Une analyse des méthodes informatiques contre la fraude documentaire

Rohan TOMER

Sous la direction de Johan BRIANTAIS

Institute for Field Education - Printemps 2018

Worldline

18 mai 2018

à Paris, FRANCE

Remerciements

Tout d'abord, je voudrais remercier considérablement M. Johan Briantais qui, en jouant les deux rôles de mon directeur de stage et mon tuteur de mémoire, m'aidait beaucoup avec mon processus de recherche et également ma formation comme un développeur, tous les deux desquels étaient inestimables pour la rédaction de cette mémoire.

Je remercie aussi l'équipe d'IFE à Paris - Mmes. Julie Rosticci & Emily Freeman et MM. Thomas Roman & Tim Carlson. Ils me donnait l'aide pour m'intégrer dans la société professionnelle et extraprofessionnelle française. En me donnant une maîtrise plus forte de la langue, ils me permettent d'écrire cette mémoire.

Et finalement, merci aux tous mes collègues à Worldline et tous mes camarades à IFE pour vos conseils occasionnels, vos petits assistances, et les "bon courages"s à propos de mes recherches.

- R. Tomer

Sommaire

Introduction

L'identité et la fraude

L'identité est un concept qui a plusieurs significations, qu'il soit une définition psychologique, philosophique, ou politique. Elle existe aussi aux échelles différents - on peut avoir une identité personnelle, communale, nationale, etc. Quand on parle d'identité d'un individu dans cette mémoire, on parle de la définition sociopolitique : une collection de ses éléments personnels qui, dans leur ensemble, lui sont intrinsèques et uniques.[1] Par conséquent, l'identité de quelqu'un est souvent utilisée pour vérifier son autorité pour accéder à un compte bancaire, à un billet d'avion, à la sécurité sociale, et aux bien plus de ressources qui lui appartiennent.

Dans une société en mondialisation constante, combinée à la dématérialisation des ressources de la plus haute importance, une identité est une chose qui contient beaucoup de pouvoir. De ce fait, il faut qu'il existe des preuves d'identité. À cette fin, une personne possède un document d'identité qui est utilisé pour prouver que quelqu'un est ce qu'il/elle dit être.[2] Se faire passer pour quelqu'un autre par voler son identité pour accéder à ses choses personnelles - cela s'appelle la fraude. Donc, la fraude documentaire est la fraude qu'on fait au moyen de document d'identité[3] (par exemple, en le volant, en le modifiant, en le falsifiant, etc.). Comme n'importe quel autre transgression, le gouvernement et les entreprises répondent avec les efforts contre la fraude, et ils contribuent beaucoup de ressources et de temps pour la lutte contre la fraude documentaire.

La motivation

Dans mon stage, je travaille sur le développement d'une solution informatique contre la fraude documentaire, particulièrement la fraude documentaire française, qui s'appelle DocID. DocID est un exemple d'une technologie anti-fraude créée dans le secteur privé. En travaillant sur DocID, une

---

[1] Olson Eric T. - "Personal Identity" - *The Stanford Encyclopedia of Philosophy* - Zalta Edward N. (ed.) - Stanford University - San Francisco, Californie - 2002 - 43 p.
Une paraphrase de cette définition anglaise de "*personal identity*" : "the necessary and sufficient conditions under which a person at one time and a person at another time can be said to be the same person"

[2] Quarmby Ben - *The case for national identification cards, 2003 Duke L. & Tech. Rev. 0002*. - Duke University - Durham, Caroline du Nord - 2003 - 34 p.

[3] Hoofnagle Chris Jay - "Identity Theft: Making the Known Unknowns Known" - *in Harvard Journal of Law and Technology (Vol. 21)* - Harvard University - Berkley, Californie – Harvard University – 2007 pp. 98 - 122

technologie qui décèle la fraude documentaire, je me suis familiarisé avec ses points forts et ses points faibles, et donc, dans une mesure plus grande, les capacités et les limites des méthodes anti-fraude. Je suis ensuite devenu intéressé d'étudier plus profondément l'efficacité des efforts informatiques contre la fraude.

De plus, l'aspect technique de la lutte contre la fraude suggère que les nouvelles technologies informatiques (comme la reconnaissance faciale, l'apprentissage machine, et "big data", qui sont toutes intimement liées à ma spécialisation scolaire de la statistique appliqué) seront appliqués pour la détection de la fraude.[4] Si on voulait déterminer la direction future des technologies anti-fraude, il faudrait évaluer ce que les technologies actuelles ont accompli et n'ont pas accompli, et donc les besoins émergents de la lutte anti-fraude. Mon intérêt dans les neuves technologies pertinentes donc me pousse d'examiner la situation de la technologie actuelle.

Finalement, la fraude documentaire est une crise très pertinente et pressante de nos jours. Selon le Ministère de l'économie et des finances de la France, les types de fraude documentaire comprennent, sans en exclure d'autres, "faux titres d'identité, fausses pièces d'état-civil, faux justificatifs de domicile, faux justificatifs de ressources"[5]. Un rapport annuel de ce ministère déclare que la fraude documentaire "est un problème fiscal épidémique" contre lequel il faut "allouer les efforts légaux et techniques" [6]. En effet, il y a des estimations de pertes financières massives à cause de fraude - environ $16,3 milliards USD (13,8 € milliards)[7] dans le monde. En focalisant sur la France, Frank McKenna, une spécialiste anti-fraude, écrit, "Le grand problème en France ... [est] la fraude d'identité. Les fraudeurs français préfère faire une demande pour les nouvelles cartes bancaires en utilisant les identités contrefaites plutôt qu'en volant ou en créant les cartes bancaires eux-mêmes.".[8] Plus que tous les autres pays développés, la fraude documentaire française d'identité forme la majorité de ses instances de fraude.

---

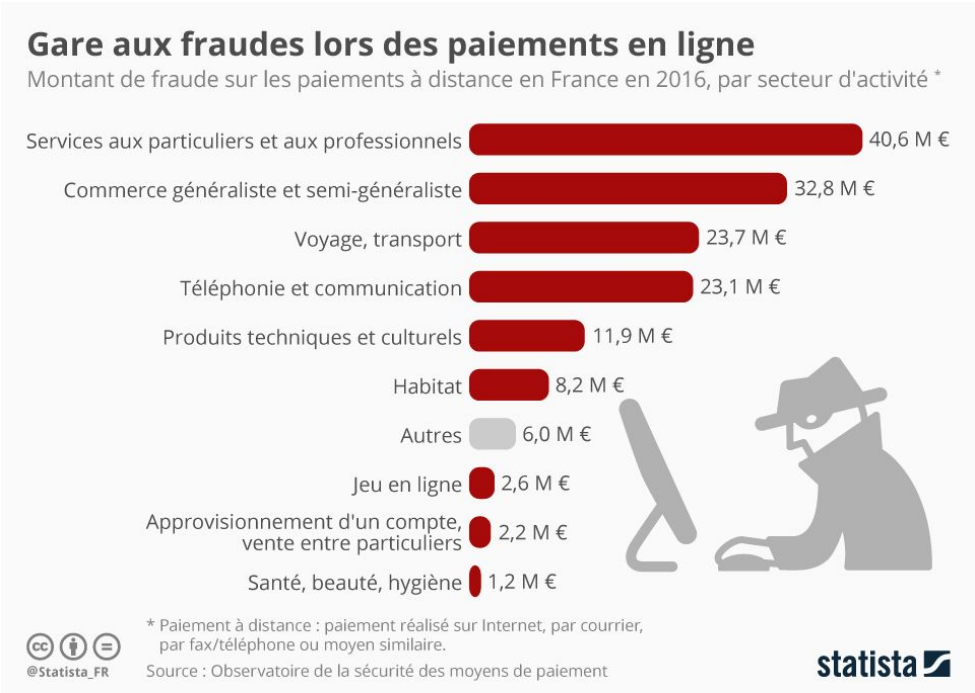
[4] Bolton R., Hand, D. - "Statistical Fraud Detection: A Review (With Discussion)" - *Statistical Science* - Project Euclid - 2002 - pp. 235–255.

[5] La République Française, "Lutte contre la fraude documentaire", *DNLF*, 2016.

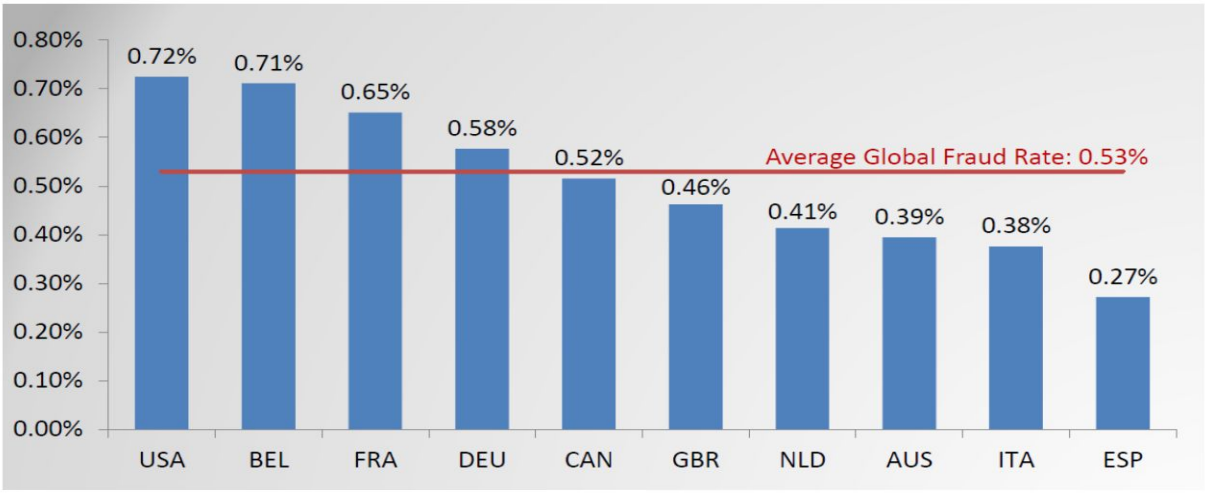
[6] Délegation nationale à la lutte contre la fraude (DNLF) – *Lutte contre la fraude aux finances publiques. Bilan 2016. - Paris* - Ministère de l'action et des comptes publiques, La République Française - 2016 - 108 p. ; p.9

[7] Fulmer Lori, "Global Card Fraud Losses Reach $16.31 Billion — Will Exceed $35 Billion in 2020", Business Wire, https://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion, 4 août 2015

[8] McKenna Frank, "Card Fraud in Europe is Higher than Ever", Business Wire, https://frankonfraud.com/fraud-trends/card-fraud-in-europe-is-higher-than-ever/, 14 juillet 2017
Traduit d'anglais : "The big issue in France, however, is not transactional fraud but origination fraud. Fraudsters in France prefer to apply for fraud brand new cards using stolen identities rather than stealing or counterfeiting credit cards."



