Immigration Document Classification and Automated Response Generation

Sourav Mukherjee¹, Tim Oates², Vince DiMascio³, Huguens Jean², Rob Ares⁴, David Widmark³, and Jaclyn Harder³

¹Fairleigh Dickinson University, Vancouver, Canada. Email: sourav.mukherjee.8@gmail.com
²Synaptiq, USA. Email: {tim.oates, huguens.jean}@synaptiq.ai
³Berry Appleman & Leiden LLP, USA. Email: {vdimascio, dwidmark, jaharder}@balglobal.com
⁴Independent, USA. Email: rob@hireredrectangle.com

Abstract—In this paper, we consider the problem of organizing supporting documents vital to U.S. work visa petitions, as well as responding to Requests For Evidence (RFE) issued by the U.S. Citizenship and Immigration Services (USCIS). Typically, both processes require a significant amount of repetitive manual effort. To reduce the burden of mechanical work, we apply machine learning methods to automate these processes, with humans in the loop to review and edit output for submission. In particular, we use an ensemble of image and text classifiers to categorize supporting documents. We also use a text classifier to automatically identify the types of evidence being requested in an RFE, and used the identified types in conjunction with response templates and extracted fields to assemble draft responses. Empirical results suggest that our approach achieves considerable accuracy while significantly reducing processing time.

I. INTRODUCTION

Preparing a U.S. work visa (e.g., H-1B, TN) petition requires compiling a large number of supporting documents, e.g., passport and visa pages, driver’s license, I-797 [1], I-797C [2], Employment Authorization Document [3], certificates, transcripts, and so on. Any immigration law firm retained by a large corporation may need to simultaneously pursue hundreds of such applications, resulting in a plethora of documents that must be systematically stored and handled. While document categorization is a necessary first step, relying entirely on humans for this does not scale with data volume. Moreover, categorization of the above document types is generally a mechanical process that does not require ingenuity, and therefore is a good candidate for automation. However, these documents are usually provided by beneficiaries of the petitions as scanned files and facsimiles of varying image quality, thereby making optical character recognition (OCR) difficult. Consequently, automatic classification of these documents based on textual content alone is error prone. We argue that classification can be made more accurate by relying on content as well as appearance. Therefore, we adopt a novel approach of employing an ensemble of classifiers, one based on textual content, and another based on visual content, for classifying supporting documents.

Once a petition has been submitted, the office of U.S. Citizenship and Immigration Services (USCIS) frequently requests additional supporting information by sending a Request For Evidence (RFE) to the petitioner. An RFE may be issued based on any one or more of the reasons listed by USCIS in [4]. E.g., USCIS may ask for more clinching evidence that the beneficiary is seeking to work in a specialty occupation, or that the beneficiary is qualified for the position, among others. In this paper, we refer to every such reason as an RFE attack. To successfully respond to the RFE, the law firm preparing the petition reviews the RFE to identify every RFE attack contained therein. Thereafter, the firm compiles a response that addresses every attack with supporting information and documents. Typically, this process is entirely manual and time consuming. However, RFEs with the same types of attack often have similar language. E.g., RFEs for two beneficiaries seeking to work as Computer Systems Analysts (Specialty Occupation Code, SOC : 15-1211; see [5], page 18), may both ask for proof that the beneficiary has a baccalaureate or more advanced degree, that such a degree is necessary for performing the job, that the employer typically requires this qualification for the position, and so on. Unsurprisingly, the responses to these RFEs also tend to have similar language. Therefore, response templates are often used to avoid having to author each response from scratch. Once all RFE attacks have been identified, the next steps consist of selecting response templates, inserting beneficiary-specific information into the templates’ placeholders, and compiling the filled templates into a draft response ready to be reviewed by a lawyer, who then modifies the content based on domain expertise prior to sending the response to USCIS. We explore whether this workflow is suitable for partial automation, not to obviate human experts, but rather, to automate rote work, thereby freeing up more time for them to fine tune responses strategically. Since RFEs originate from a single source, namely, USCIS, variability in scan quality is lower compared to those of supporting documents discussed in the previous paragraph, making RFEs more amenable to text extraction through OCR. We demonstrate that automatic identification of attack types within an RFE is indeed possible by training classifiers based on textual content. We further show that the identified attack types, together with data extracted from the RFE and queried from a beneficiary database, may be used to identify appropriate response templates and populate the
templates’ placeholders, resulting in a draft response ready for human review. Empirical results indicate that the above automation reduces manual effort and improves turnaround time substantially while achieving high accuracy.

