IJIRIS: International Journal of Innovative Research in Information Security
Volume 11, Issue 02, April 2025
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives

Smart Template Mapping and Fraud Detection

Vijayashree HP
Assistant Professor, Vemana Institute of Technology,
Koramangala, Bangalore, India
vijayashree.hp@vemanait.edu.in
Manaswi Bharti , Mirza Mohamed Asaf
Student, Vemana Institute of Technology,
Koramangala, Bangalore, India
manaswibharti@vemanait.edu.in , mirzamohamedasaf@vemanait.edu.in

Publication History:
Manuscript Reference No: IJIRIS/RS/Vol.11/Issue02/APIS10083
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IJIRIS/RS/Vol.11/Issue02/APIS10083
Received: 02,April 2025 Revised: 14, April 2025 Accepted: 25, April 2025 Published Online: 05, May 2025, Volume 2025
Article ID APIS10082 https://www.ijiris.com/volumes/Vol11/iss-02/04.APIS10083.pdf
Article Citation: Manaswi,Mirza,Vijayshree(2025). Smart Template Mapping and Fraud Detection. International Journal of Innovative Research in Information Security, Volume 11, Issue 01, Pages 87-96
doi:> https://doi.org/10.26562/ijiris.2025.v1102.04
BibTex key: Vijayashree@2025Smart

Abstract: This paper introduces the concept of a "Sample Template Mapping and Fraud Detection" system implemented for document forgery verification software that verifies a document against a pre-defined standard template. It identifies forged changes by tracking text and structural variations and finds optimal use in the applications of HR departments, banks, and law firms. With Python and OpenCV, Tkinter, and Tesseract OCR, the system can upload templates and authenticate purported documents. I treads and validates text for in consistency and cross-verifies against a registered database. Pre-processing of images such as grayscale, Gaussian blur, and noise removal improve the accuracy of OCR, while SSIM identifies structural tampering. The system is able to identify genuine and fake documents itself and identify discrepancies in real time with a simple Tk inter- based GUI. Automated fraud detection eliminates time consumed on manual checks, minimizes the chance of errors, and maximizes the efficiency. A Tesseract OCR-based system ensures accuracy, document genuineness, and compatibility with other verification systems, and therefore, it is a vital tool to combat document forgery.

Keywords: Tesseract OCR; Computer Vision; Structural Similarity Index Measure; Database Cross- Verification; Image Pre-processing; Text Extraction and Validation; Python; Tkinter; Forgery Prevention.

I. INTRODUCTION

Document forgery has been a long-standing problem for centuries since it has progressed along with document-making skills. The forged documents were initially made by manual forgery techniques, including forgery of signatures, document alteration, and forgery of printing. With the growth in technology, the sophistication level of these crimes also rose. The availability of computer editing software, high- resolution scanners, and high-end printing technology improved the scammers' ability to tamper with official documents undetected. To combat the increasing forgery of documents, government bodies and organizations have long been incorporating such features like holograms, watermarks, microprints, and digital signatures. Yet it is unavoidable of all the shortcomings because such security features are still covered by the age-old traditional verification methods which highly depend on heavy human analysis instead of tedious, error-prone, and in efficient processes. Thus, a wide gap has been created to win a more scalable approach be gotten for a completely automated and secured solution, hence this document verification system. It employs computer vision algorithms and Optical Character Recognition (OCR) in recognizing changes in documents. Thus, unlike the manual verification, this computerized mechanism minimizes the human approach, and creates reliability as it increases the speed at which checks can be made through the use of some algorithms, such as OpenCV and Tesser act OCR while improving overall quality through the Structural Similarity Index (SSIM). This program is considered to be one of the major successes in electronic document verification-an absolute safety net for the security of very sensitive documents in the fields of human resources, finance, legal, etc., where document integrity is paramount.

II. RELATED WORKS

An article published in MIT on "Best-Buddies Similarity - Template Matching using Mutual Nearest Neighbors" introduces a new similarity measure, Best- Buddies Similarity (BBS), designed to address template matching difficulties, particularly in real-world scenarios where templates are subject to non-rigid deformations, occlusions, and background clutter. Traditional template matching methods, e.g., Sum of Squared Differences (SSD), Sum of Absolute Differences (SAD), and Normalized Cross-Correlation (NCC), fail under such scenarios since they match all the points in the template, including the background regions. BBS prevents such deficiencies by taking into account Best-Buddies Pairs (BBPs), mutual nearest neighbor point pairs between the target image region and the template.