La fraude croît rapidement sur l'Internet; d'après le rapport annuel de 2016 de l'Observatoire de la sécurité des moyens de paiement, le montant total des fraudes lors de paiements à distance s'élève à 152,3 millions d'euros, et celui est décomposé dans l'infographie ci-dessus par Statista.[9] En outre, cette transition de fraude sur ligne est soutenue par la graphique ci-après qui montre que le taux de fraude française sur la commerce électronique est plus haut que le taux global[10].



Fraud Rates by Country for E-commerce Sales

[9] Boitteaux Pascaline, "Gare aux fraudes lors des paiements en ligne", Statista, https://fr.statista.com/infographie/11144/gare-aux-fraudes-lors-des-paiements-en-ligne/, 19 septembre 2017

[10] "US Payments Forum provides guidance on card-not-present fraud", Payments, http://www.paymentscardsandmobile.com/guidance-on-card-not-present-fraud/, 24 mars 2017

Titre de graphique (traduite d'anglais) : "Les taux de fraude par pays pour les ventes sur e-commerce".

Avec la fraude documentaire sur ligne, des efforts qui emploient l'intervention directe d'humaines deviennent inutils; à cette fin, on a besoin des solutions informatiques; ce besoin donc aussi motive cette mémoire.

La problématique et le plan de développement

À la lumière des définitions clés, du contexte principal, et de la motivation de recherche, la problématique de cette mémoire est comme suit : *Quelle est l'efficacité des méthodes informatiques dans la lutte contre la fraude des documents d'identités françaises ?* On précise l'efficacité d'une méthode comme sa réalisation de ses buts affichés.

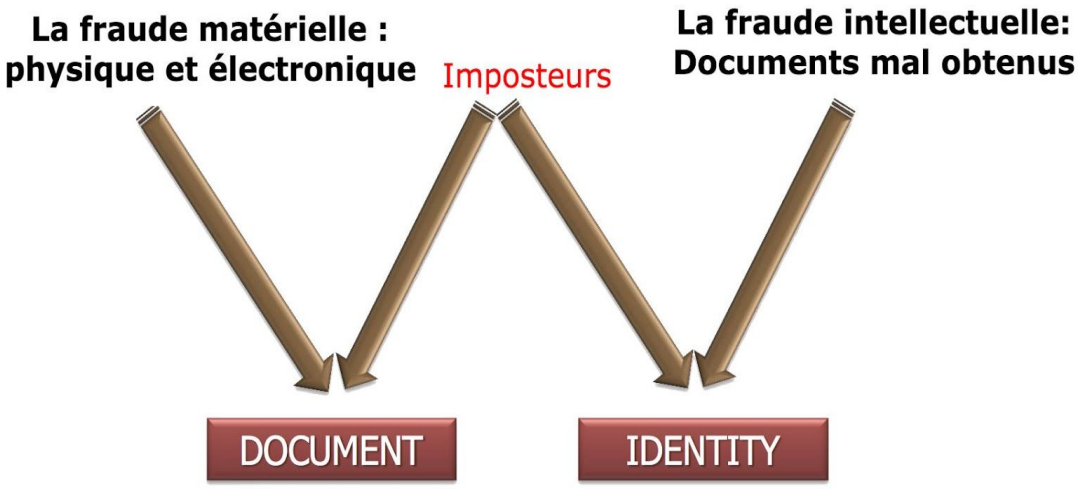
Le plan de développement s'organise autour la relation entre la fraude, sa prévention, et sa détection. Cette relation triangulaire démontrera les buts, les obstacles, les dépendances, variés des méthodes anti-fraudes, qui permettra une évaluation de l'efficacité de la technologie en empêcher et/ou déceler la fraude documentaire.

D'abord, on va présenter les méthodes utilisées le plus souvent pour effectuer la fraude, en se focalisant premièrement et principalement sur la fraude matérielle, et secondement sur la fraude intellectuelle. Cette analyse rendra plus claire les méthodes de déformation que l'anti-fraude lutte. Ensuite, on examinera les méthodes d'empêcher la fraude, en étudiant les efforts pris par des organisations internationales et l'état français avec le format de la carte et les protections physiques. On évalue l'efficacité de ces méthodes contre les obstacles susmentionnés posés par la fraude. Finalement, on verra les méthodes avec lesquelles la fraude documentaire est décelée et son efficacité comme à la fois une réponse à la fraude et un complément aux méthodes de prévention. En examinant ces constituants de l'anti-fraude en détail, on aura une bonne évaluation de l'efficacité des méthodes anti-fraude et ainsi pourra déterminer en conclusion la future de la lutte contre la fraude, sur un niveau informatique.

I. Méthodes d'effectuer la fraude

Helena Esteves, une inspectrice portugaise d'immigration, a démarré une séminaire internationale sur la sécurité anti-documentaire en dire, "Pour bien structurer nos efforts contre la fraude, il faut nous familiariser avec les moyens vers lesquels la fraude est mise à exécution".[11] Avec cette direction, elle a commencé sa présentation - "Les méthodes frauduleuses utilisées pour les documents de voyage, identité, et visa"[12] - pour le Colloque régional sur les documents d'identité, la biométrie, et la sécurité des frontières[13] par l'OACI[14].

Les découvertes d'Esteves et l'OACI globalement sur les méthodes de fraude sont corroborées par des autres organisations prestigieuses qui luttent la fraude documentaire - l'Interpol, le gouvernement français, et d'autres. On suit le modèle générale de la fraude construite par cette séminaire, particulièrement la définition de deux types de fraude documentaire - matérielle et intellectuelle - pour bien comprendre les enjeux de formes différents présentés par la fraude documentaire. Ces deux types de fraude documentaire ensemble forment la majeure partie de la fraude d'identité, comme illustré dans cette graphique[15] :



[11] Esteves Helena - "Introduction to fraudulent methods used in travel, identity and visa" - *in ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - Esteves Helena - Victoria Falls, Zimbabwe – L'Organisation de l'Aviation Civile Internationale – 2012 p. 2

[12] *Ibid.* p. 1
Traduit d'anglais : "Introduction to fraudulent methods used in travel, identity and visa"

[13] L'Organisation de l'Aviation Civile Internationale - *ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - L'Organisation des Nations Unies – Port Victoria, Zimbabwe - 2012 - 673 p.

[14] Une agence spécialisé de l'Organisation de Nations Unies qui se focalise sur la voyage en air internationale
Anglais: International Civil Aviation Organization

[15] Esteves Helena *op. cit.* p. 4.
La graphique originale est en anglais.

La fraude matérielle

En gros; la fraude documentaire qui est appelée "matérielle" est le cas où la fraude est réalisé avec l'usage d'un document d'identité qui n'est pas légitime. Le mot-clé concernant les documents d'identité liés à la fraude matérielle est "faux"[16]. Cette fraude est effectué par la falsification d'un document, et par conséquent elle peut être identifiée par une invalidation de document.[17] Ces documents frauduleux peuvent contenir les champs falsifiés, ou bien être totalement non autorisés.

Selon L'Organisation internationale de police criminelle (INTERPOL), les deux formes principales de la fraude matérielle sont la *falsification* et la *contrefaçon*.[18] L'OACI présente plusieurs façons dans lesquels ces fraudes sont réalisées.

La modification des champs biométriques

Un document qui a été falsifié est un avec une ou plus des modifications sans autorisation à un document véritable après son émission légitime,[19] où une modification pourrait être une changement / substitution, une effacement, ou une addition.

Souvent, les fraudeurs d'identité remplacent la photo d'identité avec une photo d'eux-mêmes (ou de leur client), normalement une nouvelle image au-dessus de l'image authentique. Par la cacher, on peut se présenter comme la propre titulaire de carte, avec tous les autres caractéristiques (nom, prénom, date de naissance, etc.).[20] Cette fraude marche parce que l'utilisateur/trice de document falsifié réussirait la vérification de visage et même si les autres identifiants ne sont pas les siens, ils existent dans une base de données et donc vont passer quand la carte est numérisée, parce qu'aucune modification est faite sur ni les champs écrits, ni les composants imprimés. La photo de remplacement est typiquement collée soigneusement sur la photo originale, comme montré dans les exemples suivantes, avec les preuves de ses faussetés :

---

[16] DNLF *op. cit.* p. 7
[17] *Ibid.*
[18] INTERPOL, "Counterfeit currency and security documents", *L'Organisation internationale de police criminelle*, https://www.interpol.int/Crime-areas/Financial-crime/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud, 13 juin 2017.
Interpol utilise les mots anglais "counterfeit" et "forgery", ou le premier fait référence à une contrefaçon totale d'un document, pendant que le dernier fasse référence à/aux changement(s) d'un document valide d'identité. Pour éviter l'ambiguïté de la traduction française, on utilise désormais "contrefaçon" pour "counterfeit", et "falsification" pour "forgery".
[19] Esteves Helena *op. cit.* p. 9
[20] *Ibid.* pp. 9 - 12

Un passeport falsifié chinois. Dans ce cas, une couche de la plastique extrêmement fine était collée sur la page entière d'identité.[21]

