videos," in 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), London, United Kingdom, 2023, pp. 1–4. doi: 10.1109/GlobConET56651.2023.10150143

[2] S. Chhabra, K. Thakral, S. Mittal, M. Vatsa, and R. Singh, "Low-Quality Deepfake Detection via Unseen Artifacts," IEEE Transactions on Artificial Intelligence, vol. 5, no. 4, pp. 1573–1585, 2024. doi: 10.1109/TAI.2023.3299894

[3] T. Qiao, S. Xie, Y. Chen, F. Retraint, and X. Luo, "Fully Unsupervised Deepfake Video Detection Via Enhanced Contrastive Learning," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 46, no. 7, pp. 4654–4668, 2024. doi: 10.1109/TPAMI.2024.3356814

[4] A. Barbadekar, S. Sole, and A. Shekhavat, "Enhancing Social Media Security: LSTM-Based Deep Fake Video Detection," in 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1–6. doi: 10.1109/I2CT61223.2024.10543604

[5] D. W. Deressa, P. Lambert, G. Van Wallendael, S. Atnafu, and H. Mareen, "Improved Deepfake Video Detection Using Convolutional Vision Transformer," in 2024 IEEE Gaming, Entertainment, and Media Conference (GEM), Turin, Italy, 2024. doi: 10.1109/GEM61861.2024.10585593

[6] N. U. R. Ahmed, A. Badshah, H. Adeel, A. Tajammul, A. Daud, and T. Alsahfi, "Visual Deepfake Detection: Review of Techniques, Tools, Limitations, and Future Prospects," IEEE Access, vol. 13, pp. 1923–1961, 2025. doi: 10.1109/ACCESS.2024.3523288

[7] M. Z. Hossain, M. S. S. Samu, M. K. Bhuiyan, F. U. Zaman, and M. R. Islam, "FUSE: Unifying Spectral and Semantic Cues for Robust AI-Generated Image Detection," in 2025 28th International Conference on Computer and Information Technology (ICCIT), 2025, pp. 1409–1414. doi: 10.1109/ICCIT68739.2025.11491327

[8] W. Wei, D. Hou, S. Yin, H. Wang, C. Gao, X. Li, and Y. Liu, "High-Resolution Contrastive Framework for Generalizable AI-Generated Image Detection," in 2026 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2026. doi: 10.1109/ICASSP55912.2026.11461655

[9] T.-V. Nguyen, K. H.-A. Ngo, and K. H.-A. Ngo, "DSC2F: A Multimodal AI-Generated Image Detection System Using Dual-Stream Convolutional Neural Networks with Fast Fourier Transform," in 2026 11th International Conference on Image, Vision and Computing (ICIVC), 2026, pp. 727–731. doi: 10.1109/ICIVC70586.2026.11686669