This renders BBS outlier-robust, non- parametric, and capable of dealing with complex geometric transformations without any object deformation model knowledge. The authors lay down a solid statistical groundwork for BBS, showing that it hit speak similarity when the points from both sets come from the same distribution.[1] The paper titled "Document Image Matching Using a Maximal Grid Approach" introduces a method for automating the matching of scanned document forms through this Maximal Grid Approach. This technique efficiently processes standard forms like insurance claims and tax returns by trimming away all the horizontal and vertical lines to create a strong grid- based framework.[2] The text is organized into cells created by the intersecting lines, forming a frameset. A similarity algorithm then computes the similarity between forms by a distribution of these cells, which can yield scores of 0 (no similarity) or 1 (identical). It scales similarity for the ranking of documents based on how well they express a particular query.

	Matching Cases				Not
	1-to-1	1-to-N	M-to-1	M-to-N	Matching
Quality	High	Medium	Medium	Low	Very Low
QATM (s,t)	1	$1/N$	$1/M$	$1/MN$	$1/\|\|T\|\|\|\|S\|\| \approx 0$

Table 1: Template matching cases and ideal scores.

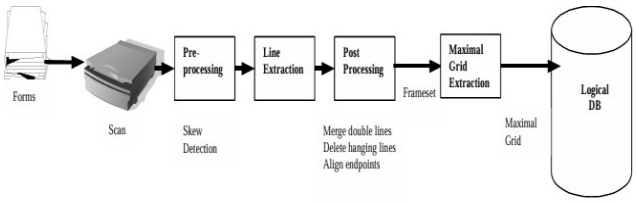

Figure 1. Schematic of the proposed approach for form representation

The process starts with scanning and detecting any skews with methods like the Hough Transform and Canny Edge Detection, then goes on to extract the frames and build a maximum grid. The similarity score is then based on how well the cells are distributed in the two respective row and column slots. This method is very good for addressing layout changes and increasing computation time, compared to the other existing techniques. The algorithm can handle low-quality scans, skewed images, and line breaks, all the while speeding up large- form processing. It's particularly well-suited for automatic document recognition and recovery within Extensive databases. Experimental findings show that it achieves high accuracy and quicker computation than existing methods. Additionally, the maximal grid method offers a strong and efficient approach for matching document images, effectively managing variations and issues related to scan quality. Looking ahead, future research will focus on applying the algorithm to more diverse data sets and incorporating text layout analysis to enhance recognition capabilities. This method is grounded in reliable techniques like the Hough Transform and Canny Edge Detection, making significant strides in both form recognition and document image processing. Using a soft-ranking system to evaluate the uniqueness of matches, the research article "QATM: Quality-Aware Template Matching for Deep Learning" offers a fresh template matching technique that beats conventional techniques. By balancing between similarity and novelty, QATM addresses several matching scenarios 1-to-1, 1-to-many, and many-to- many unlike conventional techniques depending just on similarity scores. Being an independent algorithm and a trainable layer for deep neural networks (DNNs), QATM is efficient, differentiable, and readily included into present models. Using cosine similarity and SoftMax ranking, QATM calculates the probability of the match from either the template or search picture side, therefore generating superior and unique matches. Studies reveal that QATM is more accurate and efficient than present state-of- the-art technologies including BBS, DDIS, and CoTM especially for negative samples without any desired match. Aside from template matching, QATM outperforms image-to-GPS verification by verifying whether an image matches a specific GPS location using reference panorama images. [3] It outperforms semantic image alignment (SIA) in more accurate object feature alignment, which outperforms methods like GeoCNN and SCNet in tasks like PF-PASCAL. In a nutshell, QATM can be best understood as really accurate and stable but flexible at the same time, allying up to 10 times faster performance on GPUs, which makes it suitable for just about any computer vision application- object recognition, image alignment, visual verification, and so forth. A paper titled Document Image Layout Comparison and Classification was written to explain a raster layout comparison and classification on spatial layouts of document images without the use of OCR. Interval encoding, that is ,a fixed-length vector representation of the layout for efficient comparison through Manhattan distance, is suggested by the authors. Their technique will complement document retrieval as well as categorization and early classification. Generalization involves three methods for distance computation: edit distance, accurate but slower results; interval distance, much faster with almost equivalent accuracy to edit distance; and cluster distance, quicker due to the classification process utilizing k-means clustering. The algorithm segments documents into grids, computes the row distances, and then realigns them via dynamic programming. Experiments were performed on five document types - letters, journals, and magazines, and found interval and cluster distance to be as accurate as edit distance, but with lower computational cost. A Hidden Markov Model (HMM) was also very accurate at classification, except for two-column letters because of layout differences. [4] In short, interval encoding is a high- speed, accurate layout-based document comparison and classification method applicable to document management and information extraction without OCR.

