Received: 2 November 2023 | Revised: 14 May 2024 | Accepted: 15 May 2024

DOI: 10.1002/wfs2.1528

ADVANCED REVIEW

WIREs FORENSIC SCIENCE WILEY

Forensic intelligence: Expanding the potential of forensic document examination

Ciara Devlin[1] | **Marie Morelato**[1] | **Simon Baechler**[2,3,4]

[1]Centre for Forensic Science, University of Technology Sydney, Sydney, New South Wales, Australia

[2]Police Judiciaire, Police Neuchâteloise, Neuchâtel, Switzerland

[3]Ecole des Sciences Criminelles, University of Lausanne, Lausanne, Switzerland

[4]Groupe de Recherche en Science Forensique, Université du Québec à Trois-Rivières, Québec, Canada

Correspondence
Simon Baechler, Police Judiciaire, Police Neuchâteloise, Neuchâtel, Switzerland.
Email: simon.baechler@unil.ch

Edited by: Claude Roux, Editor-in-Chief

Abstract

Forensic document examination is characterized by its longevity, diversity, and evolution over time. Predominantly, published research within this field has focused on handwriting examination, the articulation of forensic conclusions, and the development of technical instrumental advancements, focusing on the use of document examination in the resolution of casework. This is a persistent and common problem within forensic science that Kirk identified in 1963 and that other authors have reaffirmed more recently. Ultimately, this has resulted in the potential of forensic intelligence, remaining relatively underexplored in the field of document examination. Forensic intelligence is a different way to view and analyze traces, shifting the focus from the traditional identification of source and activity, to instead identifying trends in criminal activity to assist in the reduction, prevention, and proactive disruption of crime. Despite a distinct disparity between these strands of research, there has been a persevering evolution toward the implementation of a systematic forensic intelligence method for the examination of fraudulent identity documents. Since its initial inception into the research community, this method has expanded and been implemented across Europe, and Canada, with tests also being conducted in Australia. These first tangible steps toward a forensic intelligence capacity within document examination have also inspired new work using forensic intelligence and systematic comparisons within the field of handwriting examination, as well as the recognition of the transversal potential of this method, with it being applied to both physical and digital documents. In this review, the fields of document examination and forensic intelligence will first be introduced, along with a subsequent examination of the research that has led to the creation of a forensic intelligence model within the field of document examination. It should be noted that this review has largely been limited to a review of

research that has been published in English and French due to the language of the authors.

This article is categorized under:

Crime Scene Investigation > From Traces to Intelligence and Evidence

Forensic Chemistry and Trace Evidence > Emerging Technologies and Methods

Crime Scene Investigation > Epistemology and Method

KEYWORDS

documents, forensic profiling, fraudulent documents, handwriting, security documents

1 | INTRODUCTION

1.1 | Forensic document examination

For as long as the written word has existed, the practice of forgery and questions pertaining to authorship have remained ever-present; with the use of document "expert testimony" being traced back to the Roman Empire (Huber & Headrick, 1999). In these early instances, forensic document examination was focused on the examination of handwriting, reflecting the sole means through which documents could be created. The main question in these cases was generally simple doubts of authorship, and largely relied upon witness testimony and circumstantial evidence (Huber & Headrick, 1999). In time, this practice evolved and became more comprehensive, often with judges and juries conducting their own handwriting comparisons in combination with testimony from recognition witnesses; individuals who were in some way acquainted with the writing of the alleged author and could provide evidence based on this familiarity (Huber & Headrick, 1999). Despite the obvious issues and inconsistencies introduced by these recognition witnesses, it was not until the 20th Century that those giving evidence became closer to what we now recognize as expert witnesses.

This shift, along with the recognition of handwriting examination as a definitive field, specifically within English-speaking countries, has been attributed largely to the works of Daniel T. Ames and Albert S. Osborn, specifically, "Questioned Documents" published in 1910 (Huber & Headrick, 1999; Lewis, 2014; Riordan et al., 2012). In his work, Osborn expanded the scope of the field to include typewriting, paper, and ink examination, creating the framework for modern forensic document examination (Ellen et al., 2018; Harrison, 1958; Hilton, 1979; Huber & Headrick, 1999; Kelly & Lindblom, 2006; Riordan et al., 2012).

The evolution of computers and digital technologies throughout the 1980s further expanded the breadth of the document examination landscape. In the decades since, constant developments in document creation, editing, processing, and examination techniques have coalesced into our current understanding of document examination. While the work of a forensic document examiner (FDE) generally revolved around the examination and comparison of handwriting, it has expanded to typically include: the comparisons of handwriting, hand printing and signatures; the identification of alterations, deletions, and substitutions; the detection of obliterations; the examination of typewriting; commercial printing processes; computer printing; comparisons of mechanical and electronic impressions; comparison of indentations in documents; the detection of counterfeits; the restoration of damaged documents; the comparison of inks and paper; determining the authenticity of documents and identification; and document dating (Ellen et al., 2018; Kelly & Lindblom, 2006; Leaver, 2006, 2011). Document examination has consistently proven its relevance in criminal, civil, and administrative cases, and illustrated that it can be a great source of information, especially in providing links between individuals, events, crime scenes, and locations (Ellen et al., 2018; Hammond, 2013).

On a base level, the primary duties of an FDE are case dependent; however, in general, according to conventional sources, an FDE conducts scientific examinations and comparisons of documents to:

- Determine a document's authenticity and in doing so expose and reveal any alterations, deletions, or additions.
- Exclude or identify an individual as the source of a questioned handwriting.
- Exclude or identify the source of typewriting, printings or other impressions, marks, or relative evidence.

1.1.1 | Document security

Secure documents are those that contain any kind of monetary value, data, or information about the holder of the document (Ombelli & Knopjes, 2008), such as banknotes and other currency, along with identity and travel documents such as passports, driver licenses, and identity cards. Termed "secure documents" due to their embedded security features meant (1) to prevent or hamper illegal alteration, replication, or manufacture; and (2) to enable the assessment of their authenticity, these documents have long been the target of counterfeits and forgery due to their value, both monetary and socio-economic (About & Denis, 2010; Fahrmeir, 2001; Groebner, 2007).

Security documents act as the cornerstones for many aspects of modern social and economic life. While the value of currency is rather self-explanatory, the intrinsic value of identity and travel documents is somewhat more complex, as they provide individuals with access to a range of entitlements and resources such as security, health care, travel, access to property and governmental benefits (Ombelli & Knopjes, 2008). Identity and travel documents are secure documents that prove a person's identity through the inclusion of personal information such as photograph, name, and date of birth. Upon their widespread integration into society, the criminal element quickly understood the value of these documents, and the illicit market for their manufacture and distribution was quickly established. The international market for fraudulent identity and travel documents has continued to grow at such a rate, that document fraud is now considered a prolific, pervasive, and resilient crime problem that enables all other serious and organized crime (Europol, 2017).

While these forms of documentation have increased their security measures and made their manufacture much more specialized over time, there is still a strong criminal environment for document fraud (About & Denis, 2010; Fahrmeir, 2001; Groebner, 2007). Consequently, there is a basis for the argument that as the value behind these documents and the number of benefits they afford has increased, so too has the desire to produce, distribute, and use fraudulent versions (Europol, 2021, 2024; Frontex, 2019). The expansion of criminal enterprises has similarly resulted in the development of several different types of fraudulent documents, with the most often encountered including counterfeit documents, forged documents, and pseudo (or fantasy) documents. The terminology behind these documents' bears defining and is summarized in Table 1. These definitions are based on the methods, or modus operandi (MO) used by the forger(s) to create or alter them, linking back to Locard's principle (Locard, 1920). The method of alteration or manufacture (the activity undertaken by the forger to create the document) directly impacts what traces are left by the forger, therefore dictating what the FDE may observe and analyze on a given document (Baechler & Margot, 2016).

