smartKYC

False Positive Elimination Using Advanced Name Handling Technology

A client case study focused on hit resolution of names with multiple origins

Feb 2021

Contents

Executive Summary

About smartKYC

smartKYC's technology drives faster, better and more cost-effective KYC at every stage of the relationship – liberating human effort to focus on decision-making rather than laborious research.

smartKYC fuses artificial intelligence with linguistic and cultural sensitivity and deep domain knowledge to set new standards for KYC quality, whilst transforming productivity and hardwiring compliance conformance.

smartKYC applies AI to extract precise open-source intelligence (OSINT) from vast corpuses of information – internet and deep web, news archives, watchlists and corporate databases. All of this happens at speed and at scale creating new possibilities such as straight-through processing, batch remediation and continuous KYC risk monitoring.

About the project

One of the key functionalities of the smartKYC application is name matching on watchlists. It leverages a variety of technologies such as name origin detection, fuzzy matching, Damerau-Levenshtein distance (see references (1), (2)) and nickname databases within a larger optimization engine to score names for similarity.

Recently, smartKYC was engaged by a leading Asian bank to assist with completing a substantial remediation task. The bank had implemented a new name screening system and was asked by the Monetary Authority of Singapore to run its complete book of business through this new software to check for hits from their primary watchlist source. This exercise generated huge volumes of hits that had to be manually inspected before being dismissed. The task turned out to be prohibitively time-consuming, and smartKYC was asked to help.

Introduction

Running its entire book of 6 million retail banking clients through their new screening software solution resulted in about 15.2 million hits, all of which would need human review to establish whether it was a genuine hit or a false positive. The large volume of hits was a direct consequence of the bank relaxing its matching rules, at the insistence of the regulator, due to evidently poor match rates.

The bank initially spent about 15 months using human effort to discount approximately 8% (1.2 million) of the 15.2 million hits. It was clear that continuing with a human-only approach was not feasible:

- Extrapolating from the 'manually checked' data, it was estimated that just over 120,000 man hours would be needed to complete the task. Assuming that 50 people worked on hit-clearing full-time (excluding variations in output and time off) the task would have taken in excess of a year to complete.

- The bank was under pressure from the regulator to complete this in an aggressive timeframe.
- It was apparent that to conduct such a large scale manual operation was going to cost the bank millions of dollars.

The time and cost pressure motivated the bank to explore advanced technology solutions to replace the existing fully manual operation. Experience during the initial manual phase suggested that 80% of the total hit population that their name screening software had generated were false positives.

Following a successful proof-of-concept, smartKYC was commissioned to deliver the project in an innovative, compliant, cost-effective and timely manner.

Project Synopsis

Objective and scope

The objective of the project was to use selected elements of smartKYC's underlying technology to filter out the majority of the false positives, thus leaving a much smaller set of hits needing manual review. The first task was to demonstrate to the bank that it could rely on smartKYC to filter out a significant portion of the false positives while preserving the true hits. During this phase, the manually evaluated hits were used as a test bed. The planned project duration was 10 weeks inclusive of:

- software/hardware setup and testing,
- data cleansing,
- rule clarification,
- calibration and re-calibration runs,
- deployment run on un-evaluated set of hits.

From code calibration to full production execution

Two key calibration criteria were established for the project:

1. Sensitivity: measuring the proportion of actual positives that were correctly identified.
2. Specificity: measuring the proportion of actual negatives that were correctly identified.

In order to achieve meaningful sensitivity and specificity, smartKYC used the 1.2 million human-evaluated hits as a 'training set' (i.e. a set that could be used to measure the results of the code and to validate and calibrate these results). Standard methods of splitting the large training set into random pieces of training and control were used in order to go through meaningful cycles of improving the code. A significant factor in achieving the set goals was the configurability of the code. The code was designed to process purported matches with one rule after the other, allowing the removal, addition or modification of rules as needed. For example, the names screened were all bank customers, whose names were verified against official IDs. This allowed the smartKYC team to adjust the rules, for example in a situation where the input name omitted a middle name or used a nickname, in which case the hit could be dismissed.