The rest of this paper is organized as follows. Section II reviews related work while Section III describes our novel contributions. Section IV provides empirical evidence in support of our approach while V interprets the results. Finally, Section VI concludes this paper.

II. RELATED WORK

Applications of machine learning techniques to problems in the legal domain have become increasingly popular in recent years. Specific areas where machine learning has been applied include outcome prediction, e-discovery, document categorization, contract review/due diligence, automated document assembly, information retrieval, document translation, legal analytics, and so on. In this section, we briefly review research relevant to our work. For more comprehensive surveys, please refer to [6–8].

A. Outcome Prediction

The Supreme Court Forecasting Project [9] used classification trees with six input parameters, namely, circuit of origin, issue area, petitioner type, respondent type, whether the lower court ruling was pro-liberal or pro-conservative, and whether the unconstitutionality of a practice was included in the petitioner’s argument, to predict U.S. Supreme Court outcomes. Another classification tree approach to the same problem was reported in [10]. In [11], random forest classifiers were used to predict U.S. Supreme Court outcomes over a much broader time window, namely, from 1816 to 2015.

Similar predictive models have been explored in other legal jurisdictions as well. For example, support vector machine (SVM) classifiers were trained on data from European Court of Human Rights cases to predict violation of human rights convention articles; the training data in these cases was textual, featurized using n-grams and topics (word clusters) in [12], and using TF-IDF vectorization on n-grams \( n \leq 4 \) in [13].

B. E-Discovery

Given a legal matter and a large collection of documents, e-discovery refers to the process of identifying those documents that are most relevant to the matter, and filtering out irrelevant documents. This process is also sometimes referred to as predictive coding or technology assisted review [6]. Viewing e-discovery as a binary classification problem allows the application of standard supervised learning algorithms to address it. In [14], the performance of several such algorithms, namely, support vector machine (SVM), logistic regression, XGBoost, multi-layered perceptron (MLP), and 1-nearest neighbor, have been compared on a standard e-discovery benchmark. One of the challenges in e-discovery is the shortage of labeled data. While the volume of electronically stored documents has grown by orders of magnitude, it is unrealistic to expect the number of human labeled examples to grow at the same rate. As a result, iterative training protocols have been used that begin with a labeled seed dataset (obtained using a keyword search or random selection) for training a classifier, and then gradually augment the labeled training dataset and retrain. Three well known protocols, namely, Continuous Active Learning (CAL), Simple Active Learning (SAL), and Simple Passive Learning (SPL) are compared in [15].

C. Document Categorization

Even after filtering out irrelevant documents through e-discovery, the number of documents that need to be reviewed for a case may be in the hundreds. Therefore, organizing large sets of documents into manageable categories is essential. To address this problem, both supervised approaches that assume document categories to be known \textit{a priori} [16–19], and unsupervised approaches where documents are clustered based on similarity without any prior knowledge of categories [20–22], have been proposed.

D. Legal Drafting

Since legal documents of the same kind often tend to use similar language, law firms frequently use templates with placeholders for drafting new documents by populating the templates’ placeholders with appropriate values. For example, contracts between service providers and customers/clients often tend to include similar clauses. Unsurprisingly, automated legal drafting, also known as automated document assembly, has been an active area of research for at least the past three decades [23]. As of this writing, machine learning based approaches to drafting are viewed as promising [24, 25].

To the best of our knowledge, there is no published work on machine learning approaches to documents related to immigration petitions. Unlike existing document categorization approaches, we adopt an ensemble approach for classifying supporting documents based on content (i.e., text classification) as well as appearance (i.e., image classification). While existing approaches to legal outcome prediction use classifiers that predict outcomes based on featurized (i.e., vectorized) text, we use text similarity between the RFE document and known text fragments to predict the presence of an attack type. Unlike existing legal drafting approaches, our goal is to draft responses to RFEs as opposed to legal contracts.