While a counterfeit or a pseudo document is manufactured from raw materials, a forgery is instead a genuine document that has been altered. A pseudo document, on the other hand, is one that is not officially recognized by any authority, this could be a document claiming to originate from a completely fictitious country, or it could be a completely fictitious document type from a legitimate country (INTERPOL, 2019; Trubshoe & McGinn, 2013). These documents will often have the appearance of a legitimate identity document, and are often those marketed as "novelty items" (Trubshoe & McGinn, 2013). An example of a psuedo document is shown in Figure 1. It has been manufactured to look like a non-restricted Australian driver license from New South Wales (NSW); however, a "NSW Student Identification" card is not an officially recognized document.

For the sake of concision, other MO are not described here since they are much less frequent (such as stolen blank documents) or beyond forensic interest since the document itself is genuine (such as a genuine document that was issued based on fraudulent information, or an impostor using the genuine document of someone else).

The examination of security documents does not lie exclusively in the hands of FDE's. Many organizations throughout the world, such as banks, border police and security organizations have created in-house document expert units

TABLE 1 Main fraudulent document terminology and definitions as a consensus from various sources (Friedrich, 2001; INTERPOL, 2019; Levinson, 1984; Mathyer, 1980; Ombelli & Knopjes, 2008; Pfefferli, 2000; Trubshoe & McGinn, 2013).

Counterfeit	A completely unauthorized and illegally manufactured reproduction of a genuine document that includes features that attempt to replicate the layout and security features seen in a legitimate version
Forgery	A genuine document that has been partially altered to give misleading information (e.g., substituted photograph, addition of a vehicle category, erasure of an expulsion stamp)
Pseudo/fantasy document	A manufactured document that is not officially recognized by any authority, it is often made to look like a legitimate document type

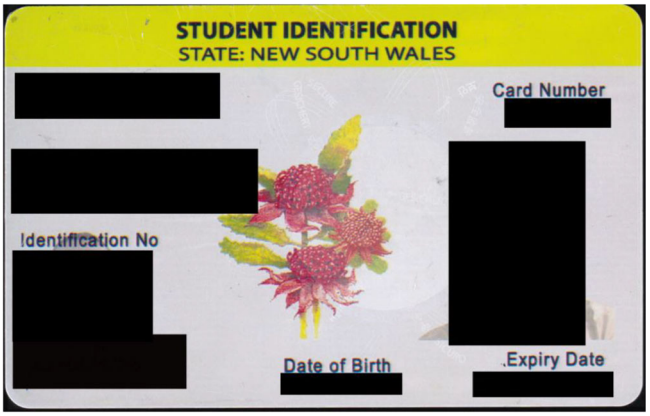

FIGURE 1 Example of a pseudo/fantasy document seized in New South Wales, Australia.

(Deviterne-Lapeyre & Ibrahim, 2023) that most of the time does not fall within the purview of forensic science. They simply apply a forensic approach to examining security documents. Depending on each nation's organization, some of these units collaborate with forensic science institutes on a regular basis, others do not. This has resulted in the forensic examination of security documents being somewhat split between two professional communities that in our opinion need to be more integrated, particularly to foster intelligence.

1.2 | Forensic intelligence

The concept of forensic intelligence, while increasing in prevalence, has remained enigmatic for many people (Coyne & Bell, 2011). This can be attributed to often inconsistent definitions for the field, with the term "forensic intelligence" having been used to simultaneously describe products, trends and processes depending on their context (Organisation for Security and Co-operation in Europe (OSCE), 2017). At its core, forensic intelligence is a different way of using traces, or remnants of criminal activity. Forensic science has conventionally focused on examining the features of a trace to elicit an answer or explanation relating to the source or activity behind its creation. Forensic intelligence builds on this and expands the scope, focusing more on the criminal activity itself to provide insights into security and the disruption, prevention and proactive reduction of crime (Cusson et al., 2008; Ratcliffe, 2008; Ribaux, 2023; Ribaux et al., 2022). The process relies on information collection, analysis, and interpretation and aims to assist decision-makers (e.g., policing and government organizations) in affecting change (Morelato, Baechler, et al., 2014).

Within forensic science, there has always been a strong focus on the resolution of cases within the judicial system, operating on a case-by-case paradigm (Morelato, Baechler, et al., 2014; Ribaux et al., 2013; Ribaux, Baylon, Lock, et al., 2010; Ribaux, Baylon, Roux, et al., 2010). While this has continued to be effective in resolving individual cases, it is often restricted in its scope. Forensic intelligence aims to complement this method, acting in a more proactive way with a transversal multi-case focus, cross-checking information gained through the traditional judicial approach, along with other detection routes (e.g., data gathered outside criminal procedures, monitoring of websites selling illegal products, etc.) (Morelato, Baechler, et al., 2014). Expanding the possible routes of detection beyond the traditional limits of the judicial system enables a more objective, and thorough understanding of the criminal environment. Where previously a successful case might result in one conviction, the implementation of forensic intelligence would mean that the MO and traces collected from that scene could be examined and compared between other cases. Thus, highlighting possible similarities and potentially linking that perpetrator to multiple criminal acts (e.g., through the similarity of traces, or MO), or identifying patterns in victimization and the locations of criminal acts (i.e., "hot spots," being locations with high levels of repeat criminality). All these observations can then be used to assist decision-makers in actioning change that can reduce the overall scale of the type of crime being focused upon.

Generally, crime is punctuated by prolific offenders and the concept of recidivism, meaning that those individuals committing a crime are likely to have done so in the past and to continue doing so into the future (Morelato, Baechler, et al., 2014). While this is a concerning thought in general, it also ensures that forensic intelligence can be wielded as a powerful tool against recurrent criminal activities. The process relies on information collection, analysis and

interpretation and aims to assist decision-makers (e.g., policing and government organizations) in affecting change (Morelato, Baechler, et al., 2014).

A parallel has been drawn between the way that governments handled the COVID-19 crisis and forensic intelligence (Roux & Weyermann, 2020). Usually within medicine patients are treated individually, on a case-by-case basis, much like in police work. However, with the evolution of the COVID-19 pandemic it was identified that to reduce the pressure on the public health system, a proactive multi-patient approach was adopted to identify infection clusters to try and reduce contamination and spread of the disease (Roux & Weyermann, 2020). This proactive method of combatting the pandemic is mirrored in the multi-case forensic intelligence approach, detecting patterns in traces and criminal activities to reduce crime and criminal behaviors, all with the aim of reducing the harm to society (Roux & Weyermann, 2020).

2 | FORENSIC INTELLIGENCE THROUGH DOCUMENT EXAMINATION

The concept of using forensic intelligence in the field of document examination, while increasing in the last decade, has remained generally underexplored, with a relatively small amount of research dedicated to examining the forensic intelligence potential of security documents and handwriting. In 2023, Deviterne-Lapeyre and Ibrahim conducted a review of all the questioned document literature that had been published between 2019 and 2022. While 1014 papers were referenced and examined, only four publications (0.4%) had a focus on forensic intelligence, with most research focusing on the articulation of forensic opinions or on the development of technical instrumental advancements (Deviterne-Lapeyre & Ibrahim, 2023). According to this review, between 2019 and 2022 there were 1226 publications and conference presentations related to the topic of security documents, most of which focused on the authentication of documents and advancements to security features and printing processes (Deviterne-Lapeyre & Ibrahim, 2023). A similar trend was noted in their 2020 review of the literature published between 2016 and 2019, with only four of the 213 publications examined focusing on forensic intelligence (Deviterne-Lapeyre, 2020). This over-emphasis on forgery detection and authentication is also true when considering digital developments of document examination (Amjed et al., 2022; Bibi et al., 2022).