Other rules were adapted to the bank's particular practices. Through multiple iterations of data cleansing and calibration, the smartKYC solution was able to produce 100% sensitivity and 76%

specificity with respect to the training data in nine weeks. This satisfied the client's requirements and allowed smartKYC to deploy the algorithm to run on the remaining 14 million un-evaluated his. This run was spot checked by the bank and found to be satisfactory.

Upon completion of the project, smartKYC and the bank's compliance team were jointly audited by their in-house audit team and no concerns were raised. This demonstrated that the technology was effective and thorough. In addition, the bank invited the regulators to inspect the results and no issues were identified.

As a consequence, smartKYC is now engaged with the bank to deploy the false hit filtering algorithms as part of its business-as usual operations.

Name origin detection

A key factor in the success of this project was the name origin identification algorithm, a native feature in the smartKYC application. The particular name origin detection component used in this situation was developed using Machine Learning techniques. It was used to identify the origin of the input names so that culture-specific rules could be applied to the name matching. For example, a crucial success measure for this project was the technology's ability to successfully identify Chinese names, a large percentage of the data, and handle them differently than, say, Western or Muslim names.

A pair of Chinese names should be compared in a different way than a pair of Western or Muslim names, for various reasons. For example, middle names that are common in Western or Muslim names and could be omitted are not present in Chinese names, even though the first name is often split into two tokens ('pieces'). For example, 'Jingpin', which is a first name, is often written as 'Jing Pin'. However, given the name 'Xi Jin Pin', one cannot omit 'Jin' and match with 'Xi Pin'. This, of course, would be acceptable for Western names, where 'John Paul Smith' could match with 'John Smith'. On the other hand, Chinese people can have an additional Western first name which could be dropped or be present in different positions of the name, such as 'Sandra Yang Liping', 'Yang Sandra Liping', 'Sandra Yang' and more, resulting in name variations that are acceptable for Chinese names but not for Western or Muslim names. Another particular feature of Chinese names is that the Western transliteration (from Chinese to Latin characters) is different region to region (for example Mainland China vs. Hong Kong) and sometimes seemingly different names could in fact be two transliterations of the very same name.

Methodology

For this project, the goal was to clear a customer's information against a watched person's information ('watched person' being the entity name appearing on the watch list) producing a confident decision that the individuals were not the same. Where no such confidence could be achieved, the result was triaged for human review by an analyst at the bank. Relevant customer information used by smartKYC to accomplish this task consisted of the following fields:

- Customer primary name
- Customer other name(s)
- Country of citizenship

Watched person information used consisted of:

- Hit name (the name that was matched by original software screening)
- Primary name
- Original script name
- Country of citizenship

In order to guarantee that no potential true hit was missed, smartKYC first distinguished between unambiguous cases and ambiguous ones. This was then repeated over and over; cases that remained ambiguous were left for a manual decision. A key element in this process was identifying data irregularities in the training set, which in this case were inconsistent decisions by the manual classifiers. For example, two pairs of names which were either identical or exhibited similar patterns were in one case accepted as a possible match and in another case were dismissed as a mismatch. Such cases were highlighted and fixed manually so that the calibration could proceed. This, in turn, pointed to another advantage of the automatic classification, which treated all potential matches in a consistent manner.

Analysis steps

The analysis steps taken when coming to a decision consisted of:

- Origin(s) identification:
  The purpose of origin identification was to segregate the data into sub-problems, each configured for different name types. For example, the methodology used when evaluating a Chinese-origin name was entirely different than that used for a Tamil name. When the origin decision was difficult (i.e. deciding between Chinese, Burmese and Tibetan names) several possible origins were suggested. The origin identification was done using smartKYC's proprietary rules. These rules are developed based on smartKYC's experience and linguistic expertise and then applied to machine learning techniques.