III. METHODOLOGY

Formally, we define the following problems.

A. Problem Statement

- **P1 (Supporting Document Classification).** Let \( C \) be a finite, known set of document classes, and dataset \( \mathbb{D}_1 = \{(x, y) : x \text{ is a document, } y \in C \text{ is its unique class}\} \). Given any new document \( x \), calculate the probability \( P(y|x) \) that the document belongs to class \( y \) for every \( y \in C \).

- **P2 (RFE Attack Identification).** Let \( A \) be a finite, known set of RFE attack types, and dataset \( \mathbb{D}_2 = \{(x, y) : x \text{ is a Request For Evidence (RFE), } y \in \)
\( \mathcal{P}(A) - \emptyset \) is a nonempty set of attacks}, where \( \mathcal{P}(\cdot) \) denotes power set. Given a new RFE document \( x \), predict the set of attacks \( y \) contained therein.

- **P3 (RFE Response Generation).** Suppose the \( B \) is the beneficiary of a petition, and \( \text{data}(B) \) represents data about the beneficiary available to the petitioner. Suppose \( y \in \mathcal{P}(A) - \emptyset \) is the set of RFE attacks identified in an RFE issued to the beneficiary. Generate a response draft based on \( y \) and \( \text{data}(B) \).

### B. Approach: Supporting Document Classification

Recall from Section [I] that the supporting documents for a work visa petition are usually received by the law firm from the beneficiary as scans or facsimiles of varying image quality. As a result, text extraction using optical character recognition (OCR) is error-prone, which may reduce the accuracy of a classifier based on textual content alone. To address this challenge, we use an ensemble of two classifiers, namely an image classifier that considers the appearance of a page, and a text classifier that considers its textual content. Figure 1 depicts the process of training these classifiers based on the same training dataset.

1) **Training the Image Classifier:** To train the image classifier, we convert each document in the training dataset into a set of images, one image per page, resulting in a dataset of labeled images, which are fed as training data to a convolutional neural network (CNN) classifier. Since training a CNN to learn visual features from scratch requires huge volumes of training data, CNN-based image classifiers frequently rely on transfer learning [26], with lower level feature extractors pretrained on a different, much larger dataset, and higher level layers trained on the dataset of interest. Following this approach, we use the VGG-16 [27] architecture trained on the ImageNet dataset [28], but excluding the final decision layer, as feature extractor. The weights of this CNN are frozen, i.e., never changed. We then append a fully connected decision layer to this CNN, and an output layer of size \(|C|\). The weights of this final decision layer are trained using labeled, featurized images, whereas the features themselves are extracted by the pretrained CNN.

2) **Training the Text Classifier:** To train the text classifier, we first use optical character recognition (OCR) to extract text from the documents, and then tokenize the text by splitting by whitespace. Once a document has been tokenized, we represent it as an \( n \)-gram vector \((n \in \{2, 3\})\) weighted by term frequency-inverse document frequency (TF-IDF). Since Support Vector Machines (SVM) are known to achieve high accuracy in classifying text based on sparse vector representations [29], we use the resulting labeled feature vectors to train an SVM classifier.

3) **Predicting Document Type:** Given a new document \( x \), the ensemble model estimates the probability \( P(y|x) \) that the document belongs to class \( y \), for every \( y \in C \), as shown in Figure 2. Taking \( x \) as input, the image classifier calculates

\[
\{P_{\text{image}}(y|x) : y \in C\}, \text{ i.e., its estimates of the document belonging to class } y \text{ for every } y \in C. \text{ The entropy of this distribution is given by}
\]

\[
H_{\text{image}}(x) = - \sum_{y \in C} P_{\text{image}}(y|x) \log (P_{\text{image}}(y|x))
\]

![Fig. 1. Training image classifier and text classifier based on labeled supporting documents.](image1)