While authentication and forgery detection are admittedly important areas of document examination, the over-emphasis on this process makes it seem as though the only useful information to be gained from a document is its authentication status, that is, whether it is genuine or fraudulent. However, this is a very limited approach toward documents, as identifying a document to be fraudulent is simply the start of the next challenge, being the extraction of as much information and intelligence as possible from the document. Furthermore, the focus on developing more technical instruments to assist in the authentication and detection process results in an underutilization of information that can be gained from simpler, traditional examinations. Realistically, only a small number of fraudulent documents are ever of such a quality that highly sensitive and resource-intensive techniques are required to differentiate them from their legitimate counterparts (Baechler et al., 2012). This leads to most research having a limited impact on practice (Weyermann et al., 2008).

This imbalance is not anomalous to these review papers. Previous Interpol Forensic Science Managers Symposium (IIFMS) reviews of the forensic document examination literature showed a limited but growing mention of the notion of forensic intelligence, particularly since 2010 (Angstrom, 2004; Fritz, 2007, 2010; Partouche, 2013; Pfefferli, 2001). The lack of intelligence research within document examination is surprising given that ideas related to document intelligence can be traced back to Morton (1984), who suggested that once a document is identified as fraudulent, two further steps can be undertaken, the first one being to link the document to others based on the comparison of forensic features, the second one being common source attribution. Since this first notion of how document authentication could be extended, there have been numerous additions to this concept. Pfefferli et al. (1999), suggested that fraudulent documents should be compared with previous seizures to, based on forgery techniques, identify series, origin, and delivery routes. Friedrich (2001) extended this idea further, considering how the different forgery techniques in these documents could assist in the identification of vulnerabilities and the creation of new controls and stronger security features for future documents.

The gradual development of the ideas of document examination continued into 2004, with Ng et al. (2004) proposing the study of trends in MO within the manufacture of documents, and Estabrooks et al. (2004) suggesting that documents could be linked based on the quality of their printing. In a report published in 2010 about the use of forensic science to combat and prevent identity-related crime, experts from the United Nations Office on Drugs and Crime

"considered the feasibility of databases that would give law enforcement officials and forensic examiners access to sample genuine documents for comparison, and also compile information about forged and other illicit documents so as to permit identification of linkages to generate intelligence about identity-related crime offences and offenders" (United Nations Office on Drugs and Crime (UNODC), 2010). The experts also underlined the lack of awareness related to forensic intelligence amongst policing and forensic actors, as well as a lack of resources to engage in document intelligence (Morton, 1984; Ng et al., 2004; Pfefferli et al., 1999; United Nations Office on Drugs and Crime (UNODC), 2010). Despite this sporadic research that provided suggestions for ways that forensic intelligence could be implemented within document examination, what was still lacking within the field was a systematic forensic intelligence method that could be used to properly understand the pervasive and prolific document fraud criminal environment.

The manufacture and distribution of fraudulent documents occurs on a large scale (Pfefferli, 2000), so much so that document fraud is considered a "cross-cutting criminal threat [that] enables and facilitates most, if not all, other types of serious and organized crime" (Europol, 2017). Such documents have been used to facilitate a broad range of criminal activities such as the trafficking of illegal goods, drugs, and firearms as well as in human trafficking, migrant smuggling, large-scale fraud, and terrorist activities (Auberson et al., 2016; Australian Criminal Intelligence Commission (ACIC), 2017; Baechler, 2020; Baechler et al., 2013; Europol, 2011, 2017; Gordon, 2003; Jorna & Smith, 2017; Ombelli & Knopjes, 2008; Pfefferli, 2000; Schloenhardt, 1999; Schloenhardt et al., 2012; Trubshoe & McGinn, 2013; United Nations Office on Drugs and Crime (UNODC), 2013). As put by Kephart in 2015, "To terrorists, travel documents are as important as weapons" (Kephart, 2015). Beyond the use of fraudulent documents to enable serious crimes, the volume of document fraud is also a challenge, as underlined by the increasing rate of identity crime in Australia (i.e., the illegal production, possession, trafficking, and/or use of personal information and identity documents), of which document fraud is a key component and enabler (Jorna & Smith, 2017). Especially when considering that document fraud is not limited to the physical world, with the use of scans and images of identity documents for online identity verification creating another avenue through which the criminal environment can flourish, including over the internet and the dark web (Bellido et al., 2017; Borisova et al., 2018; Romagna, 2014, 2015). This is compounded further by the growing rate of demand for and production of fraudulent documents in Europe (Frontex, 2019).

The fraudulent document market, which operates on an international level, is punctuated by a small number of organized recidivists who are responsible for a disproportionately large number of the products for sale (Baechler et al., 2012; Europol, 2009; Willox & Regan, 2002). These offenders are so prolific that, whether they be individual forgers or large operations, their production volume has been recorded to range from hundreds of documents, up to millions (Baechler et al., 2012; Europol, 2009; Willox & Regan, 2002). In stark contrast to the proven organization and structure behind this criminal environment are the methods most often used by police and security organizations to combat this crime problem, and for many years, the fight against identity document fraud has been suffering from a reactive and case-by-case approach. Traditionally, organizations have placed a strong focus on authentication, the process of determining if a document is fraudulent or legitimate. This reactive method, while effective in detecting singular instances of forgery, neglects to consider what should happen to the document after it is identified as fraudulent, and instead, solely takes action against the individual using the document (Baechler et al., 2012; Baechler et al., 2013). Building upon the suggestions of earlier work, Baechler et al. took the first concrete step toward creating a systematic forensic intelligence method to assist in intelligence-led policing, a step that relied on the use of forensic profiling.

2.1 | Forensic profiling as a tool for forensic intelligence

In forensic intelligence the term "profiling" refers to the selection and extrapolation of information from a trace to generate a set of features (i.e., profile) that are characteristic or representative of that trace, like, for example, what is done in DNA profiling. This "profile" can then be used as is, or converted into a numerical form, to easily compare traces between sets (or instances of criminality) to determine linkages. In the realm of document intelligence research, three different types of features have been targeted, or profiled, to try and help address the ever-increasing criminal environment of identity document fraud; visual, digital, and chemical features. Outside of the examination of identity and security documents, there has also been research into the forensic intelligence potential of handwriting examinations, which is explored in Section 2.2.

2.1.1 | Forensic profiling of visual features

In 2011–2012, Baechler et al. postulated that visual features of fraudulent identity documents, such as their printing methods (e.g., if they use laser or inkjet printing), replication of security features, and/or errors in the document template, are traces that have been left behind during the manufacturing process (Baechler, 2015; Baechler et al., 2011, 2012). They proposed that these features could be used in a systematic forensic intelligence method that expanded on and complemented the traditional method of document examination techniques. Through the examination, profiling, and comparison of these traces, it is possible to identify similarities between documents, which can then be extrapolated to indicate the use of a similar method of manufacture, and in turn, the presence of a similar source. Beyond that, the intelligence produced can also provide insight into the criminal environment, highlighting trends or patterns relating to the manufacture and distribution of the documents. The major premise behind this method is that a source, whether that is an individual or an organization, will produce documents using the same MO. This MO will be based on what the source *knows*, such as their knowledge and techniques, what the source *has*, that is, the materials and equipment available to them, and also what the source *is* in terms of their physiological characteristics (Baechler et al., 2012). Utilizing all this information, the method highlights a "trademark" or "signature" aimed to link instances of criminality, and potentially indicates the presence of organized crime groups, while also providing more accessible information about the criminal environment surrounding document fraud. This method is summarized in Figure 2.

Within the method (illustrated in Figure 2), once a document is seized, it is visually examined under white light and UV light, and features of interest are then identified. The features that are targeted are those that are intrinsically linked to the method of manufacture of the document and include things such as the replication of security features (UV features, security threads, optically variable devices, microprinting, etc.), the printing processes used, serial numbers, fonts, and errors in the machine-readable zone (Baechler et al., 2012).

