**Week 2 — Literature Survey**

* **Background**

The last several years have seen an accelerated rate of digital transformation of services in banking, education, e-governance, and in corporations, driving the need for secure and trusted digital document verification. It is normal to have humans manually carry out verification, and this is labour intensive, involves potential errors, and creates opportunities for fraud around forgery, tampering, and identity theft. In fact, the emergence of advanced image editing tools and AI-generated fakes (via deepfake technologies) has made manual verification even less reliable.

- **Existing Systems**

1. DocVerify – Automated Documents Verification System

Link:<https://www.researchgate.net/publication/392576984_DocVerify_Automated_Documents_Verification_System>

3. Mitek Systems – Document Verification with AI (2025 blog)

Link:-<https://www.miteksystems.com/blog/document-verification-with-ai?utm_source=chatgpt.com>

4. Jumio – AI Document Verification (April 2024)

Link:-<https://www.jumio.com/contact/request-information/>

6. ShuftiPro – AI Document Verification 2025

Link:- <https://backoffice.shuftipro.com/login>

7. docuexprt - AI Document Verification 2025

Link:- <https://docuexprt.com/>

* **Limitations of Existing System(s)**

1. OCR Accuracy Issues – Existing OCR tools (like Tesseract, EasyOCR) often fail when documents are noisy, blurred, handwritten, or multi-language. This reduces overall verification accuracy.
2. Forgery Detection Challenges – Many systems struggle to detect subtle tampering (e.g., replacing small text, photos, or digital signatures) especially when edits are high quality.
3. High Dependency on Templates – Some solutions rely on fixed document layouts or templates, which makes them less effective for diverse document formats.
4. Integration Problems – Blockchain, digital signatures, and proprietary vendor systems are not always interoperable, leading to adoption and scalability challenges.
5. Liveness & Anti-Spoofing Limitations – Without strong face liveness detection, attackers can bypass verification using photos, videos, or deepfakes.