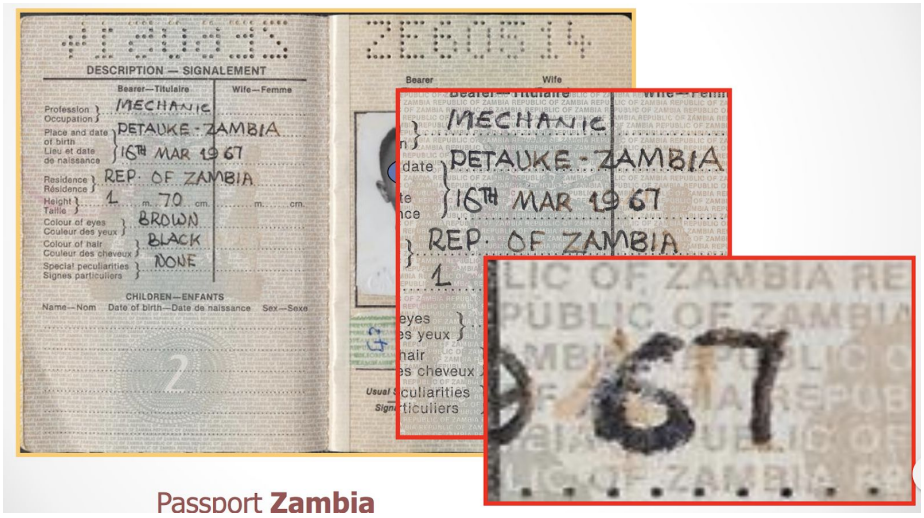
Une carte d'identité falsifiée portugaise. Dans ce cas, la couche plastique originale était enlevée pour que le fraudeur ait pu coller une nouvelle photo. C'est plus difficile de déceler.[22]

De plus, cette forme de fraude matérielle de falsification est une des plus répandues[23]parce qu'il ne faut pas avoir une connaissance rigoureuse de format d'une particulière pièce d'identité pour faire la substitution de photo. Quelquefois, on remplace entièrement la page d'identité d'un livret d'identité[24] (par ex. un passeport), mais cela est plus rare car elle est difficile de simuler son authenticité.[25]

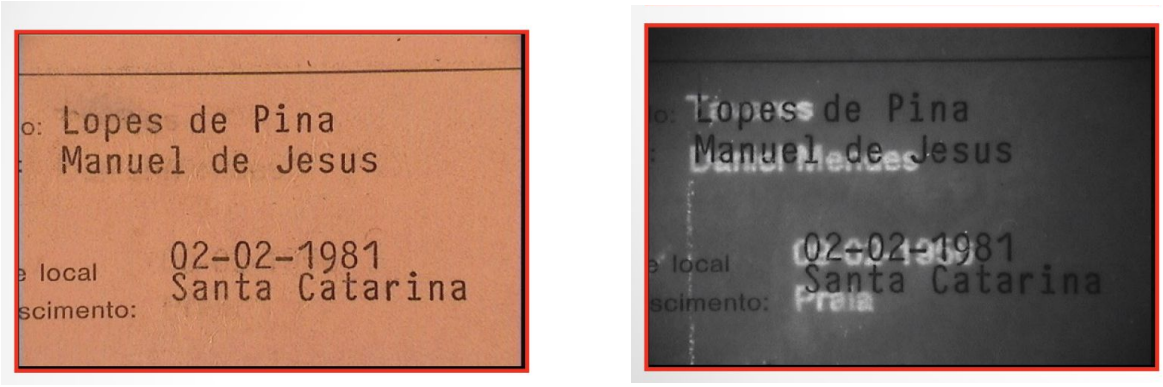
---

[21] Esteves Helena *op. cit.* p. 10
[22] *Ibid.* p. 11
[23] Siciliano Mauricio - "THE ICAO MRTD PROGRAMME" - *in ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - Siciliano Mauricio - Victoria Falls, Zimbabwe – L'Organisation de l'Aviation Civile Internationale – 2012 pp. 27-28
[24] Esteves Helena *op. cit.* p. 13-15
[25] *Ibid.*

Cependant, la modification des quelques unes (pas toutes) des données biométriques écrites (c.-à-d. le nom, la nationalité, etc.) se produisent autant que le remplacement de photo.[26] Cette type de falsification est généralement appliqué sur la pièce d'identité propre d'un(e) fraudeur/euse; c'est-à-dire que cette fraude ne comporte pas un vol d'identité, mais un changement subversif à cette identité[27]. Cette distinction rend difficile d'être averti vers cette fraude, parce qu'il n'y a pas un/e victime qui préviendrait les autorités ou responsables d'un vol d'identité[28]. Voilà des exemples, encore avec des démonstrations de fraude :



Un passeport de la Zambie ou l'année de naissance était modifié - on peut discerner l'année vraie effacé en derrière.[29]

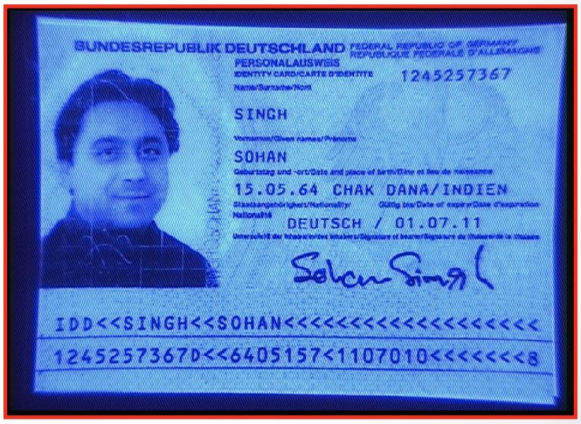


Une license de conduire du Cap Vert. Les champs originaux ont été rendu quasiment invisible, et le fraudeur a imprimé un nouveau nom, nouvelle année de naissance, et nouvelle ville d'origine.[30]

[26] Esteves Helena *op. cit.* pp. 16 - 19
[27] INTERPOL, *op. cit.*
[28] *Ibid.*
[29] Esteves Helena *op. cit.* p. 16
[30] *Ibid*. p. 17

Les cartes et documents contrefaits

Bien que la falsification consiste des changements partiels sur une base authentique, les pièces d'identité par contrefaçon sont entièrement illégitimes.[31] Un document d'identité contrefait est "un document qui constitue une reproduction non autorisée d'un document véritable. Ces documents ne sont pas créés légitimement, ni remis ni reconnus par une autorité officielle."[32] D'après INTERPOL, les documents contrefaits bien faits sont créés avec l'aide d'une imprimerie du "calibre officiel / gouvernemental"[33]. Contrairement aux documents falsifiés, les documents contrefaits sont très difficile d'identifier comme faux à l'œil nu. Il faudrait créer les conditions exceptionnelles, comme dans les images suivantes[34] [35] :



Seulement sous la lumière ultraviolette est-ce on peut distinguer que ces documents (une carte nationale d'identité française et une autre allemande) sont contrefaits. Même si que les responsables nationales (i.e. les douanes, les représentants d'état, etc.) ont accès à ces outils, le/la vendeur/euse ne les ont pas[36]; donc, les documents contrefaits constituent une menace forte pour la lutte contre la fraude.

---

[31] Esteves Helena *op. cit.* p. 6

[32] INTERPOL, *op. cit.* Traduit d'anglais : "...a document that constitutes an unauthorized reproduction of a genuine document. These documents are not legitimately manufactured, nor issued or recognized by an official authority."

[33] *Ibid.*

[34] Image à gauche :
CTMS, "Comment on décèle une fausse carte d'identité ?", *CTMS*, https://www.ctms.fr/fraude-documentaire/content/239-comment-déceler-une-fausse-carte-d'identite-, 23 mars 2018.

[35] Image à droit :
Esteves Helena *op. cit.* p. 8

[36] DNLF, *op. cit.* 70 - 75

La fraude intellectuelle

La distinction entre la fraude matérielle et la fraude intellectuelle est que la dernière est effectuée sans besoin d'un pièce d'identité faussé. Donc, la fraude intellectuelle n'implique pas ni falsification ni contrefaçon d'identité; cependant, cela ne veut pas dire qu'elle n'implique pas les méthodes frauduleuses dont mentir, soudoyer, ou suborner[37]. INTERPOL et L'OACI établissent deux types clés de la fraude documentaire intellectuelle : l'obtention frauduleuse et être l'imposteur.

L'obtention frauduleuse d'un document valide

Cette fraude est réalisée avec des documents (i.e. des passeports, cartes d'identité, etc.) véritables, mais obtenus frauduleusement. La définition du document en cette forme de fraude intellectuelle est pareille parmi les organisations anti-fraude : un document authentique d'identité ou de voyage obtenu, soit au moyen de déception en soumise des autres documents falsifiés ou contrefaits, soit au moyen de coopération d'un/e responsable corrompu(e).[38] Ce qui rend cette fraude tellement insidieuse est que la carte est totalement valide, soit par l'œil nu ou sous les lumières spéciales - "En utilisant le pièce d'identité comme seul contrôle de validité, c'est décidément impossible de le reconnaître correctement comme un pièce faux."[39]

Une façon d'obtenir frauduleusement un document valide est par aller utiliser les faux documents pour la création d'un autre document. Par exemple, pour une carte nationale d'identité française, il faut fournir un justificatif de domicile, une photo d'identité, une acte de naissance, et un justificatif de nationalité française[40]. Si on fait la fraude pour n'importe lequel de ces documents (par ex. une acte de naissance falsifiée, un justificatif de domicile contrefait) et ils passent les contrôles, on va recevoir une véritable, valide carte nationale d'identité. On peut donc fournir cette carte valide et faire la fraude avec cela sans s'inquiéter, car la carte passerait les contrôles qui découvrirait les fraudes matérielle. L'autre façon de faire cette type de fraude est par corrompre un responsable qui peut donner un fraudeur un valide pièce d'identité sans autorisation. Un fraudeur ferait la corruption en soudoyant un officiel, en appelant des relations personnelles (i.e. des amis, membres de famille, etc.), ou en faisant des autres actes criminelles (comme le chantage).