To create the profiles of the documents, these features are then codified, often converting the features into numeric values, as illustrated in Table 2. These numeric values are then compiled to create the profile of the document, as an example, the profile of the document from Table 2 would be *[1,3,526,507,084,1]*. This profile would then be stored and structured within a memory where the profile is compared systematically to all other documents of the same type using optimized comparison metrics. The result of this process is a similarity score (ranging from 0 to 100) which indicates the level of affinity between the profiles, with 0 indicating no similarity between any of the features, and 100 indicating that all features within the profile of the two documents correlate. Depending on the threshold set by the operator, these similarity scores can be interpreted as being either the presence or absence of a link. If a link is present, then the documents could have been produced by the same manufacturing method or MO, and they can therefore be considered as likely sharing a common source (Baechler et al., 2012; Baechler et al., 2013; Baechler & Margot, 2016).

Beyond this level, the relationships are further analyzed and treated with external information to provide deeper meaning and to enable spatial and temporal trend analysis, highlighting trends in manufacture, distribution, and use of the documents. This can then be communicated to decision-makers, in the form of intelligence alerts or reports.

To prove the theories postulated by the initial study, the researchers conducted a proof of concept pilot study, in which they examined a collection of 393 fraudulent documents that originated from a pre-existing database used to assist in the authentication process (Baechler et al., 2012). Four different groups of documents were examined, and 25 visual features were extracted for each document, codified, and then compared. Of the four document groups the highest percentage of links occurred in the counterfeit Portugal identity cards where 68% of the 170 documents were linked to at least one other document (Baechler et al., 2012). Compared with traditional investigative techniques, the forensic intelligence-based process proved to be more effective and efficient in detecting links between related documents, with the number of links detected increasing by more than double (Baechler et al., 2012). Similar results were obtained in a further study concerning 363 documents composed of counterfeit Portuguese identity cards, counterfeit French identity cards, and stolen blank French passports (Baechler & Margot, 2016). Two-thirds of the documents examined were linked to at least one other document, with 30%–45% of the documents being linked to four or more documents.

These research works not only proposed a novel forensic intelligence model to combat document fraud, but also used that method to clearly illustrate the level of organization present within the document market, illustrating the underlying structure of criminal networks and prolific offenders. Before this research, it had been assumed within the document examination field that such structure did exist, now, with this work researchers and practitioners have tangible forensic intelligence supporting that the criminal environment for document fraud is organized.

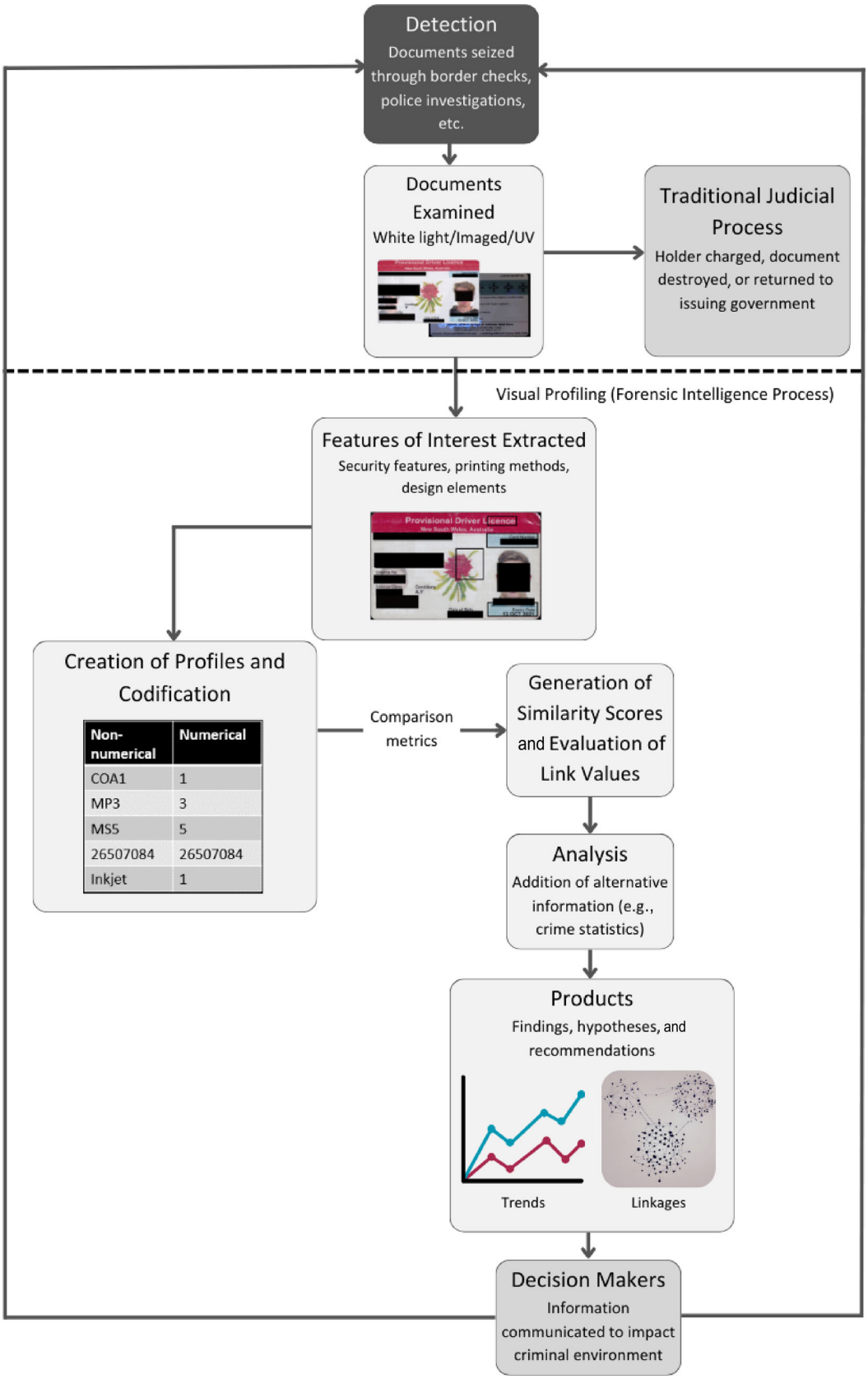

FIGURE 2 The forensic intelligence process for fraudulent identity documents. Adapted from Morelato, Baechler, et al. (2014).

TABLE 2 Example profile of a document, illustrating the conversion from features to the numerical profile.

Feature	Shortened profile	Numerical
Coat of Arms Style 1	COA1	1
Microprinting Style 3	MP3	3
Magnetic Strip Style 5	MS5	5
Serial/ID number	26,507,084	26,507,084
Inkjet printing	1	1

A subsequent validation study used 347 documents of three different types that were seized across France and Switzerland between 2000 and 2012 (Baechler et al., 2013). As 68 of these documents were known to have originated from nine different sources, due to the dismantling of document factories through police investigations, the authors were able to assess the ability of the forensic profiling method to attribute documents to a common source. The performance of the method was examined through Type I (false positive) and Type II (false negative) error rates, using both a binary classification system and likelihood ratios. In both methods, the error rates remained below 0.75% when operating in optimized conditions, well within the acceptable uncertainty range of forensic intelligence (Baechler et al., 2013). Admittedly, the intra-variability was limited in this examination as the documents seized from the same source were produced in a relatively short period of time before the seizure. However, even if produced across a broader timeline, the reported error rates of the profiling method were considered low enough to be acceptable within a forensic intelligence paradigm.