- Matching scoring:
  On completion of the origin identification, the following sub tasks were executed to categorise the customer name as a potential hit or not;
  - Information aggregation and scoring job generation
    The purpose of this processing stage was to reduce the problem of matching many names (of the customer) with many names (of the watched person) into a set of single name-vs-name matching subproblems.
  - Variant generation
    In some cases some extra variants were generated and the results were added to the submatching problems described above. The variants generated were dependent on the name origin.
  - Part labelling
    Understanding which part of the name was the 'last' name and which part was the 'first', for example. This was given in some cases and deduced in others.
  - Scoring and registration
    The name scoring component used by smartKYC received two names as input, each consisting of optionally labelled name parts, and each with one or more possible name origins. Each pair of origins and name variants was scored and the highest scoring

match 'won' and was the final scoring result. In this scoring different fuzzy matching techniques were used such as Demerau Levenstein distance, metaphones, variance of names from different origins (for example, 'ee' and 'i' in Tamil), merging various components into one and more.

Rules applied

While the rules applied cannot be shared in this paper due to client confidentiality, some illustrative examples are shown here.

As mentioned above, special rules were applied for Chinese name matching. Some possibilities for Chinese name matching are mentioned below (in the examples the last name is Teng and the first name is Xiaoping, or Xiao Ping):

Allow different Chinese dialects (for example Mainland China and Hong Kong)	Possible match	Teng Xiaoping	Deng Hsiaoping
Allow flipping of first/last vs. last/first	Possible match	Teng Xiaoping	Xiaoping Teng
First name can appear as one word or two	Possible match	Teng Xiaoping	Teng Xiao Ping
Disallow reordering of parts of first name	Mismatch	Teng Xiao Ping	Teng Ping Xiao
A name with three Pinyins cannot match against a name with two Pinyins	Mismatch	Xi Jin Ping	Xi Ping

Two examples for Islamic names are given below:

Only missing part is Sheik/Haji	Possible match	Abdul Salim	Abdul Sheik Salim
Names with patronymics, but the order is reversed	Mismatch	Ibrahim bin Mahmud	Mahmud bin Ibrahim

In addition to the above sample of rules, there were also general rules used, such as 'apply fuzzy matching', which were used based on the name origin. Each origin also had specific transformations allowed, such as 'ee' vs. 'I' for Islamic or Tamil names.

Conclusion

smartKYC's algorithms were tested vigorously and thoroughly with an extreme number of real customer names that originated from at least six different cultural backgrounds. Success was measured in three ways.

- **Accuracy**. smartKYC was able to reduce false positives by almost 80%, while maintaining very high sensitivity (100% on test data).

- **Consistency**. As mentioned above, the training set originally contained cases of identical data that were manually processed in contradictory ways: A pair that was once declared a potential hit was declared a mismatch in another instance. smartKYC's automatic evaluation did not suffer from such inconsistencies as the same rules were applied programmatically.

- **Speed**. The production run on the 14,000,000 rows of un-evaluated hits took 50 hours of continuous and uninterrupted machine processing time in total. Using the bank's available and qualified human resources would have taken an estimated 120,000 man hours, which would not have been continuous. In other words, smartKYC's technology was able to perform this task at least 2,400 times faster than 50 humans.

The combination of smartKYC's artificial intelligence technology, linguistic know-how and tailored methodology meant smartKYC was able to drastically reduce the time and labour required to perform this daunting and high risk task and allow the client to meet its regulatory requirements.

The same approach can be applied to any other institutions facing this same challenge of excessive false positives.

References

(1) Bard, Gregory V. (2007), "Spelling-error tolerant, order-independent pass-phrases via the Damerau–Levenshtein string-edit distance metric", *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers : 2007, Ballarat, Australia, January 30 - February 2, 2007*, Conferences in Research and Practice in Information Technology, **68**, Darlinghurst, Australia: Australian Computer Society, Inc., pp. 117–124, ISBN 978-1-920682-49-1.

(2) Damerau, Fred J. (March 1964), "A technique for computer detection and correction of spelling errors", *Communications of the ACM*, **7** (3): 171–176, doi:10.1145/363958.363994, S2CID 7713345