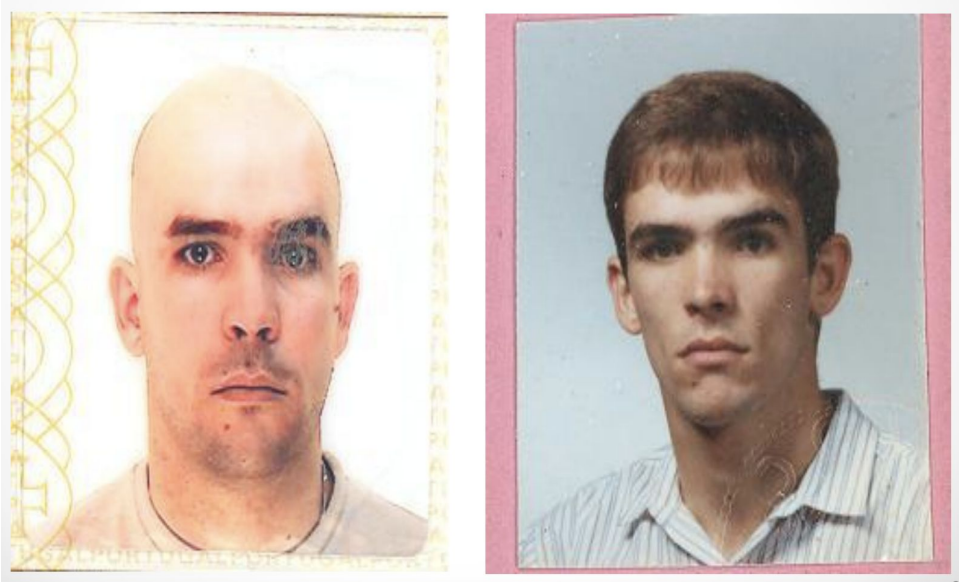
---

[37] INTERPOL, *op. cit.*
[38] *Ibid.*
[39] Esteves Helena *op. cit.* p. 23
[40] Service Publique, "Carte nationale d'identité d'un majeur", *La République Française*, https://www.service-public.fr/particuliers/vosdroits/F1341, 23 mars 2018.

Être un imposteur ou une imposteuse

On define être imposteur comme être quelqu'un qui sciemment se présenter faussement en utilisant le document d'identité d'une autre personne, duquel les données biométrique et la photographe quasiment ressemble l'imposteur, comme ce fraudeur était la vraie titulaire du document.[41] La différence entre ce type de fraude et l'obtention frauduleuse est subtile mais importante. En ce cas, le document est proprement de quelqu'un autre, alors que le document d'obtention frauduleuse est proprement de fraudeur.

Les imposteurs profitent d'une ressemblance avec la titulaire pour faire semblant d'une autre personne et donc accéder aux ressources qui appartient à cette personne. Dans l'image suivante, on peut voir l'imposteur à gauche, et la photo de vraie titulaire (pris de son pièce d'identité volé par l'imposteur) et donc les similarités visuelles qui causent un officiel de commettre un erreur en vérifiant l'identité de fraudeur:[42]



* * *

En étudiant les formes différentes de fraude documentaire, on peut bien évaluer les qualités principales de la fraude documentaire : quelles faiblesses du système de documentation elle exploite,

[41] Esteves Helena *op. cit.* pp. 26 - 28
[42] *Ibid.* p. 28

les moyens de changement / faussement, etc. Puis, on peut identifier quels problèmes technique il faudra résoudre avec l'anti-fraude, et enfin créer ces solutions.

Le problématique veut juger l'efficacité des solutions anti-fraudes, et évidemment, ce n'est pas possible de résoudre un problème efficacement sans bien savoir le problème et toutes ses facettes. Maintenant, avec les informations concrètes sur les fraudes qui doivent être arrêtées, on peut continuer naturellement par voir la prévention de ces fraudes en les rendant plus difficile d'effectuer.

Méthodes d'empêcher la fraude

On dit souvent que trouver comment prévenir un problème est mieux que de le résoudre. Sans surprise, cela vaut pour les méthodes anti-fraude; La documentation de l'OACI stipule que le document d'identité idéal devrait pouvoir servir à deux fins principales. Premièrement, il devrait contenir toutes les informations qui distinguent le détenteur de la carte de toute autre personne (c'est-à-dire établir leur identité propre et unique).[43] Deuxièmement, il devrait rendre la duplication plus difficile en contenant des informations qui distinguent le document de toute copie ou modification frauduleuse.[44]

Ce mécanisme secondaire concernant le format des documents d'identité - les rendant difficiles à dupliquer illégalement - est le centre de la prévention de la fraude documentaire; c'est-à-dire, des méthodes contre la fraude de document qui impliquent dans le document lui-même.

La prévention de la fraude est gérée logiquement par ceux qui gèrent la création et la délivrance du document d'identité; Généralement, un gouvernement ou une organisation gouvernementale.[45] Puisque l'on discute des documents d'identité français dans cette mémoire, on s'intéresse naturellement aux efforts déployés par le gouvernement français pour prévenir la fraude documentaire. Cependant, le gouvernement français, dans sa délivrance de documents d'identité tels que les cartes d'identité nationales (CNI) et les passeports, suit les normes des organisations internationales dans l'espoir de prévenir la fraude; par conséquent, on se préoccupe également des efforts de ces organisations susmentionnées.

Les efforts internationaux

En second lieu seulement à l'ONU, INTERPOL est l'une des plus grandes organisations internationales. Son objectif déclaré est de "connecter la police du monde entier». Leur mission est d'utiliser leur réseau pour aider à résoudre et prévenir les crimes de nature internationale, tels que le crime organisé, la cybercriminalité et le terrorisme; dans cette optique, il est évident que INTERPOL a tout intérêt à lutter contre la fraude, en particulier la fraude documentaire. Comme indiqué précédemment, les documents d'identité sont le plus souvent utilisés pour valider l'identité de voyage,

[43] Siciliano Mauricio *op. cit.* p. 2
[44] Ibid.
[45] Assemblé de l'OACI, "Resolutions adopted by the Assembly", *OACI*, https://www.icao.int/Security/FAL/Documents/a39_res_prov_en%20A39-20%20B.pdf, 6 mars 2016. 6 p.

souvent à l'étranger. Afin de prévenir les crimes de tromperie, tels que la traite des êtres humains, il est nécessaire de pouvoir prévenir et détecter la fraude documentaire.

INTERPOL, étant donné son rôle d'organisation internationale de police, se concentre davantage sur la détection de la fraude, sur laquelle on se concentrera dans la prochaine partie du développement. Néanmoins, il a fait des efforts pour prévenir la fraude. à savoir, la base de données de documents de voyage volés et perdus d'INTERPOL. Cette base de données contient des documents sur les documents d'identité volés, révoqués et perdus qui ont été signalés à la police dans le monde entier. L'utilisation de cette base de données est préventive car elle empêche la fraude de documents intellectuels, en particulier l'imposture: on ne peut pas passer avec succès en tant que détenteur d'un document volé ou perdu si le document est enregistré dans la base de données. En conservant également les numéros de série des documents d'identité vierges, mais révoqués, INTERPOL empêche également la méthode intellectuellement frauduleuse de document valide, obtenu illégalement, car un fraudeur ne peut désormais utiliser un document vierge obtenu pour se remplir lui-même. Cependant, INTERPOL n'est pas chargé d'empêcher les fraudes matérielles, car elles n'imposent pas les composants des documents.

Cette responsabilité incombe à l'OACI. ou l'Organisation de l'aviation civile internationale. Elle est une agence spécialisée des Nations Unies. Formé en 1947[46], ses objectifs sont de faciliter le transport international face à un réseau humain mondial en pleine croissance tout en assurant la sûreté et la sécurité des personnes et de leurs informations[47]. L'OACI est investi dans la prévention de la fraude documentaire en raison de sa mission centrale de fournir un transport aérien sûr et fiable, ce qui implique des documents d'identité. Il est également plus habilité que toute autre organisation mandataire en raison de son statut de membre des Nations Unies, lui accordant des ressources et l'accessibilité pour transmettre les méthodes anti-fraude au reste du monde.

L'OACI remplit de nombreux rôles en tant qu'organisation mondiale, mais son rôle le plus important dans la lutte contre la fraude documentaire est son rôle d'organisme de normalisation - un organe directeur qui établit des critères techniques pour un élément utilisé par de nombreuses autres organisations. Dans le cas de l'OACI, elle établit des normes physiques et techniques pour les

[46] L'OACI, "Vission and Mission", *OACI*, https://www.icao.int/about-icao/Council/Pages/vision-and-mission, 2017
[47] *Ibid.*

documents de voyage et d'identité; ces normes sont utilisées comme lignes directrices par les nations et les organismes souverains.[48]

Les deux règles les plus significatives que l'OACI a mises en place pour prévenir la fraude documentaire sont les critères physiques pour les documents d'identité - la taille, les ratios et les informations affichées, entre autres - et la création de la zone lisible par machine. Les spécifications relatives à ces deux aspects figurent en *Document 9303: Documents de voyage lisibles à la machine*[49], actuellement sur sa septième édition.[50] Ces règlements entraînent divers degrés de succès dans la prévention de certains types de fraude documentaire, qui on va analyser ensuite.

Les critères physiques du document

Lors de la 39e session de l'Assemblée de ses États membres à Montréal à l'automne 2016, l'OACI a adopté trois nouvelles résolutions concernant la facilitation des documents de voyage. Dans la Résolution 1, Annexe B - "Mesures nationales et internationales pour assurer la sécurité et l'intégrité de l'identification des voyageurs et des contrôles aux frontières» - l'un des points clés est que les États membres assureront "la conception et la fabrication de documents de voyage lisibles à la machine ... conformes aux spécifications de l'OACI ... comme spécifié dans *Document 9303* de l'OACI.[51]"

Dans *Document 9303*, l'OACI spécifie des critères physiques pour trois types (en particulier, les tailles) de documents d'identité: TD1, TD2 et TD3. Les critères de spécification de ces documents suivent la même formule: Dimensions, disposition générale et contenu. Les types TD diffèrent non seulement par la taille, mais aussi par les informations qu'ils contiennent et leur disposition; néanmoins, la manière dont l'OACI spécifie les critères de chaque document est cohérente, variable uniquement dans les mesures / informations précises contenues dans le document. Par conséquent, pour l'analyse suivante de leur efficacité, des exemples visuels seront montrés à partir des trois types de documents.

Premièrement, les dimensions d'un document selon les spécifications de l'OACI doivent être presque exactes par rapport aux critères documentés. Par exemple, dans la figure ci-dessous, qui

[48] L'OACI, "Vision and Mission" *op. cit.*
[49] Anglais : Machine Readable Travel Documents ; Acronyme : MRTD
[50] Assemblé de l'OACI, *op. cit.* p. 2
[51] Texte originale en anglais : "the design and manufacture of standardized Machine Readable Travel Documents (MRTDs) … that comply with ICAO specifications… as specified in ICAO Document 9303."

détaille les dimensions interne et externe d'un document d'identité TD1, on peut voir que l'OACI permet une erreur de 0,75 mm sur une spécification de largeur de 85,6 mm[52] - une marge relative de seulement 0,87%.