The potential of this profiling method has been recognized since Baechlers' initial work, so much so that a systematic method for the profiling of fraudulent identity documents was created and has been used in an operational context since 2017 in Europe and Canada (R. Volery, & M. Tapps, oral communication, 2022). This system known as ProFID (standing for Profiling Fraudulent ID documents) was initially developed by the School of Criminal Justice of the University of Lausanne in collaboration with forensic document experts from Swiss and European law enforcement agencies. Using visual features, it facilitates the profiling and comparison of fraudulent identity documents to assist in identifying those likely to have been produced by the same source (Ribaux et al., 2022). Documents are examined, with their technical characteristics being described, before being scanned and uploaded into ProFID. Once within the secure web platform, the profiling of the document is carried out and a comparison is done between the new document, and all documents of the same type within the system (Ribaux et al., 2022). Between 2017 and 2020, 2000 documents were integrated into the ProFID system, which revealed 51% of those documents belonged to one of 150 identified series (Baechler, 2020). In addition to the facilitation of the manual profiling and comparison, automatic image comparison methods based on computer vision have also been integrated within ProFID to assist in the identification of series, and this will be discussed further in Section 2.1.2.

The method has been further refined with the research conducted by Moulin et al. (2022). This work investigated how an efficient, and more standardized method could be applied to the profiling workflow of ProFID. Given the often-subjective nature of profiling visual characteristics, Moulin et al. endeavored to create a more standardized method for the use of ProFID, profiling and the identification of series. To move the method forward, they took inspiration from the ACE method that was first introduced into document examination by Huber (1972), defining the steps of the method, from the documents initial inception into ProFID, through its analysis and profiling of its features, its comparison to other documents within the database and finally its evaluation of its series status. One of the main points of interest in this article is the evaluation of the method that they developed. When comparing the performance of a set of professionals using ProFID before and after introducing the new method, the participants were able to detect similarities more quickly and with greater confidence. The use of the method, along with its clear definitions and delineations between classes of characteristics, enabled the professional examiners to more clearly explain how they had identified the links and series of documents. Furthermore, they conducted similar evaluations of the method using forensic science masters' students, and similar results were obtained (Moulin et al., 2022).

The document profiling approach and ProFID have also proved to be effective at a cross-border level. Documents seized across France and Switzerland (434 and 2143, respectively) were examined to identify the potential of cross-border comparisons of fraudulent identity documents. Using the method previously published by Moulin et al. (2022), it was found that 19% of the documents examined from France and Switzerland were linked to documents from the

other country, identifying 33 Franco-Swiss series that totaled 484 documents (Moulin et al., 2024). These transnational links extended the series that were previously identified on a national level, illustrating the contribution of forensic intelligence to investigations and cross-jurisdictional cooperation (Moulin et al., 2024). This research resulted in the founding of the ISF ProFID project funded by the Internal Security Fund—Police of the European Commission (project ISFP-2020-AGPOLCOP no. 101036247). Forensic and law enforcement agencies from 16 European countries are involved in this project with the support of several international organizations, namely Frontex, Europol, CEPOL, and Interpol. In this framework, more than 400 document examiners were trained across Europe to use the ProFID system and above 11,000 fraudulent documents were profiled, revealing around 500 series associated with potential organized crime groups. This underlines the key contribution forensic intelligence can bring at the international level (Ribaux et al., 2022).

In an operational sense, the method has shown great success in impacting the criminal environment of document fraud and organized crime. As an example, in 2020, the forensic profiling and comparison method was vital in the detection of an organized crime group's activity and in building the case that led to the arrest of nine suspects involved in document fraud that had facilitated the illegal immigration of North African migrants (Europol, 2021). Similarly, a paper published in 2017 claimed to have successfully dismantled a criminal group in Spain through the forensic profiling and comparison of fraudulent identity documents, illustrating the use of document profiling in a different geographical context. However, in this case, the specifics of the method were not provided, so its validity and similarity to other document profiling work could not be established (De Alcaraz-Fossoul & Roberts, 2017).

Noticeably, most of this research has been published and executed in Europe and Canada, so the question remained as to whether its success could be replicated in a different geographical context. Recently, within Australia, Devlin et al. illustrated the potential organization and structure behind the Australian fraudulent document marketplace (Devlin et al., 2022). Again, while this level of organization has been assumed in the document examination field, there has only been limited research published around the world that illustrates this structure. Overall, these international adoptions of the method clearly illustrate its potential, along with its transversality in that it can easily be applied to a range of document types, with similar methods even being used on counterfeit currency (Fürbach, 2013).

2.1.2 | Forensic profiling based on image processing techniques

Where the original work by Baechler et al. focused on the comparison of manually extracted visual characteristics, there has been increasingly more research dedicated to investigating the application of the profiling method in a more digital space. Given that much of forensic intelligence aims to produce actionable intelligence as efficiently as possible, there has been some research focusing on how the profiling method could be made more efficient with the addition of an automated triaging step, while also adding another aspect of comparison. Not replacing the human manual method, rather, complementing it, promoting a human–machine coupling approach.

In these methods, researchers began investigating the use of a combination of image processing filters and data processing techniques, to assist the manual profiling method and to introduce a degree of automation into the characteristic extraction (Talbot-Wright et al., 2016). This method was further developed by Auberson et al. who introduced the use of a computer vision-based method into the previously established intelligence framework (Auberson et al., 2016). Inspired by methods used to manage digital images of Ecstasy tablets, it was postulated that, in the same way that similarities in visual characteristics of the documents could be used to indicate a community of source, so too could similarities in image processing methods such as color, hue, and texture. After the document was scanned, a semi-automated selection of regions of interest was performed, after which they were imported into an image collection management system. These images were then filtered using 10 common image processing tools: red/green/blue; gray levels; hue/saturation/brightness; texture and edge. Profiles were derived from the histograms from each image and were subsequently compared using metrics. These metrics produced a similarity score which indicated the affinity between profiles. The method was applied to a data set of 32 counterfeit Portuguese passports and 26 counterfeit Italian driving licenses, and much like the original profiling method, showed very promising results. The counterfeit Italian driving licenses were classified with an exceptionally high accuracy of 92.4%, with the counterfeit Portuguese passports close behind with an accuracy of 90.3% (Auberson et al., 2016). While the accuracy rates of the validation set were somewhat lower with an accuracy of 71.4% and 88.2%, respectively, the misclassifications encountered were often due to differences in the physical appearance of the licenses, either due to wear and tear, fading, or inconsistent ink supply during the original printing of the document. Used in conjunction with the original profiling method, it

provided a rapid triaging system to help explore large data sets and indicate potential classes, clusters, or relationships that warrant further examination (Auberson et al., 2016). This provided the basis on which the automated image comparison approach implemented in ProFID was developed.

In a similar vein, work by Vieira et al. (2016, 2017) looked at the use of digital image processing techniques and algorithms. Their work specifically focused on digitally examining texture analysis, image areas, and imperfections in text areas to identify points of similarity between documents. These algorithms (including those such as Harris Corner Detection and Scale-Invariant Feature Transform) produced a percentage score to indicate the degree of similarity between documents. In this paper, Vieira et al. tested their algorithms through the comparison of an image of the Coat-of-Arms of the Portuguese Republic (which is a part of the Portuguese identity card) to a database of 1368 images that included forged images of both the coat of arms and the whole identity card (Vieira et al., 2017). This comparison only took 5 min and 32 s, and identified four images with a similarity to the input image of between 83% and 95%. The efficiency and results from this system are very promising, especially when considering the algorithms potential in triaging large document sets, however, expert validation of these comparisons is still required, as the algorithm is not flawless (Vieira et al., 2017).

