

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 24 October 2025

Hand-in Date: 15 November 2025

Hand-in Method: Online Submission via E-Learning

Assignment Report: Literature Review – Detection System for Digital Brand Protection (Cepro Case Study)

Student ID: 253000463

Student Name: Sulaiman Fahad Alquwayfili

Table of Contents

- Summary of Research Papers
- Critical Analysis
- Connections
- Conflicts Between Findings
- Synthesis Matrix for Literature Review
- References

Summary of Research Papers

Paper 1: AI-Based Image Matching for Counterfeit Detection

This study employs convolutional neural networks (CNNs) to detect counterfeit brand logos by comparing extracted visual features to authentic samples. The research reports a high accuracy of 97%.

Limitations: Requires large datasets for proper training; cannot detect text or URL-based impersonation attacks.

PDF Link: <https://www.ijtsrd.com/papers/ijtsrd75067.pdf>

Paper 2: Domain & WHOIS Behavioral Analysis for Detecting Impersonation

This research analyzes WHOIS records and domain registration behaviors to detect domain impersonation (e.g., typosquatting).

Findings: Achieved 92% early detection capability.

Limitations: WHOIS masking reduces identification accuracy.

PDF Link:

https://informatik.rub.de/veroeffentlichungenbkip/sysec/veroeffentlichungen/2021/pdfs/2021_Digging_Deep_An_Analysis_of_Domain_Impersonation_in_the_Lower_DNS_Hierarchy.pdf

Paper 3: Detecting Social Media Impersonation Using NLP

This paper focuses on detecting impersonation on social media platforms using Natural Language Processing and behavioral signals.

Findings: High recall of 95% in detecting impersonation accounts.

Limitations: API access restrictions; limited effectiveness for image-only accounts.

PDF Link: <https://www.usenix.org/system/files/usenixsecurity24-acharya.pdf>

Paper 4: Hybrid Web Scraping + Machine Learning for Phishing Detection

This study presents a hybrid model that combines HTML/JavaScript web scraping with machine learning classification to detect phishing websites.

Findings: Achieved an F1-score of 98%.

Limitations: High computational cost; weaker performance on dynamic web pages.

PDF Link: <https://www.researchgate.net/publication/384777984>

Paper 5: AI for Digital Trademark Protection

This study reviews AI-based trademark protection methods that integrate text analysis, image analysis, and behavior-based detection.

Findings: Hybrid systems outperform traditional rule-based systems.

Limitations: Limited Arabic-language support; lack of comprehensive multi-channel protection.

PDF Link: <https://www.ijsat.org/papers/2025/3/7158.pdf>

Critical Analysis

The reviewed studies collectively highlight the growing importance of AI-driven detection in digital brand protection. CNN-based image detection is highly accurate for counterfeit logos, while NLP models offer strong performance in analyzing social media impersonation. Hybrid systems that combine multiple signals show superior performance across all research.

However, common challenges persist:

- Heavy reliance on simulated datasets instead of real-world data
- Poor support for Arabic content and right-to-left patterns
- Lack of unified solutions that cover domains + websites + social media simultaneously
- Some advanced models require high computational resources

These limitations create strategic opportunities for **Cepro**, especially in:

- Arabic-language detection
- Unified cross-channel protection
- Automated takedown pipelines
- Saudi-hosted data processing

Connections

1. All studies focus on increasing risks of impersonation and misuse of brand assets.
2. AI and machine learning form the core of modern detection strategies.
3. Hybrid systems show the strongest results compared to single-method approaches.
4. Real-time detection remains a challenge due to computational complexity.
5. Multi-source data aggregation appears consistently across studies.

Conflicts Between Findings

1. **Computer vision vs NLP:** Some studies show better performance using image analysis, others show stronger results with text/NLP models.
-

- 2. **Centralized vs distributed detection:** Approaches vary based on network architecture and target environment.
- 3. **Rule-based vs ML models:** Rule-based methods are lightweight but less accurate, while ML methods require more resources.
- 4. **Simulation vs real-world testing:** Many studies rely heavily on simulations rather than real testing environments.
- 5. **Attack coverage:** Some studies handle only image attacks, others cover domains and phishing, while others address social media impersonation.

Study	Year	Method	Key Findings	Limitations
Fake Logo Detection	2021	CNN	97% accuracy	Needs large datasets
Domain Impersonation	2021	WHOIS/DNS	92% early detection	WHOIS masking
Social Impersonation	2024	NLP	95% recall	API limitations
Hybrid Phishing Model	2024	Hybrid ML	F1 = 98%	High computation cost
AI Trademark Protection	2025	Hybrid AI	High accuracy	Weak Arabic support

Synthesis Matrix for Literature Review

References (APA 7)

Acharya, S., et al. (2024). *Exploring brand impersonation attacks on social media*. USENIX Security.

International Journal of Trend in Scientific Research and Development. (2021). *Fake logo detection using AI*.

Osman, M., He, J., et al. (2024). *Hybrid ML model for phishing detection*. ResearchGate.

Thio, W., Christiawan, R., & Wagiman, A. (2025). *AI in detecting and preventing trademark counterfeiting*. IJSAT.

Taran, V., et al. (2021). *Domain impersonation detection via DNS analysis*.