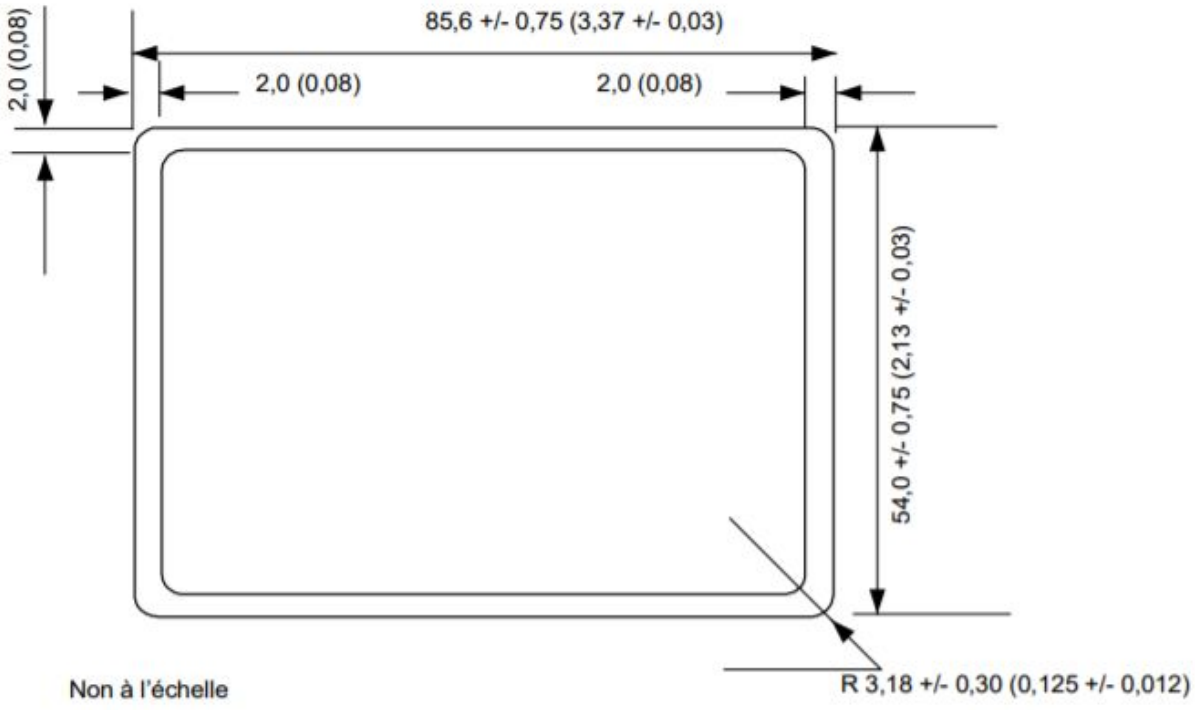


Figure 2. Marges de bordure et dimensions nominales d'un DVOLM de format TD1

Cette exigence de précision extrême est courante dans la spécification de Document 9303, et pas seulement pour la hauteur et la largeur générales, mais aussi pour l'épaisseur de la carte et des zones d'éléments de données individuelles sur la carte, comme indiqué sur le gabarit suivant pour une carte TD3:[53]

[52] L'OACI - "Partie 5 : Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD1" - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L'OACI - Montréal, Canada – L'Organisation de l'Aviation Civile Internationale – 2015 - 36 p.
[53] L'OACI - "Partie 4 : Spécifications pour les passeports lisibles à la machine (PLM) et autres DVLM de format TD3" - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L'OACI - Montréal, Canada – L'Organisation de l'Aviation Civile Internationale – 2015 - 38 p.

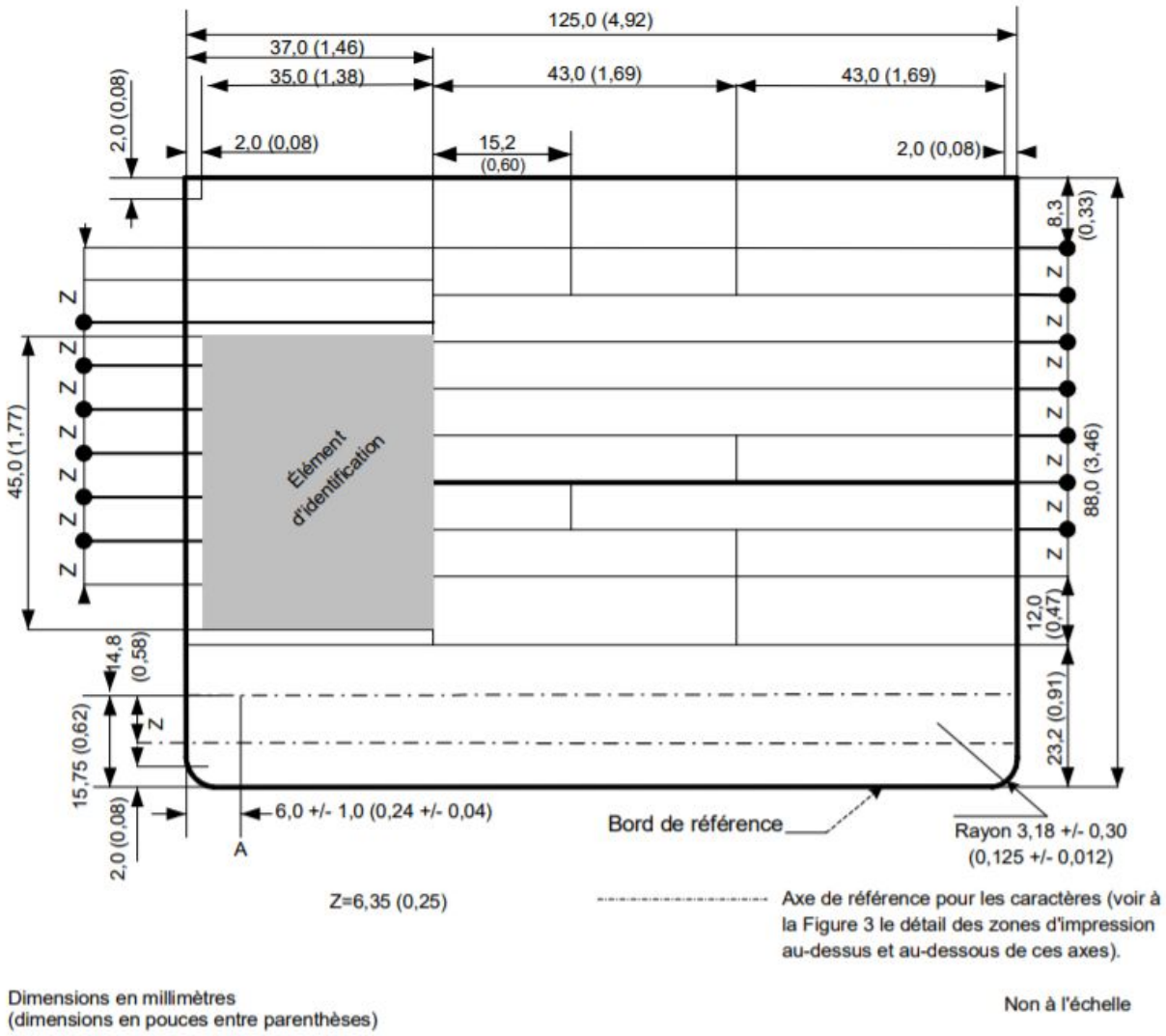


Figure 7. Gabarit pour les champs de personnalisation des renseignements

La rigueur et la cohérence des spécifications physiques définies par l'OACI présentent des avantages pratiques évidents. Il en résulte une production de documents automatisée moins coûteuse, ainsi que moins de réglementations pour les fonctionnaires des frontières et donc une réduction des coûts de formation du personnel.[54] Les critères physiques ont également des avantages en tant que méthode anti-fraude. Ils rendent la fraude matérielle plus difficile - les différences entre une pièce d'identité valide et une pièce d'identité frauduleuse ne peuvent plus être attribuées à une erreur humaine, et il serait très difficile de fabriquer une carte entièrement contrefaite à partir de zéro. En

[54] Assemblé de l'OACI, *op. cit.* p. 1

effet, à tout le moins, ces critères physiques stricts devraient réduire la quantité de contrefaçon matérielle.

D'un autre côté, ces spécifications n'ont aucun effet sur certains autres types de fraude discutés précédemment. Il n'a aucun effet sur la fraude d'identité intellectuelle - un imposteur utilise une pièce d'identité légitime; par conséquent, il suivra toutes ces spécifications à la lettre. En outre, il est inefficace contre les documents partiellement frauduleux - c'est-à-dire une fraude matérielle impliquant une falsification, et non une contrefaçon. Par exemple, si un fraudeur remplace la photo d'identité et modifie la date de naissance sur une carte de type TD2, il / elle n'a modifié aucun des aspects dimensionnels, donc ce type de fraude n'est pas empêché non plus. Heureusement, l'autre grande obligation imposée par les MRTDs - les zones lisibles par machine - aide à prévenir cela.

La zone lisible par l'ordinateur

Les documents d'identité lisibles à la machine (en particulier les passeports) ont commencé à être publiés dans les années 80s. L'OACI a normalisé le format de document lisible par machine et a poussé les États membres à adopter le format dans leur résolution de 2016, en écrivant dans la Résolution 1, Appendice B, Déclarations 7 et 8 qu'il "exhorte les États membres qui ne l'ont pas encore fait délivrer des passeports lisibles à la machine conformément aux spécifications du Doc 9303, Partie 4 »[55] et " Rappelle aux États membres de veiller à ce que les passeports non lisibles par machine soient retirés de la circulation »[56]. Aujourd'hui, en 2018, la plupart des États membres de l'OACI - en l'occurrence la France - ont émis des documents d'identité lisibles à la machine et éliminé la plupart des non-MRTD d'ici à aujourd'hui.