Research work conducted by Girelli examined the forensic profiling potential of the fingerprints included on Brazilian identity documents (Girelli, 2015, 2016). They compared 100 images of fingerprints (and their laterally reversed images) collected from the internet to fingerprints present within the Brazilian Federal Police Automated Fingerprint Identification System (AFIS). After their AFIS search, they had 3434 HIT decisions between the fingerprint images from the internet and fingerprints examined as part of criminal cases, all related to fraudulent identity documents. As three of the HIT decisions were from laterally reversed images of the internet fingerprint images, they concluded that 31% of the fingerprint images from the internet were used in forged Brazilian ID documents (Girelli, 2016). Some of the identified criminal cases involved multiple fraudulent identity documents, all with the same fingerprint image used, clearly illustrating the potential of using the profiling of the fingerprints to assist in the identification of links between document sources (Girelli, 2016). This expansion of the profiling method to include the use of a well-established and common database is an excellent example of how already established facilities can be used to assist in the pursuit of forensic intelligence, minimizing costs, and maximizing the production of intelligence.

Most recently, in 2021 there was an investigation into the potential of using Formal Concept Analysis to assist in the detection of forgeries and grouping them together to help identify their origin and obtain details about the forgers activities (Ojeda-Aciego & Rodriguez-Jimenez, 2021). In this work, the authors describe the combination of a forger's mistakes as their *signature*, which can be taken as another way of describing the "profile" of a document. Formal Concept Analysis, in simple terms, can be seen as a conceptual clustering technique that compares sets of attributes (or features) between entities, in this case, fraudulent documents. In the work by Ojeda-Aciego et al., the different attributes within the profile are compared and marked true or false depending on whether the author successfully replicated the security measure. This leads to the "signature" (aka profile) of the document which is represented as a binary sequence of Boolean values that can be easily compared between documents. In this method, the focus appears to be on the forger's ability to replicate the details of the security measures embedded within the documents, which is a different approach when compared with the previous examples of fraudulent document profiling. With further research and validation of the method, it could be an interesting addition.

2.1.3 | The forensic profiling of chemical features

The use of chemical analyses within forensic document examination is widespread, however, the use of these chemical analyses within forensic profiling, that is, creating a profile for the document based off the result of chemical analyses, and then comparing those profiles between documents has been less explored within the literature.

With the use of plastics in documents increasing, Mireault et al. decided to investigate the potential of using chemical profiling on polymer substrates as an addition to the current profiling method (Mireault et al., 2017). Due to the highly variable nature of the composition of polymers, the researcher believed that they would be able to differentiate the chemical profiles of polymer cards from different sources and manufacturers using high-performance liquid chromatography—time of flight mass spectrometry (HPLC-QToF). In their case study, they examined 60 genuine and false driving licenses from Nigeria and Bangladesh, some of which were already identified to be linked due to their visual profiling. They found after their chemical profiling that the forgers were using a different plastic substrate from the genuine documents, and they were able to connect the visually linked documents based on their chemical profiles,

indicating that they were produced using the same MO and that the same substrate was used in their manufacture (Mireault et al., 2017). While this method is limited, in that it can only determine whether cards were made by the same manufacturer, it does have the benefits of enabling some profiling of blank polymer cards and substrates and would enable comparison between documents of different types, for example, driver licenses and identity cards, that would not be able to be compared based on the visual features. However, some of the main benefits of the visual profiling method are its accessibility, that is, the targeting of easy-to-access visual features that require no specialized training or specific equipment, its efficiency, and that the features can be extracted without damaging the document. The incorporation of chemical profiling, while providing an interesting new characteristic to compare, would reduce these factors.

2.1.4 | Value of security document profiling

Since its first postulation in 2011–2012, the potential of using forensic profiling in the examination of identity and travel documents has expanded from its roots of visual characteristics, to encompass digital and chemical characteristics as well. This, coupled with the implementation of the method and research conducted across Europe, Canada, and Australia illustrates the methods transversality and adaptability to different geographical contexts, feature types, and document formats. The value that this method provides in understanding a typically difficult-to-access criminal environment (being that of organized crime and the like), is expansive, and it will continue to grow as the use of the method broadens to more countries and geographical contexts, leading toward what we can only hope will become an international information sharing network that can help to proactively combat the fraudulent document criminal environment.

2.2 | The forensic profiling of handwriting

Given the success of the profiling method within the examination of security documents, and the information that provided about the criminal environment for document fraud, the potential of applying this systematic method to handwriting examinations was then explored.

According to published literature, a large portion of the work for FDEs revolves around handwriting examinations, including digital and physical handwriting (Agius et al., 2017). Traditionally, this area of document examination, much like the rest of the field, has had a strong focus on serving the judicial paradigm, with the main tasks of the FDE being to identify the source of a given piece of handwriting, detect questionable signatures, or to determine whether a single individual authored a series of documents (Ellen, 2005; Hilton, 1993).

Like many other traces analyzed in forensic science, handwriting exhibits both class and individual characteristics, however this area of forensic document examination is often debated within the field. For the sake of this research, we have considered class characteristics to be those that are built from the handwriting system that the individual was taught, influenced by their age and geography (Hilton, 1993; Huber & Headrick, 1999). This would therefore be common to a group of writers. We have also defined individual characteristics as those unique elements that distinguish writers, such as the individual habits that emerge as the writer begins focusing more on the subject matter being written rather than the writing process itself (Hilton, 1993; Huber & Headrick, 1999).

While most judicially driven handwriting examinations focus on looking at the individual characteristics of an authors' writing, the intelligence perspective instead focuses on the underutilized potential of the class characteristics. It is theorized that by understanding the teaching practices and systems taught within a particular country, it would be possible to analyze these class characteristics to indicate the nationality and academic background of the writer (Agius et al., 2017; Hilton, 1993). It has been well established in previous research that it is possible to identify different national, and in some cases regional, class characteristics within handwriting specimens depending on the alphabet or language used (Al-Hadhrami et al., 2015; Cheng et al., 2005; Muehlberger, 1989; Turnbull et al., 2010). Some authors examined the class characteristics in English handwriting of Polish, Hispanic, Chinese, Malay, and Indian authors (Al-Hadhrami et al., 2015; Cheng et al., 2005; Muehlberger, 1989; Turnbull et al., 2010). In all these works distinctions between the authors of different background were made based on the class characteristics of their handwriting. While admittedly, most of the research in this area focuses on examining English handwriting, a similar result was found in the examination of Arabic handwriting of authors from Morocco, Tunisia, Jordan, and Oman (Al-Hadhrami

et al., 2015). In these works, the potential for a forensic intelligence model was clear, however, the focus remained on identifying these class characteristics within the data set, rather than on proposing a forensic intelligence method for their systematic examination and comparison.

The work published by Agius et al. (2018) aimed to determine how the class characteristics of handwriting could be used within a forensic intelligence paradigm to infer a writer's country of origin. Inspired by the success of profiling and comparison methods implemented within the fields of fraudulent identity documents (refer to Section 2.1.1) and illicit drug profiling (Baechler et al., 2015; Esseiva et al., 2003, 2007; Guéniat & Esseiva, 2005; Ioset et al., 2005; Marquis et al., 2008; Morelato et al., 2013; Morelato, Baechler, et al., 2014; Morelato, Beavis, et al., 2014; Weyermann et al., 2008), the researchers set out to answer the question of whether these methods could be applied to handwriting.