![Fig. 2. Prediction of document type by ensemble classifier.](image2)
where \( \lg(.) \) denotes logarithm to the base 2. Similarly, the text classifier calculates its own estimates \( \{ P_{\text{text}}(y|x) : y \in \mathcal{C} \} \) with entropy

\[
H_{\text{text}}(x) = - \sum_{y \in \mathcal{C}} P_{\text{text}}(y|x) \log(P_{\text{text}}(y|x))
\]

We quantify the confidence \( w \) of a classifier as the reciprocal of the above entropy. Thus,

\[
w_{\text{image}}(x) = \frac{1}{\max(H_{\text{image}}(x), \epsilon)} \quad (1)
\]

and

\[
w_{\text{text}}(x) = \frac{1}{\max(H_{\text{text}}(x), \epsilon)} \quad (2)
\]

where \( \epsilon = 0.001 \) is a small constant. To avoid divide-by-zero errors, \( \max(H_{\text{image}}(x), \epsilon) \) and \( \max(H_{\text{text}}(x), \epsilon) \) are used in the denominator instead of \( H_{\text{image}}(x) \) and \( H_{\text{text}}(x) \). Finally, the class probabilities estimated by the ensemble are calculated as follows:

\[
P(y|x) = \frac{w_{\text{image}}(x) P_{\text{image}}(y|x) + w_{\text{text}}(x) P_{\text{text}}(y|x)}{w_{\text{image}}(x) + w_{\text{text}}(x)} \quad (3)
\]

C. Approach: RFE Attack Identification

Recall from Section I that the office of U.S. Citizenship and Immigration Services (USCIS), in response to a work visa petition, frequently requests additional information by sending a Request For Evidence (RFE) to the petitioner, to establish more conclusively that, e.g., the beneficiary is seeking employment in a specialty occupation, has the necessary qualification, and so on. In this paper, we use the term RFE attack to refer to reasons for issuing an RFE; the set of all possible reasons is listed in [4]. The first step in producing a successful response is to identify all the RFE attacks contained within an RFE. In this section, we address this problem.

Since all RFEs originate from a single source, namely, USCIS, there is greater consistency in scanned image quality. Consequently, RFEs are more amenable to OCR based text extraction. We find textual content thus extracted to be useful in attack type identification. On the other hand, the visual content, i.e., appearance, of an RFE does not vary across different attack types. Therefore, image classification is not a suitable approach for this problem. Figure 3 depicts the workflow for identifying RFE attacks contained in a document. The starting point is an RFE document, \( x \). The historical data used for predicting attack types consists of a set \( \mathcal{E} \) of example sentences previously found in these types of attacks. The expectation is not that sentences identical to these example sentences will appear in the new RFE, but that semantically similar sentences may occur. Textual content, extracted using OCR, is preprocessed by converting text to lowercase, and removing stopwords, numeric information, and non-English characters. The preprocessed text is then split by one or more newlines yielding a set of sentences. After vectorizing both the RFE sentences and the example sentences to TF-IDF weighted \( n \)-gram representation (\( n \in \{1, 2, 3\} \)), we compute pairwise cosine similarities between every RFE sentence and every example sentence, resulting in a cosine similarity matrix. Finally, we predict that an attack is present in document \( x \) if there is at least one sentence \( s_1 \in \mathcal{A} \) and at least one sentence \( s_2 \in \mathcal{E} \) such that the cosine similarity between their vectorized representations is greater than a pre-defined threshold \( \tau \) (we set \( \tau = 0.6 \) through manual tuning). For every such example \( s_2 \), we say that the attack represented by \( s_2 \) is present in the document. In other words, the decision rule is given by:

\[
(\forall a \in \mathcal{A})[\exists s_1 \in x, s_2 \in \mathcal{E}][(\text{sim}(s_1, s_2) > \tau)] \Rightarrow (\text{attack}(s_2) \in \text{attacks}(x)) \quad (4)
\]

where \( s_1, s_2 \) are TF-IDF weighted \( n \)-gram vector representations of sentences \( s_1, s_2 \), \( \text{sim}(., .) \) is the cosine similarity metric

\[
\text{sim}(s_1, s_2) = \frac{s_1 \cdot s_2}{|s_1||s_2|}
\]

\( \text{attack}(s_2) \) is the attack type of example sentence \( s_2 \), and \( \text{attacks}(x) \) is the set of attacks contained in the document \( x \). Identification of RFE attack types in a document makes
automated drafting of the response possible, as we discuss next.