Selon l'OACI, une zone lisible par machine (acronyme: MRZ) pour les documents d'identité est un ensemble de deux ou trois lignes de caractères noirs sur un fond blanc, utilisant une police uniforme à espacement fixe. Ces éléments permettent une faisabilité maximale pour la reconnaissance optique de caractères (OCR). La MRZ contient la plupart des informations sur la pièce d'identité dans un format qui peut être analysé automatiquement par un ordinateur. La disposition exacte de la MRZ (quelle information, quel positionnement) dépend du fait que le document d'identité soit TD1, TD2 ou TD3. Les normes de l'OACI permettent également l'ajout d'éléments facultatifs par le pays émetteur, ce qui contribue également un peu plus à la variabilité. A titre d'exemple, voici une carte nationale

[55] Assemblé de l'OACI, *op. cit.* p. 2
[56] *Ibid.*

d'identité de France (de type TD2), avec un MRZ soulignée[57]. On note la corrélation avec les éléments de données sur la partie non-MRZ de la carte :

On peut voir deux lignes de données textuelles, chaque ligne montrant 36 caractères alphanumériques, avec quelques chevrons (<). Le tableau ci-dessous montre comment la MRZ correspond aux données d'identité du titulaire de la carte :

Indice[58]	Texte dans la MRZ	Information	Données correspondantes de la VIZ[59]	Notes
1 | 0 - 1	ID	Type de document	Carte nationale d'identité	L'OACI exige que la première lettre soit "I" pour une pièce d'identité, mais la deuxième lettre est à la discrétion du pays émetteur.

[57] Feuvre Christophe, "NATIONALITÉ, CITOYENNETÉ FRANÇAISE ET CITOYENNETÉ EUROPÉENNE", *Le Livre Scolaire*, https://www.lelivrescolaire.fr/#!manuel/62/histoire-geographie-education-civique-3e/chapitre/833/nationalite-citoyennete-francaise-et-citoyennete-europeenne/document/715203, 2014

[58] Le format pour une indice est (# de ligne | position de 1er caractère (0 - 35) - position de 2ème caractère (0 - 35))

[59] VIZ est une acronyme qui veut dire 'Visual Inspection Zone", la zone de carte qui n'est pas la MRZ ni la photo.

1 | 2 - 4	FRA	Le pays émetteur	La République Française	Cela suit une liste de codes de pays fournie par l'OACI
1 | 5 - 29	REUVRE<<<<<<<<<<<<<<<<<<<<	Le nom de famille	Reuvre	S'il y a l'espace vide après le nom de titulaire (comme ce cas), on rempli la reste avec <. Si le nom est trop grand, on arrete à la 25ème lettre. Les espaces dans le nom / la punctation sont traités selon la guide d'OACI.
1 | 30 - 32	782	Office de remise	S.O.[60]	
1 | 33 - 35	112	Code interne d'office	S.O.	
2 | 0 - 3	0905	Date de remise	[mai 2009][61]	Format : aa / mm
2 | 4 - 6	782	Office de remise	S.O.	Pareil à [1 | 30 - 32]
2 | 7 - 11	00155	Code interne de titulaire	S.O.	
2 | 0 - 11	090578200155	Numéro de carte	090578200155	Cela est la combinaison des derniers 3 champs.
2 | 12	7	Clé de controle	S.O.	Expliqué dans la troisième partie de développement
2 | 13 - 26	CHRISTOPHE<<TH	Le(s) prénom(s)	Christophe, Thierry, Christian	Selon la guide d'OACI, chaque prénom est séparé par deux <. Il arrête après la 13ème caractère.
2 | 27 - 32	910614	Date de naissance	14 juin 1991	Format :aa / mm / jj
2 | 33	2	Clé de controle	S.O.	Expliqué dans la troisième partie de développement
2 | 34	M	Sexe	Male	"F" pour femelle.
2 | 35	8	Clé de controle	S.O.	Expliqué dans la troisième partie de développement

Selon les standards de l'OACI expliqués dans Doc 9303.[62]

La MRZ empêche la fraude matérielle - pas seulement la contrefaçon, mais aussi la falsification des données. Les changements dans la VIZ devraient être reflétés dans la MRZ. Par exemple, si le nom de famille d'un détenteur de carte a été changé, le contenu de la MRZ à la ligne 1,

[60] Sans objet
[61] Trouvé sur l'autre côté de la carte
[62] L'OACI - "Partie 6 : Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD2" - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L'OACI - Montréal, Canada – L'Organisation de l'Aviation Civile Internationale – 2015 - 32 p.

les indices 5 à 29 devraient également changer. Il est peu probable qu'un fraudeur puisse répliquer les données de la MRZ de manière passable pour que la machine analyse correctement les données. En outre, la MRZ contient plusieurs champs, tels que les codes internes, qui ne figurent pas sur la VIZ et ne peuvent être contrefaits de façon fiable (sauf si le fraudeur a l'aide d'un fonctionnaire corrompu ou d'autres moyens internes).

Cependant, l'institution d'une MRZ est tout aussi inefficace que les critères physiques pour prévenir la fraude intellectuelle. Et, comme le note le DNLF, la fraude matérielle est toujours possible parce que tout le matériel de l'OACI est accessible au public et facilement accessible.[63]

Les efforts français

Depuis le moyen âge, la France a délivré des passeports aux diplomates et aux nobles qui étaient enclins à voyager; Cependant, la carte d'identité nationale est une innovation qui n'a été introduite qu'au 20e siècle. Il a été introduit pour la première fois en 1917 pour les étrangers dans la crainte des espions pendant la Première Guerre mondiale, et a été réintroduit de manière obligatoire pour tous les Français pendant l'État français de la Seconde Guerre mondiale. La carte d'identité nationale actuelle de la France a été établie par un décret en 1955, et si ce décret a été modifié en fonction de l'évolution des technologies, la carte reste non obligatoire d'avoir. Depuis 1944, la création de l'OPACI[64], la France a suivi le protocole de l'OACI concernant les passeports[65].

En réponse à la fraude croissante, le gouvernement français a créé la Délégation nationale à la lutte contre la fraude, connue sous le nom de DNLF, le 18 avril 2008. La DNLF s'engage "professionnaliser les démarches d'échanges entre organismes, d'assurer l'absence de déperdition d'informations entre entités, de mettre en évidence les mesures à prendre pour combler les lacunes juridiques ou les failles opérationnelles des dispositifs anti-fraudes.[66]" Mais avant même la création de cette délégation, le gouvernement français a institué des codes légaux et des attributs physiques concernant leur carte d'identité nationale qui aident à prévenir les activités frauduleuses.

---

[63] DNLF, *op. cit.* p. 111
[64] L'organisation *prévisionnelle* de l'aviation civile internationale
[65] L'OACI, "The History of ICAO and the Chicago Convention", https://www.icao.int/about-icao/History/Pages/Default.aspx, 2015
[66] La DNLF, "Le rôle de la DNLF", *Ministère de l'Economie*, https://www.economie.gouv.fr/dnlf/role-dnlf, 6 avril 2016

Les codifications légales

Dans le Décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité, il est expliqué au Titre I, Article 1:

> *"Il est institué une carte nationale certifiant l'identité de son titulaire. Cette carte a une durée de validité de quinze*[67] *ans lorsqu'elle est délivrée à une personne majeure et de dix ans lorsqu'elle est délivrée à une personne mineure."*[68]

Et plus tard, dans l'Article 2 du même titre:

> *"La carte nationale d'identité est délivrée sans condition d'âge à tout Français qui en fait la demande.*
> *Elle est délivrée ou renouvelée par le préfet ou le sous-préfet.*
> *A Paris, elle est délivrée ou renouvelée par le préfet de police.*
> *A l'étranger, elle est délivrée ou renouvelée par le chef de poste diplomatique ou consulaire."*[69]

Le reste du décret contient davantage de spécifications techniques et officielles concernant la carte d'identité nationale, mais ces deux articles, centrés sur la période de validité et les sources légales d'émission, ont contribué à établir une force préventive contre la fraude documentaire. La période de validité lutte contre l'imposture; par exemple, un imposteur ne peut pas revendiquer des apparences radicalement modifiées à partir de la photo d'identité si la carte a plus de quinze ans. Ceci permet également (avec l'ordre pour tout émission de venir d'une poste gouvernementale) à la préfecture / au gouvernement local de mettre à jour leurs enregistrements biométriques pour être plus précis, en prévenant davantage l'imposture. Une période de validité limitée est si importante, car c'est la seule méthode anti-fraude codifiée qui combat la fraude documentaire intellectuelle, que les autres méthodes décrites sont incapables de combattre.

La sécurité physique

En plus de suivre les procédures de normalisation de l'OACI concernant leurs cartes d'identité nationales, la France a également ajouté des caractéristiques physiques supplémentaires de la carte qui

[67] C'était dix ans pour un majeur jusqu'à 1 janvier 2014, quand l'âge était changée rétroactivement à quinze ans.
[68] La République Française, "Décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité", *LegiFrance*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006060725, 5 novembre 2017
[69] *Ibid.*

aident à prévenir la fraude documentaire. Cette sécurité s'appelle la sécurité ultraviolette (UV); elle permet de vérifier la bonne réflexion des sécurités sous une source de lumière UV.[70] La carte fera ressortir des fibrettes de couleur verte, bleue, rouge, comme montré dans l'image suivante[71]. On fait attention aux fibrettes de couleur qui sont visibles seulement sous l'ultra-violette:

Grâce à la sécurité UV, il est plus difficile de commettre une fraude de contrefaçon, car la réplication de la sécurité UV ne peut être accomplie avec une imprimante / fabricant de cartes facilement accessible. Cependant, à l'instar d'autres méthodes de prévention de la fraude basées sur la création de la carte, cette méthode en elle-même ne fait rien pour arrêter la fraude intellectuelle.

* * *

Toutes les méthodes de prévention de la fraude mentionnées ci-dessus varient de différentes manières: dans l'organe légal de prévention de la fraude, dans la prévention (la carte physique, la codification légale, etc.) et le type de fraude qu'elles préviennent efficacement. Cependant, l'élément unique parmi eux est qu'ils empêchent la fraude en la rendant plus difficile à faire, pas en l'empêchant de se produire. C'est-à-dire que si un fraudeur a l'intention de commettre une fraude, aucune de ces méthodes ne peut l'arrêter, mais cela devient plus coûteux et donc moins durable pour le fraudeur.

Donc, prévenir la fraude ne suffit pas. La fraude de document se produira toujours, et l'objectif conséquent est de détecter et arrêter l'utilisation du document frauduleux. À cette fin, bon nombre des méthodes de prévention examinées sont des outils utilisés par les méthodes de détection. Tout en analysant les méthodes de détection, on verra comment les normes et spécifications établies par l'OACI et d'autres organismes sont utilisées comme outils pour détecter la fraude.