Handwriting specimens were collected from 74 participants, 37 Vietnamese individuals who had learned English in Vietnam, and 37 English Australians who had learned to write in New South Wales (Agius et al., 2018). Much like the method proposed by Baechler et al. (2012, 2013), features of interest were extracted from the handwritten specimens before being codified to form the profiles. These features included the writer characteristics, such as their age and handedness, spatial characteristics, and construction characteristics. Using both a logistic regression model and a classification and regression tree model (CRT), 93% of cases were correctly classified, with three or less misclassifications occurring within each model. The agreement between these two very different statistical methods illustrates the accurate performance of the method and highlights its potential as a surface level screening method to detect patterns in handwritten material, such as address labels. However, the method was not without its limitations, one of the most obvious being the over reliance of profiling characteristics related to the letter "h." Of the five most effective characteristics identified from the logistical regression and CRT model, four of these were reliant on the presence of the letter "h." This will pose problems for non-prescribed handwriting specimens, and future work should perhaps trial the model using letters and words likely to be encountered on address labels, given the operational desire to use this method in indicating the country of origin of packages containing illegal goods or drugs (Agius et al., 2017; Agius et al., 2018). Furthermore, the method has focused on profiling the characteristics of only two nationalities, being Vietnamese and Australian, so further expansion is required to properly evaluate the potential of this method.

With the increasing use of digital media, the potential for the use of linguistics profiling within forensic science has been identified. Linguistics is the science of understanding the language system, enabling the examination of language structure to identify patterns within the spoken word, and more relevant to this work, written text such as e-mails, messages, contracts, letters, books, and the like (McMenamin & Choi, 2002). A recent article by Degeneve et al., examined the potential of computational linguistics, specifically textometry to investigate the fraudulent document market on the dark web (Degeneve et al., 2022). By examining the text written by vendors when creating their advertisements for their products, Degeneve et al. were able to not only illustrate the structure of this online marketplace for documents but also group those vendors based on the types of products being offered (Degeneve et al., 2022). The forensic linguistics field is expansive, so while this is just one example of this area, it is an interesting avenue worth mentioning, especially with increases in computer-mediated communication. However, given that this topic is outside the scope of this article, this area will not be explored further.

2.3 | Transversality of the forensic intelligence framework

Forensic science is becoming an increasingly specialized field, with almost all scientific sub-disciplines having a forensic counterpart (i.e., forensic biology, forensic chemistry, digital forensics, etc.). While advantageous in one respect, the most prominent effect of this is the reinforcement of siloes within forensic science that are detrimental to information sharing and proliferate linkage blindness and the wall effect. These eventualities are counterproductive and hamper the move toward a broader, intelligence-driven use of forensic information and traces (Baechler, 2020; Roux et al., 2012; Roux et al., 2021). The aim of forensic intelligence is to gain a broad picture of the criminal environment, study crime phenomena and enact change to reduce, prevent, and/or disrupt criminal activities. This relies heavily on not only the interpretation of trace information, but also information sharing between forensic specialties, organizations, and jurisdictions.

The key component of most of the forensic intelligence models within the literature (the majority of which are focused on illicit drugs) is the concept of profiling. External to the trace type being examined, the basic profiling method follows the same structure. Visual, physical, chemical, or digital characteristics of the trace are extracted and systematically compared with identify those with similar characteristics that have likely been produced by the same source while

differentiating between those created by different sources. These comparisons and profiles are then integrated into a memory that is constantly updated and evolving. In addition to the applications mentioned above relating to fraudulent identity documents, handwriting, and illicit drugs, iterations of the model have been used to profile and examine for instance counterfeit medicines and their packaging (Been et al., 2011; Dégardin et al., 2015; Dégardin et al., 2018), counterfeit luxury goods such as watches (Hochholdinger et al., 2019), and deliberate fires (Bruenisholz et al., 2017).

Interestingly, most forensic intelligence models proposed in the literature are falling prey to the specialization effect and have been developed to address a particular type of trace or problem (Baechler, 2020; Morelato, Baechler, et al., 2014). A transversal forensic intelligence method was proposed after Morelato et al. identified some marked similarities between two intelligence models developed for illicit drug profiling in Australia and fraudulent identity document profiling in Switzerland (Baechler et al., 2015; Morelato, Baechler, et al., 2014; Ribaux, 2023). This work proposed a general and multi-commodity model that could guide the use of forensic case data in an intelligence-led perspective. At its core, the authors identified that all forensic intelligence models, regardless of trace type, abide by the following forensic intelligence rationale; "the observation of similarity between the comparable features of different objects may indicate that these objects are repetitive effects of a same cause or type of cause" (Morelato, Baechler, et al., 2014).

3 | CONCLUSIONS

While still a niche field, forensic intelligence applied to documents has, early in its development, distinguished itself from the judicial, reactive, and authentication-driven focus still prevalent in general document examination, which while necessary, is limited when considering bigger picture crime reduction efforts. The work presented here has successfully proposed, and in several countries, implemented, a systematic forensic intelligence model capable of gathering intelligence from the comparison of fraudulent identity documents. This more phenomenological approach drives energy toward understanding complex, organized, and often hard-to-access criminal environments, providing intelligence to decision-makers to assist in affecting change.

Traces can provide a goldmine of intelligence if exploited properly; however, the general underappreciation of forensic intelligence results in a lot of unrealized potential. A change in the workflow of forensic document examination is required to fully take advantage of the information potential of documents, building on the wealth of knowledge within the field, to add another dimension where forensic intelligence can co-exist with the day-to-day operations of document examination. This of course must start with wider forensic intelligence-based education, not just of the individuals working on the front lines of document examination, but throughout the workflow structure, including management.

Overall, beyond authentication and forgery detection, documents have a lot to tell, and with the integration of forensic intelligence within the field, the contribution to fighting document fraud, identity crime and crime in general can be significantly expanded. Forensic intelligence through document examination should be regarded as a worthwhile research area, with concrete and fruitful applications. By exploiting existing traces present on the documents, and using readily available, accessible techniques, it is possible to gather useful and previously under-utilized information that can provide crucial insight into the criminal environment for document fraud. So, let's make documents talk.

AUTHOR CONTRIBUTIONS

Ciara Devlin: Conceptualization (equal); data curation (equal); formal analysis (equal); investigation (equal); methodology (equal); writing – original draft (equal). **Marie Morelato:** Investigation (equal); methodology (equal); project administration (equal); resources (equal); supervision (equal); validation (equal); writing – review and editing (equal). **Simon Baechler:** Conceptualization (equal); data curation (equal); formal analysis (equal); investigation (equal); methodology (equal); project administration (equal); resources (equal); supervision (equal); validation (equal); writing – review and editing (equal).

ACKNOWLEDGMENT

Open access funding provided by Universite de Lausanne.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Marie Morelato https://orcid.org/0000-0001-7616-0623
Simon Baechler https://orcid.org/0000-0002-1883-165X

RELATED WIREs ARTICLES

Towards another paradigm of forensic science?
The role of forensic science in the generation of intelligence to address environmental water contamination problems

REFERENCES

About, I., & Denis, V. (2010). *Histoire de l'identification des personnes*. La Découverte.

Agius, A., Jones, K., Epple, R., Morelato, M., Moret, S., Chadwick, S., & Roux, C. (2017). The use of handwriting examinations beyond the traditional court purpose. *Science & Justice*, *57*(5), 394–400. https://doi.org/10.1016/j.scijus.2017.05.001

Agius, A., Morelato, M., Moret, S., Chadwick, S., Jones, K., Epple, R., Brown, J., & Roux, C. (2018). Using handwriting to infer a writer's country of origin for forensic intelligence purposes. *Forensic Science International*, *282*, 144–156. https://doi.org/10.1016/j.forsciint.2017.11.028

Al-Hadhrami, A. A. N., Allen, M., Moffatt, C., & Jones, A. E. (2015). National characteristics and variation in Arabic handwriting. *Forensic Science International*, *247*, 89–96. https://doi.org/10.1016/j.forsciint.2014.12.004

Amjed, A., Mahmood, B., & Almukhtar, K. A. K. (2022). Approaches for forgery detection of documents in digital forensics: A review. Paper presented at the international conference on emerging technology trends in internet of things and computing, Erbil, Iraq.