D. Approach: RFE Response Drafting

Figure 4 depicts the workflow for drafting a response to an RFE, which assumes that the workflow for RFE attack type identification discussed in the previous section has already been completed. For preparing a response draft, we do not remove any stopwords or symbols from the text extracted using OCR, since these may be useful in extracting fields from the RFE. We find several essential fields to be readily extractable from RFEs using regular expression matching: these fields include case number, employee name, employer name, attorney name, date of the RFE, due date of the response, and so on. These fields are used to query a database containing additional data about the beneficiary, such as specialty occupation code (SOC) [5], field of study, degree received, name of institution, and so on. Extracting the above pieces of data from the RFE and the database is necessary for two reasons. First, determining which templates to select may depend on certain field values in addition to attack types; e.g., for attacks of type specialty occupation, different specialty occupation codes [5] require different response templates. Second, this data is also used to populate template placeholders. Once templates have been selected based on detected attack types and extracted fields, and placeholder values have been populated, these filled templates are concatenated and a preamble is added, resulting in a response draft ready for expert review. The next section presents empirical results.

IV. Evaluation

To empirically validate our approach, we use real-world end-to-end workflows used at a large law firm, and execute the workflows with and without the partial automation methods described in Section III using validation data that is completely disjoint from training data. Comparison of the total execution times with and without automation helps us quantify the advantage of our approach. We also report predictive accuracy scores. The following tools were used: (a) programming language: Python 3, (b) optical character recognition: Tesseract OCR [30], (c) SVM and logistic regression: scikit-learn [31], and (d) CNN: Keras [32] with Tensorflow [33].

A. Supporting Document Classification

1) Experimental Setup: Figure 5 depicts the workflow for supporting document classification, and consists of opening an uncategorized document, classifying it, and placing the document in a folder determined by its category. In the approach being evaluated, each of the above steps is automated. In the baseline, each step is manual.

2) Results:

a) Accuracy: Prediction accuracy for the above dataset is shown in Table I. Of the 104 documents used in the above evaluation, 102 were correctly classified, resulting in a prediction accuracy of 98.08%. Of these 104 documents, all
33 out of 33 I-797 approvals were correctly classified, whereas 69 out of 71 I-797 receipts were correctly classified.

| Document type  | Count | Correct prediction count | Accuracy (%) |
|----------------|-------|--------------------------|--------------|
| All            | 104   | 102                      | 98.08%       |
| I-797 Approval | 33    | 33                       | 100%         |
| I-797 Receipt  | 71    | 69                       | 97.18%       |

**TABLE I**

**ACCURACY OF SUPPORTING DOCUMENT CLASSIFICATION.**

b) Processing Time.: Figure 6 compares histograms of processing time (measured in seconds) using the manual and automated document classification workflows, while Table II compares their means, medians, standard deviations, minimum and maximum values.

![Histograms of document classification time](image)

**Fig. 6.** Histograms of document classification time (in seconds) using manual and automated workflows.

|                | Manual | Automated |
|----------------|--------|-----------|
| mean (seconds) | 196.87 | 144.98    |
| median (seconds) | 187.5 | 135.0     |
| standard deviation (seconds) | 79.66 | 36.37     |
| min (seconds) | 104    | 75.6      |
| max (seconds) | 532    | 240       |

**TABLE II**

**COMPARISON BETWEEN PROCESSING TIMES OF MANUAL AND AUTOMATED DOCUMENT CATEGORIZATION WORKFLOWS.**

B. RFE Attack Type Classification and Response Generation

1) Experimental Setup: Figure 7 depicts the workflow for responding to an RFE, consisting of opening the document, determining attack types based on textual content, extracting data from the RFE and beneficiary database, selecting response templates based on the attack types and extracted data, populating template placeholders with the values, and assembling the response. We compare the performance of manual and automated implementations of this workflow. A test set of 49 RFEs containing various types of attacks was selected. The frequency distribution of attacks in this set is depicted in Figure 8. As seen in this figure, the predominant attack type is specialty occupation, which is unsurprising since H-1B visa is only applicable to such occupations [34]. Although our RFE attack classifier can classify a broad range of attacks, in this paper, we only focus on specialty occupation attacks.