[70] CTMS *op. cit.*
[71] *Ibid.*

Méthodes de déceler la fraude

La détection de la fraude est la suite logique de la prévention de la fraude documentaire. La prévention de la fraude, comme on l'a vu dans la partie précédente, n'est pas parfaite. Afin d'identifier et d'arrêter les cas de fraude documentaire qui n'ont pas été évités, il est nécessaire de disposer de moyens pour détecter les fraudes. Contrairement aux méthodes de prévention de la fraude documentaire, les méthodes de détection de fraude documentaire ne sont pas seulement développées par des entités gouvernementales, mais aussi des entreprises et des entreprises qui développent des solutions pour documenter la fraude dans un monde de plus en plus dématérialisé. Ces méthodes de détection travaillent en étroite collaboration avec les normes établies par l'OACI et le gouvernement français afin de détecter la fraude documentaire.

La détection de la fraude est construite autour de l'idée de la vérification. Les deux principaux types de détection de fraude documentaire sont les vérifications de documents et les vérifications de données; le premier vérifie la véracité du document d'identité lui-même, tandis que le second vérifie les informations d'identité (c.-à-d. les données) contenues dans le document d'identité. On étudiera dans quelle mesure ces méthodes détectent la fraude.

Les contrôles de document et d'identité

Le GBG[72], une entreprise d'assurance spécialisée dans la détection de la fraude documentaire, identifie quatre choses clés qu'un bon logiciel de détection recherche lorsqu'il cherche une fraude dans un document d'identité: son modèle, sa structure, sa qualité, et son intégrité.[73]Toute solution logicielle espérant détecter la fraude documentaire doit instituer ces quatre contrôles dans une certaine mesure. DocID, développé par Worldline, vise à mettre en œuvre ces contrôles sur différentes plates-formes pour valider les documents d'identité. Cette mémoire utilisera DocID comme étude de cas pour discuter des forces et des limites générales du logiciel de détection de la fraude, soit en raison de sa nature inhérente ou de l'état actuel de la technologie pertinente.

Le processus de DocID va généralement comme suit:

[72] Forme longue: “Global Benefits Group, PLC”
[73] GBG, PLC., “Document Validation”, *Global Benefits Group*, https://www.gbgplc.com/what-we-do/fraud-risk-compliance/manage-risk-prevent-fraud/document-validation/, 2018

Identifier / Choisir le type de document → Tentative de lecture des données des champs pertinents → Déterminer si les données sont correctement positionnées → Effectuer une vérification croisée des données récupérées correspondantes

Cette division du processus est faite afin d'appliquer les contrôles GBG au processus DocID. À chacune des étapes générales ci-dessus, l'un des contrôles (modèle, structure, qualité, intégrité) est appliqué. Chacune des étapes ci-dessus a le potentiel de détecter la fraude indépendamment.

Les contrôles de modèle

Chacun des chèques GBG est centré sur une question. Pour les vérifications de modèles, la question est: " Est-ce que le document est un document d'identité reconnu?[74] La première étape de DocID consiste à déterminer quel type de document est analysé en l'associant à un modèle de document potentiel, tel que déterminé par l'OACI: TD1, TD2, ou TD3. La forme DocID qui s'appelle DocID Serveur tente de déterminer d'abord quel type de document est en cours de traitement - c'est la vérification de modèle. S'il est capable de déterminer un type de document qui fonctionne, il continue. Sinon, il détecte une fraude potentielle et met fin au processus de validation. Malheureusement, sur d'autres plateformes de DocID (iOS, Android), l'utilisateur doit sélectionner le type de document, il n'y a donc pas de vérification de modèle.

Les contrôles de modèles dans les logiciels de détection fonctionnent en étroite collaboration avec les normes OACI définies dans le document 9303. Par conséquent, ces spécifications de document physique sont maintenant utilisées comme outils pour les logiciels de détection. Les contrôles de modèles sont en mesure de lutter contre les fraudes matérielles contrefaites, mais pas de détecter efficacement les falsifications, car le gabarit n'est pas modifié dans ce cas.

Les contrôles de structure

La question centrale concernant les contrôles structurels est " Est-ce que les informations et les éléments du document sont correctement positionnés et affichés?"[75] Après une évaluation générale du modèle du document d'identité, et suite à une identification réussie du type de document, un logiciel de détection utilise les spécifications spécifiques du modèle (les mesures de différentes zones,

[74] GBG, PLC. *op. cit.*
[75] *Ibid.*

l'organisation des champs de données, etc.) et voit si les éléments du document sont correctement positionnés.

DocID le fait lors de la validation des éléments dans la VIZ - il applique les spécifications établies par l'OACI pour le type de document précédemment identifié (TD1, TD2, TD3) et en essayant de reconnaître les données contenues dans les zones déterminées, implicitement le logiciel effectue des contrôles structurels. Si les données sont récupérées, la structure est vérifiée et est validée. Si les données ne sont pas récupérées, cela signifie que la structure des éléments de données dans le document d'identité est incorrecte et que le document pourrait être frauduleux.

Les contrôles de qualité

La fonction principale de DocID concernant la récupération et la validation des données est sa lecture de la MRZ, la zone lisible par machine, du document d'identité en cours d'analyse. Généralement, un logiciel de validation comme DocID utilise la vision par ordinateur et un logiciel de reconnaissance optique de caractères (OCR) pour y parvenir. DocID utilise OpenCV et Tesseract OCR pour extraire et analyser la MRZ, en récupérant les informations nécessaires. Au cours de cette lecture de la MRZ, un contrôle implicite de la qualité est effectué. Une vérification de la qualité répond à la question "Est-ce que les données contenues dans l'image du document peuvent être lues correctement?" [76]

Si l'OCR Tesseract réussit la reconnaissance MRZ, la qualité peut être assurée. Sinon, le document d'identité est invalidé et DocID échoue. Cependant, contrairement à d'autres contrôles, la fin prématurée de DocID en raison de l'impossibilité de lire le document par machine n'implique pas directement une activité frauduleuse. Le contrôle de qualité échoue pour de nombreuses raisons non frauduleuses: un document d'identité usé, une erreur faite par l'OCR (comme un caractère mal lu) ou une incapacité à lire à cause d'un problème d'éclairage (éblouissement, ombre, etc.).

Avec ce problème, on trouve le plus gros problème avec les méthodes de détection de la fraude documentaire; Souvent, un échec de validation d'un document n'est pas dû à une fraude documentaire, mais à des limitations technologiques[77] . De plus, les contrôles de qualité ne peuvent pas déterminer si les informations contenues (c'est-à-dire les données extraites de la MRZ) sont frauduleuses ou non.

[76] GBG, PLC. *op. cit.*
[77] Comme pour tout logiciel de validation, on discute des erreurs de type 1 et de type 2. Le problème discuté ici est la probabilité d'erreurs de Type 1 (faux positif): qu'un document valide sera incorrectement étiqueté comme frauduleux.

Les contrôles d'intégrité

Le GBG définit les contrôles d'intégrité en utilisant la question " Est-ce que l'information est valide et cohérente avec la véritable identité de l'individu?"[78] Les contrôles d'intégrité sont effectués dans l'application du contrôle croisé. En d'autres termes, les données extraites de la MRZ du document sont comparées aux données correspondantes dans des sources indépendantes afin de valider les informations sur le document d'identité et donc sur le document lui-même. Les données utilisées pour le contrôle croisé peuvent provenir de nombreux endroits. Par exemple, DocID effectue deux vérifications d'intégrité en interne. Premièrement, il vérifie les clés de contrôle (comme indiqué dans la partie précédente) de la MRZ. Ce sont des nombres correspondant au résultat de l'arithmétique modulaire; Si la clé correspond aux résultats de calcul de DocID, la vérification réussit - sinon, le document est frauduleux. Deuxièmement, DocID effectue un contrôle croisé entre les données extraites de la MRZ et les données extraites de la VIZ, en utilisant un algorithme pour calculer et renvoyer un score d'intégrité, censé résumer la force de la validité des données d'identité.

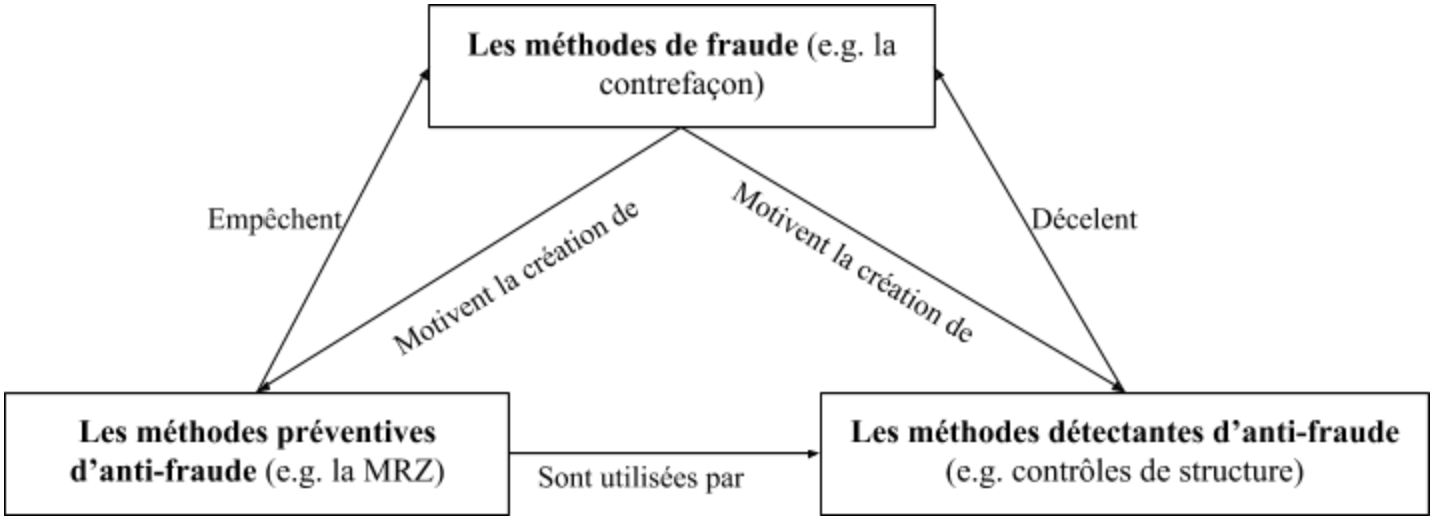
Alors que DocID effectue son contrôle d'intégrité via une référence croisée MRZ vs VIZ, d'autres solutions de détection avec accès à d'autres sources de données existent. Par exemple, une banque a généralement les informations personnelles de ses clients à partir du moment où elle a créé son compte. Par conséquent, si un client doit fournir son document d'identité comme preuve d'identité, les données de la MRZ et / ou de la VIZ peuvent être recoupées par rapport aux équivalents de données que possède la banque à partir de l'enregistrement. Les autorités nationales et internationales ont également accès à des bases de données: par exemple, INTERPOL a DISCS, une base de données contenant des certificats d'état civil tels que naissance, mariage, décès, identité et citoyenneté[79], tandis que le gouvernement français conserve des registres de naissance documents.