III. TECHNOLOGY USED

In order to create a robust and efficient fraud detection system for document verification, we have made use of a combination of latest technologies and frameworks. The system employs the following pioneering technologies:

1. **Python:** This is the main programming language for developing this system due to its massive libraries and simplicity. Python has the support of many frame works including OpenCV for image processing, Tkinter for GUI, and Tesser act OCR for optical character recognition.
2. **OpenCV:** OpenCV is a completely free and open- source computer vision library that used all its functions to perform operations on images like Grayscale conversion, noise removal, structure similarity measure among others. There is no scenario where edge detection or contour detection becomes vital, except using OpenCV functions on images. These activities should be vital in template matching or forgery detection.
3. **Tesseract OCR:** This implies a significant package for Optical Character Recognition to read text from scanned documents or images. It can process multilingual and customizable datasets for document text recognition and further customizes setting training datasets if the documents consist of specific type fonts or handwritten entries.[5]
4. **Tkinter:** The quite light weight Python GUI tool kit, used in developing the user-friendly interface of this application. Therefore, the users will be able to upload documents through this Tkinter, view the verification results, and report the fraud detection.
5. **Structural Similarity Index Measurement (SSIM):**This index looks for similarities in a given document that help to spot very minute differences in the same document. The changes measured are structural, luminance, and contrast with the differences bringing out some fine forgery identification.
6. **Database Cross Verification:** A database has now been defined for official purposes which will ensure that original templates are stored, retrieved and cross-verified against any new documents uploaded. SQL and NoSQL framework were applied in this process to cross-verify and fetch stored templates on time.
7. **Relevant Machine Learning:** Any relevant machine learning technique or techniques that would be used to improve accuracy in OCR and enhance detection of mismatched text data. This would include CNNs, NLP algorithms, and other ML techniques used for anomaly detection and classification.
8. **Image pre-processing techniques:** The purpose of pre-processing techniques is to include thresholding preceded by Gaussian blur, morphological processes, and adaptive binarization applied to correct scanned image qualities that subsequently feed the OCR process.
9. **RIX Algorithm:** The RIX algorithm is a work package under this project for the Fraud Detection Module that basically does template matching between an original document (standard template) and a claimed document for the checking of tampering or changes made for fraudulent purposes. It inspects the same titled template, present in both documents, and flags any discrepancies or changes.

IV. PROPOSED METHODOLOGY

The process to be adopted is precise, effective, and real-time for fraud detection. The system process is step-by- step to authenticate documents and identify counterfeit content. The step-by-step process is as follows:

1. **Initialization of System and User Interface:** The initial opening and start of the DOC-U- MATCH-RIX system occurs along with the beginning of the Graphical User Interface (GUI)to be loaded. The GUI has been designed for user-friendly interaction with the tool. No users are uploading documents for some of the verification requirements, but they have a number of functions and a fairly intuitive design systems where it would be easy to browse the results of the document authentication procedure by someone who has a little experience with software operations.
2. **Open the standard template document:** The initial step in the procedure for document verification is to upload the template document. This template document will be the reference document against which all other documents are measured. This template is usually government issued documents, authenticated documents such as identity cards, contracts, or financial certificates. These documents are indeed very crucial, as they will stand as a yardstick whose authenticity will greatly contribute to the accuracy and reliability of the verification process. Once the template is uploaded into the system, it remains there in the repository for other future comparisons.
3. **Upload documents for debate for Verification:** This also allows users to upload claimed documents currently being verified, other than selecting a standard template.These documents need investigations; authenticating one or more documents may be required. The system permits multiple file uploads to allow organizations to run bulk processes into the system, benefiting the efficiencies involved in processing verifications. Therefore, the system should integrate document authentication handling of more than one file to maximize scalability and availability and reduce lead times.
4. **Preprocessing Documents through Image Processing:** OpenCV image preprocessing strategies are used to enhance the evenness and accuracy just before the verification process actually begins. The first step in preprocessing is grayscale conversion, whereby the entire colour information of the document is without return stripped off to obtain a pure form of the structure for easy comparison.[6] The next series of processes is Gaussian blurring, which assesses noise and gives a clear output text from the OCR engine. Thresholding finally separates the part of the text from the background, giving further contrast for the extraction of only relevant information. All these preprocessing steps intend to purify and disqualify distortion, and they work quite well in a much more accurate text recognition system.
5. **Text Extraction via Optical Character Recognition (OCR):** Tesseract executes preprocessing of text extraction from both a standard template and claimed documents.
6. OCR implies the process of transforming textual information present in an image into a common machine-readable format for interaction by a system with them. The user saves the extracted text through several mouse clicks and keystrokes in multiple file formats for purposes of comparison.[5] This proves to be a very important stage of converting physical document formats to electronic for review: manipulation, inconsistency, or lack of data.

7. Extraction Text Comparison with Standard Template: After this process extracts text, the system then analyses the comparison of the texts to determine whether any words were added, deleted, or changed within the documents compared. Such comparison studies will compare the standard template with extracted text from the claimed document. Even a mere date change or modified name or changed clause will be a sign of fraud. These differences can thus be reviewed with ease by anyone flipping through the document and can act, therefore, in decision-making regarding suspected tampering.

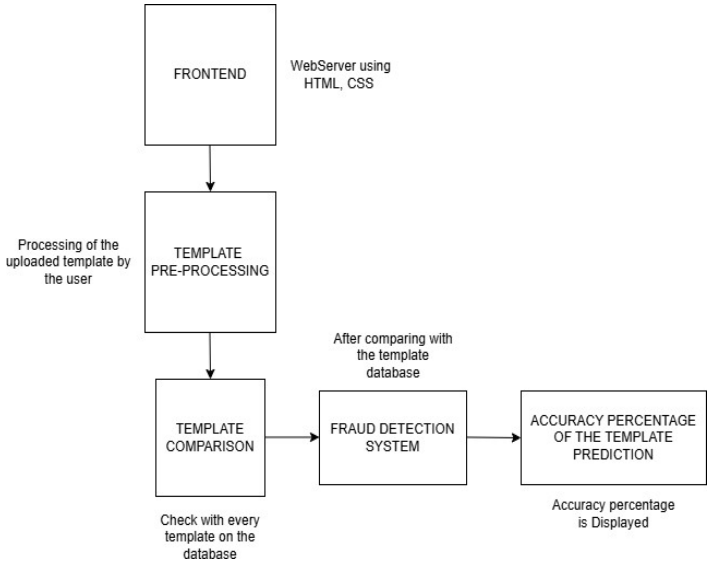

Figure 2. Frame work for Template Preprocessing with Accuracy Evaluation

8. The establishment of Layout Analysis to Detect Structural Divergence: Aside from text verification, the document analysing system can perform layout analysis for detecting structural variation in the self-proclaimed document. The Structural Similarity Index (SSIM) and Contour Detection of OpenCV are used by the system to examine the placement of logos and signatures, stamps, and text formatting. Any modifications made to such visual elements are marked by red boundary boxes, which will instantly tell users of its mutability. This allows forgery detection even if the forgery affects the physical visual structure of the document.