2) Results:

a) Accuracy.: Accuracy results for detection of specialty occupation attacks are presented in Table III. Here, a correct prediction refers to a scenario where an RFE contains a specialty occupation attack and the classifier flags the presence of this attack (true positive), or where an RFE does not contain a specialty occupation attack and the classifier does not flag this attack (true negative). If an attack is present but undetected (false negative), or if an attack is flagged but not actually present (false positive), we consider the prediction incorrect. We define prediction accuracy as the fraction of predictions that are correct. We also measure the precision, recall, and F1-score.

b) Processing Time.: Figure 9 and Figure 10 show the histograms of processing time (measured in seconds) using manual and automated document classification workflows, respectively. We show these histograms in separate figures because...

1See, e.g., [https://scikit-learn.org/stable/auto_examples/model_selection/plot_precision_recall.html](https://scikit-learn.org/stable/auto_examples/model_selection/plot_precision_recall.html)
because the manual processing times are two orders of magnitude higher than the automated processing times, making it difficult to include them in the same figure. Table IV compares their means, medians, standard deviations, minimum and maximum values.

In the next section, we interpret these results.

V. DISCUSSION

The results presented in the previous section allow us to quantify the advantage of our approach over purely manual processes. In the supporting document classification problem, the classifier can distinguish documents of two different types with strong visual and textual similarities with an accuracy of 98.08%. On the other hand, Table II shows that the automated workflow lowers the average document processing time from 196.87 seconds to 144.98 seconds, resulting in a reduction of 26.36%. Moreover, we also see that the standard deviation decreases from 79.66 seconds to 36.37 seconds, suggesting that the processing time of the automated workflow is more consistent. This is supported by Figure 6 which shows that manual processing time has a much wider spread than automated processing time.

In the RFE attack type detection problem, Table III shows that the prediction accuracy is 73.47%. We also note that the precision is 0.7097 and recall is 0.8462. In other words, out of all the RFE documents in which the classifier flags a specialty occupation attack, 70.97% actually contain the attack. On the other hand, of all the RFE documents that actually contain the specialty occupation attack, our classifier is able to flag its presence in 84.62% of the cases. In terms of processing time, the average end to end time decreases from 1803.53 seconds (approximately, 30 minutes) to 57.81 seconds (approximately, 1 minute), resulting in a reduction of 96.79%.

In view of the above, our approach reduces the amount of repetitive manual work necessary in both problems. However, a human in the loop is necessary for reviewing the outputs of our automated workflows.

VI. CONCLUSION

In this paper, we have considered the problem of categorizing documents necessary for supporting U.S. work visa petitions, as well as preparing responses to Requests For Evidence (RFE) issued by the U.S. Citizenship and Immigration Services (USCIS). Typically, both processes are entirely manual, and a significant portion of the work is repetitive without requiring any human ingenuity. To reduce the burden of manual repetitive work, we have demonstrated that machine learning methods may be applied to partially automate these workflows. In particular, we have used an ensemble of an image classifier and a text classifier to categorize supporting documents. We have also used a text classifier to detect the types of evidence being requested in an RFE, and used the identified types in conjunction with response templates and extracted fields to assemble draft responses. Finally, we have empirically demonstrated that these automated workflows achieve considerable accuracy while significantly reducing processing time.

REFERENCES

[1] U.S. Citizenship and Immigration Services, “Form I-797: Types and Functions,” https://www.uscis.gov/forms/filing-guidance/form-i-797-types-and-functions, accessed: August 13, 2020.
[2] ——, “Form I-797C, Notice of Action,” https://www.uscis.gov/forms/form-i-797c-notice-of-action, accessed: August 13, 2020.