Si on peut garantir la légitimité de la source de référence, le contrôle croisé et par conséquent les contrôles de l'intégrité constituent le moyen le plus efficace de détecter toute forme de fraude matérielle. Toute falsification ou contrefaçon serait exposée sous un renvoi croisé. Néanmoins, les contrôles d'intégrité ne permettent pas de détecter la fraude matérielle dans deux cas: soit les données de référence ont été délivrées frauduleusement aussi, soit le fraudeur prétend être le détenteur légitime de la carte. Comme avec toutes les autres méthodes de prévention et de détection de la fraude, les contrôles d'intégrité ne sont pas très efficaces contre la fraude de documents intellectuels.

[78] GBG, PLC. *op. cit.*
[79] INTERPOL, *op. cit.*

Conclusion

Pour boucler la boucle, on réitère la problématique de cette mémoire : “Quelle est l’efficacité des méthodes informatiques dans la lutte contre la fraude des documents d’identités françaises ?” Pour bien répondre à cette question, il fallait créer un cadre qui bien relierait la fraude et l’anti-fraude. Ce cadre était établi au moyen du plan du développement, comme résumé dans le diagramme ci-dessous :



Avec ce cadre, on pourrait définir robustement comment on mesure l’efficacité d’une méthode anti-fraude : par analyser à quelle mesure une méthode réussit à empêcher ou à déceler la fraude documentaire.

Au cours du développement, on a trouvé et a analysé plusieurs méthodes anti-fraudes, dont la standardisation, la lisibilité par machine, et la référence croisée, entre autres. Indépendamment, chacune de ces méthodes ont une efficacité limitée; cependant, quand ces méthodes sont utilisées ensembles, ils réussissent à lutter bien contre quasiment toutes les méthodes de fraude documentaire *matérielle*.

Mais encore, les solutions techniques ne peuvent pas fournir une bonne réponse anti-fraude contre la fraude intellectuelle, parce que toutes ces méthodes concernent le document lui-même, et la fraude intellectuelle implique l’activité frauduleuse hors du document lui-même.

Néanmoins, il y a des technologies émergentes qui peut pas seulement améliorer les méthodes actuelles anti-fraudes, mais également créer les nouvelles méthodes contre même la fraude intellectuelle. Une de ces technologies développantes et la reconnaissance de personne basé sur une photo. La reconnaissance faciale est une technologie qui a existé toujours, mais jamais très efficace; cependant, avec les avancements dans le champ d'apprentissage machine, il y a déjà les tentatives à créer les solutions anti-fraude en utilisant la reconnaissance faciale et l'apprentissage machine qui sont en train d'être introduites aux conférences anti-fraudes.[80] Cette technologie pourrait améliorer beaucoup l'efficacité présente des méthodes anti-fraudes.

Malgré avoir les méthodes efficaces contre la fraude documentaire, il faut continuer de trouver plus de méthodes et également d'améliorer les méthodes actuelles, pour que le monde peut continuer de mondialiser et dématérialiser ses informations tandis que ne pas sacrifier la sécurité des gens et leurs ressources - pour garantir la croissance florissante de la France et du monde.

[80] European Conference on Artificial Intelligence - "Facial Recognition applied on the Identification of Fraudulent Documents" - *European Conference on Artificial Intellgience, 2016* - Institute of Electrical and Electronics Engineers (IEEE) - La Hague, Pays-Bas - 2016

Abstract

This paper analyzes the effectiveness of existing technological solutions combatting document fraud, specifically in the French context. To do so, it first determines the ways fraud is effectuated, then sees how well the anti-fraud methods resolve the problems raised by the fraudulent methods. It identifies two kinds of anti-fraud solutions - preventative and detective - which also interact with one another, as methods of detection use the standards set forth by methods of prevention. This paper concludes in saying that currently existing methods of fraud prevention and detection work in concert to effectively hinder material document fraud (that is, fraud that involves direct manipulation or counterfeit of the identity document), but is unable, both by practical and theoretical limitations, to resolve intellectual document fraud, such as imposterhood. The paper concludes by looking to future technologies, such as deep machine learning and advanced computer vision, to be applied to facial recognition and other anti-fraud relevant technologies.

Bibliographie

Assemblé de l'OACI, "Resolutions adopted by the Assembly", *OACI*, https://www.icao.int/Security/FAL/Documents/a39_res_prov_en%20A39-20%20B.pdf, 6 mars 2016. 6 p.

Boitteaux Pascaline, "Gare aux fraudes lors des paiements en ligne", Statista, https://fr.statista.com/infographie/ 11144/gare-aux-fraudes-lors-des-paiements-en-ligne/, 19 septembre 2017

Bolton R., Hand, D. - "Statistical Fraud Detection: A Review (With Discussion)" - *Statistical Science* - Project Euclid - 2002 - pp. 235–255

CTMS, "Comment on décèle une fausse carte d'identité ?", *CTMS*, https://www.ctms.fr/fraude-documentaire/ content/239-comment-déceler-une-fausse-carte-d'identite-, 23 mars 2018.

La DNLF, "Le rôle de la DNLF", *Ministère de l'Economie*, https://www.economie.gouv.fr/dnlf/role-dnlf, 6 avril 2016

Délégation nationale à la lutte contre la fraude (DNLF) – *Lutte contre la fraude aux finances publiques. Bilan 2016. - Paris* - Ministère de l'action et des comptes publiques, La République Française - 2016 - 108 p.

Esteves Helena - "Introduction to fraudulent methods used in travel, identity and visa" - *in ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - Esteves Helena - Victoria Falls, Zimbabwe – L'Organisation de l'Aviation Civile Internationale – 2012

European Conference on Artificial Intelligence - "Facial Recognition applied on the Identification of Fraudulent Documents" - *European Conference on Artificial Intellgience, 2016* - Institute of Electrical and Electronics Engineers (IEEE) - La Hague, Pays-Bas - 2016

Feuvre Christophe, "NATIONALITÉ, CITOYENNETÉ FRANÇAISE ET CITOYENNETÉ EUROPÉENNE", *Le Livre Scolaire*, https://www.lelivrescolaire.fr/#!manuel/62/histoire-geographie-education-civique-3e/chapitre/833 /natonalite-citoyennete-francaise-et-citoyennete-europeenne/document/715203, 2014

Fulmer Lori, "Global Card Fraud Losses Reach $16.31 Billion — Will Exceed $35 Billion in 2020", Business Wire, https://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reac h-16.31 -Billion, 4 août 2015

GBG, PLC., "Document Validation", *Global Benefits Group*, https://www.gbgplc.com/what-we-do/fraud-risk-compliance/manage-risk-prevent-fraud/documen t-validation/, 2018

Hoofnagle Chris Jay - “Identity Theft: Making the Known Unknowns Known” - *in Harvard Journal of Law and Technology (Vol. 21)* - Harvard University - Berkley, Californie – Harvard University – 2007

INTERPOL, “Counterfeit currency and security documents”, *L’Organisation internationale de police criminelle*, https://www.interpol.int/Crime-areas/Financial-crime/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud, 13 juin 2017.

McKenna Frank, “Card Fraud in Europe is Higher than Ever”, Business Wire, https://frankonfraud.com/fraud- trends/card-fraud-in-europe-is-higher-than-ever/, 14 juillet 2017

L’OACI, “The History of ICAO and the Chicago Convention”, https://www.icao.int/about-icao/History/Pages /Default.aspx, 2015

L’OACI - “Partie 4 : Spécifications pour les passeports lisibles à la machine (PLM) et autres DVLM de format TD3” - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L’OACI - Montréal, Canada – L’Organisation de l'Aviation Civile Internationale – 2015 - 38 p.

L’OACI - “Partie 5 : Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD1” - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L’OACI - Montréal, Canada – L’Organisation de l'Aviation Civile Internationale – 2015 - 36 p.

L’OACI - “Partie 6 : Spécifications pour les documents de voyage officiels lisibles à la machine (DVOLM) de format TD2” - *in Doc 9303: Documents de voyage lisibles à la machine, 7e édition* - L’OACI - Montréal, Canada – L’Organisation de l'Aviation Civile Internationale – 2015 - 32 p.

L’OACI, “Vission and Mission”, *OACI*, https://www.icao.int/about-icao/Council/Pages/vision-and-mission, 2017

Olson Eric T. - "Personal Identity" - *The Stanford Encyclopedia of Philosophy* - Zalta Edward N. (ed.) - Stanford University - San Francisco, Californie - 2002 - 43 p.

L’Organisation de l'Aviation Civile Internationale - *ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - L’Organisation des Nations Unies – Port Victoria, Zimbabwe - 2012 - 673 p.

Quarmby Ben - *The case for national identification cards, 2003 Duke L. & Tech. Rev. 0002*. - Duke University - Durham, Caroline du Nord - 2003 - 34 p.

La République Française, “Décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité”, *LegiFrance*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006060725, 5 novembre 2017

La République Française, “Lutte contre la fraude documentaire”, *DNLF*, 2016.

Service Publique, “Carte nationale d'identité d'un majeur”, *La République Française*, https://www.service-public.fr/particuliers/vosdroits/F1341, 23 mars 2018.

Siciliano Mauricio - “THE ICAO MRTD PROGRAMME” - *in ICAO Regional Seminar on MRTDs, Biometrics and Border Security* - Siciliano Mauricio - Victoria Falls, Zimbabwe – L’Organisation de l'Aviation Civile Internationale – 2012 pp. 27-28

“US Payments Forum provides guidance on card-not-present fraud”, Payments, http://www.paymentscardsand mobile.com/guidance-on-card-not-present-fraud/, 24 mars 2017