9. Validating Information Against a Company Database: To further strengthen the verification process, the extracted text from the claimed document is cross- checked against a company database stored in a CSV file. The abovementioned database contains an account of all company-aligned user accounts, including but not limited to employees, customers, or authorized representatives. In case they said document bears a name that does not correspond with any company database record, it becomes a suspect document as per the validation criteria considered in the checking. Therefore, the document is properly shaped, containing real living persons' names who are eligible to own such documents.

10. Final Decision Concerning Document Authentication: Finally, the global judgment of authenticity of the document is given by the system based on text comparison, layout analysis, and authentication against company records. If there is an anomaly in the text, then there is at least an anomaly in the structure, and if there is a mismatch against company records detected by the system, it is flagged an attempt at forgery. But if it is certain for the document to have been tampered with, then it is touted as forgery.[7] Ultimately, the automation of the entire decision-making process renders the effort required by a human to be extremely low and the reliability of fraud detection to be very high.

11. Segregation of Genuine and Fraudulent Documents: After the system classifies a document, it will be routed to a specific folder according to its classification. The path for fraudulent documents goes directly into the fraud folder for further inspection or to serve as evidence for the investigation. The legitimate ones are safely secured in a genuine folder for the purposes of record-keeping. Such organization provides an efficient mechanism for storing verified documents and easy retrieval and review by users.

12. Generating a Summary Report for User Review: At the end of the verification process, the system generates a summary report displaying the results of document authentication. The report provides details such as the total number of verified documents, the number of fraudulent cases, and the specific modifications detected. Fraudulent documents that have been flagged with red markers are displayed in the GUI, allowing users to review them in real time. This reporting feature helps organizations make informed decisions based on the verification results.

13. Completion of the Verification Process: Once the verification process is completed, the system returns to the main interface, ready for a new batch of documents. Users can upload additional documents and repeat the process as needed. This ensures that the system is continuously available for document authentication. The entire workflow is designed to be fast, accurate, and user-friendly, reducing manual effort while increasing efficiency in detecting forged documents.

V. RESULT

Figure 3. Select a Standard Template and Claimed Document

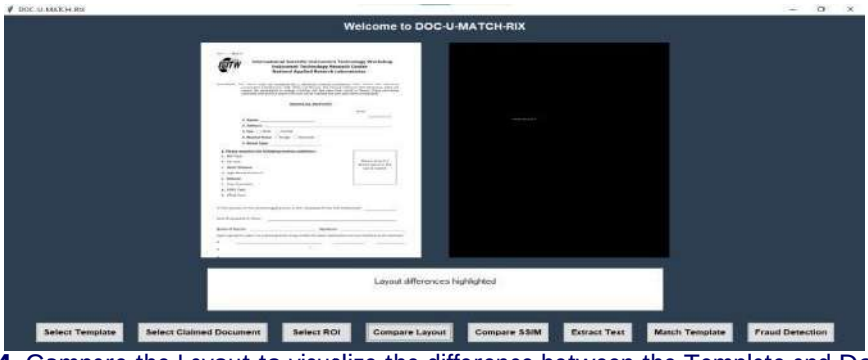

Figure 4. Compare the Layout to visualize the difference between the Template and Document

Figure 5. Structural Similarity Index Measure (SSIM) for Genuine Document

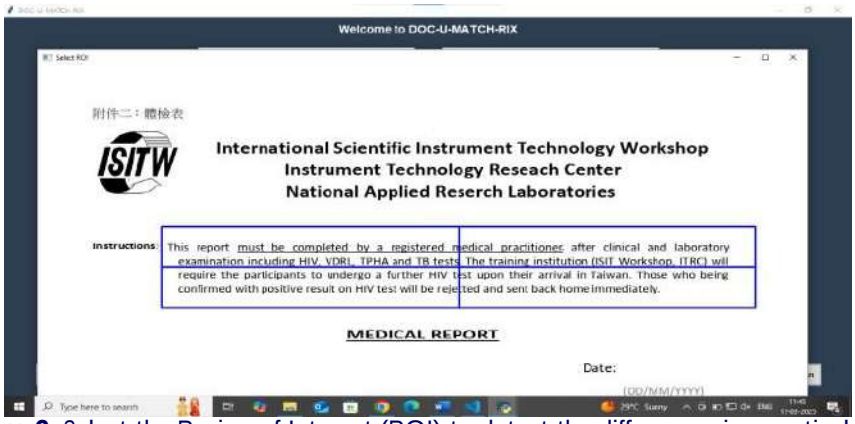

Figure 6. Select the Region of Interest (ROI) to detect the differences in a particulate area

Figure 7. Extracted Text displayed after selecting ROI (By pressing "SPACEBAR" or "ENTER")

Figure 8. The system compares Documents with a Predefined Template and Displays "Template Matched" if identical

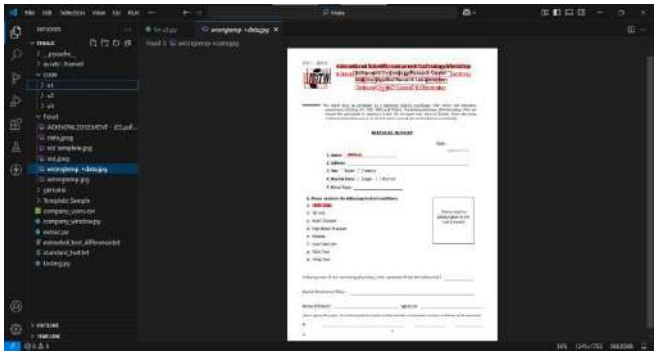

Figure 9. If the Template matches, the system confirms "No Fraud Detected"

Figure10. Fraudulent Document with Highlighted Discrepancies

VI. CONCLUSION

The Smart Template Mapping and Fraud Detection System offers an elaborate, fully automated solution for document verification, well aware of the rising forgery threats, with accuracy and efficiency. It works with text extraction via Tesser act OCR, structural analysis using Structural Similarity Index Measure, advanced image preprocessing techniques to detect tampering and text inconsistency.

Python, OpenCV, and Tkinter are used to build a platform that is friendly, scalable, fast, and capable of real-time authentication. With automated text checks, structural checks, and cross-verification from databases, this system does not require much manual intervention, thus giving an accurate answer in fraud detection. Since it can detect minute changes in the layout and content of a document, greater security is offered in those industries that require document integrity, such as banking and finance, human resources, and legal services. This provides for a marked improvement in the efficiency, reliability, and prevention of fraud, all due to a lowered reliance on traditional manual verification; thus, this system is a great aid for modern-day document authentication.

REFERENCES

1. T.Dekel, S.Oron, S.Avidan, M.Rubinstein, and W. Freeman, “Best buddies similarity for robust template matching,” in Computer Vision and Pattern Recognition (CVPR), 2015IEEE Conference on. IEEE, 2015.
2. Tzacheva, Y. El-Sonbaty, and E. A. El-Kwae, "Document image matching using a maximal grid approach," in Proceedings of SPIE - The International SocietyforOpticalEngineering,vol.4670,Dec.2001, pp.121-128.doi:10.1117/12.450721.
3. J. Cheng, Y. Wu, W. Abd-Almageed, and P. Natarajan, "QATM: Quality-Aware Template Matching for Deep Learning," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 11545-11554. https://doi:10.1109/CVPR.2019.01182.
4. J.Hu,R.Kashi,andG.Wilfong," Document image layout comparison and classification," in Proceedings of the International Conference on Document Analysis and Recognition (ICDAR), Sep. 1999, pp. 1-6.
5. S. Dome and A. P. Sathe, "Optical Character Recognition using Tesseract and Classification,"2021 International Conference on Emerging Smart Computing and Informatics (ESCI),Pune,India,2021, pp.153-158, https://doi:10.1109/ESCI50559.2021.9397008.
6. H. Peng, F. Long, and Z. Chi, "Document Image Recognition Based on Template Matching of Component Block Projections, " IEEE Transactions on Pattern Analysis and Machine Intelligence, vol.25,no. 9, pp.1188-1192, Sept.2003.
7. Y. Sun, X. Mao, S. Hong, W. Xu, and G. Gui, "Template Matching-Based Method for Intelligent Invoice Information Identification," IEEE Access, vol. 7,pp.28392-28401,Feb.2019, https://doi:10.1109/ACCESS.2019.2901943.