Angstrom, N. (2004). Questioned documents – A review: 2001 to 2004. Paper presented at the 14th international forensic science symposium, Lyon, France.

Auberson, M., Baechler, S., Zasso, M., Genessay, T., Patiny, L., & Esseiva, P. (2016). Development of a systematic computer vision-based method to analyse and compare images of false identity documents for forensic intelligence purposes—Part I: Acquisition, calibration and validation issues. *Forensic Science International*, *260*, 74–84. https://doi.org/10.1016/j.forsciint.2016.01.016

Australian Criminal Intelligence Commission (ACIC). (2017). Organised crime in Australia.

Baechler, S. (2015). Des faux documents d'identité au renseignement forensique: Développement d'une approche systématique et transversale du traitement de la donnée forensique à des fins de renseignement criminel (PhD thesis). University of Lausanne.

Baechler, S. (2020). Document fraud: Will your identity be secure in the twenty-first century? *European Journal on Criminal Policy and Research*, *26*, 379–398. https://doi.org/10.1007/s10610-020-09441-8

Baechler, S., & Margot, P. (2016). Understanding crime and fostering security using forensic science: The example of turning false identity documents into forensic intelligence. *Security Journal*, *29*, 618–639. https://doi.org/10.1057/sj.2015.26

Baechler, S., Fivaz, E., Ribaux, O., & Margot, P. (2011). False identity documents profiling: A promising forensic intelligence method to fight identity document fraud. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, *64*(4), 467–480.

Baechler, S., Morelato, M., Ribaux, O., Beavis, A., Tahtouh, M., Kirkbride, K. P., Esseiva, P., Margot, P., & Roux, C. (2015). Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring. *Forensic Science International*, *250*, 44–52. https://doi.org/10.1016/j.forsciint.2015.02.021

Baechler, S., Ribaux, O., & Margot, P. (2012). 2012 student paper: Toward a novel forensic intelligence model: Systematic profiling of false identity documents. *Forensic Science Policy & Management*, *3*(2), 70–84. https://doi.org/10.1080/19409044.2012.744120

Baechler, S., Terrasse, V., Pujol, J. P., Fritz, T., Ribaux, O., & Margot, P. (2013). The systematic profiling of false identity documents: Method validation and performance evaluation using seizures known to originate from common and different sources. *Forensic Science International*, *232*(1-3), 180–190. https://doi.org/10.1016/j.forsciint.2013.07.022

Been, F., Roggo, Y., Degardin, K., Esseiva, P., & Margot, P. (2011). Profiling of counterfeit medicines by vibrational spectroscopy. *Forensic Science International*, *211*(1), 83–100. https://doi.org/10.1016/j.forsciint.2011.04.023

Bellido, L., Baechler, S., & Rossy, Q. (2017). The sale of false identity documents on the internet. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, *70*(2), 233–249.

Bibi, M., Hamid, A., Moetesum, M., & Siddiqi, I. (2022). Document forgery detection using source printer identification: A comparative study of text-dependent versus text-independent analysis. *Expert Systems*, *39*(8), e13020. https://doi.org/10.1111/exsy.13020

Borisova, B., Rossy, Q., & Baechler, S. (2018). La recherche inversée par image: un moyen pour débusquer les espaces de vente sur Internet pourvoyeurs de faux documents d'identité. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, *71*(4), 418–427.

Bruenisholz, E., Delémont, O., Ribaux, O., & Wilson-Wilde, L. (2017). Repetitive deliberate fires: Development and validation of a methodology to detect series. *Forensic Science International*, *277*, 148–160. https://doi.org/10.1016/j.forsciint.2017.06.009

Cheng, N., Lee, G. K., Yap, B. S., Lee, L. T., Tan, S. K., & Tan, K. P. (2005). Investigation of class characteristics in English handwriting of the three main racial groups: Chinese, Malay and Indian in Singapore. *Journal of Forensic Sciences*, *50*(1), JFS2004005-8. https://doi.org/10.1520/JFS2004005

Coyne, J. W., & Bell, P. (2011). The role of strategic intelligence in anticipating transnational organised crime: A literary review. *International Journal of Law, Crime and Justice*, *39*(1), 60–78. https://doi.org/10.1016/j.ijlcj.2011.02.003

Cusson, M., Dupont, B., & Lemieux, F. (2008). *Traité de sécurité intérieure*. Presses Polytechniques et Universitaires Romandes (PPUR).

De Alcaraz-Fossoul, J., & Roberts, K. A. (2017). Forensic intelligence applied to questioned document analysis: A model and its application against organized crime. *Science and Justice*, *57*(4), 314–320. https://doi.org/10.1016/j.scijus.2017.04.003

Degeneve, C., Longhi, J., & Rossy, Q. (2022). Analysing the digital transformation of the market for fake documents using a computational linguistic approach. *Forensic Science International: Synergy*, *5*, 100287. https://doi.org/10.1016/j.fsisyn.2022.100287

Deviterne-Lapeyre, C. M. (2020). Interpol review of questioned documents 2016–2019. *Forensic Science International: Synergy*, *2*, 429–441. https://doi.org/10.1016/j.fsisyn.2020.01.012

Deviterne-Lapeyre, M., & Ibrahim, S. (2023). Interpol questioned documents review 2019–2022. *Forensic Science International: Synergy*, *6*, 100300. https://doi.org/10.1016/j.fsisyn.2022.100300

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., & Morelato, M. (2022). The potential of using the forensic profiles of Australian fraudulent identity documents to assist intelligence-led policing. *Australian Journal of Forensic Sciences*, *55*(6), 720–730. https://doi.org/10.1080/00450618.2022.2074138

Dégardin, K., Guillemain, A., Klespe, P., Hindelang, F., Zurbach, R., & Roggo, Y. (2018). Packaging analysis of counterfeit medicines. *Forensic Science International*, *291*, 144–157. https://doi.org/10.1016/j.forsciint.2018.08.023

Dégardin, K., Roggo, Y., & Margot, P. (2015). Forensic intelligence for medicine anti-counterfeiting. *Forensic Science International*, *248*, 15–32. https://doi.org/10.1016/j.forsciint.2014.11.015

Ellen, D. (2005). Handwriting: The variations between normal writings. In D. Ellen, S. Day, & C. Davies (Eds.), *Scientific examination of documents* (3rd ed.). CRC Press.

Ellen, D., Davies, C., & Day, S. (2018). *Scientific examination of documents: Methods and techniques* (4th ed.). CRC Press (an imprint of Taylor and Francis).

Esseiva, P., Dujourdy, L., Anglada, F., Taroni, F., & Margot, P. (2003). A methodology for illicit heroin seizures comparison in a drug intelligence perspective using large databases. *Forensic Science International*, *132*(2), 139–152. https://doi.org/10.1016/S0379-0738(03)00010-0

Esseiva, P., Ioset, S., Anglada, F., Gasté, L., Ribaux, O., Margot, P., Gallusser, A., Biedermann, A., Specht, Y., & Ottinger, E. (2007). Forensic drug intelligence: An important tool in law enforcement. *Forensic Science International*, *167*(2–3), 247–254. https://doi.org/10.1016/j.forsciint.2006.06.032

Estabrooks, C., Gilmour, C., Park, H., Vallières, R., & Warias, C. (2004). Authentication of travel documents via the imagexpert system. *Journal of the American Society of Questioned Document Examiners*, *7*(2), 97–104.

Europol. (2009). *European Union organised crime threat assessment 2009*. Europol.

Europol. (2011). *European Union organised crime threat assessment 2011*. European Police Office.

Europol. (2017). European Union serious and organised crime threat assessment, crime in the age of technology. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

Europol. (2021). *European Union serious and organised crime threat assessment, a corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*. Publications Office of the European Union. https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Europol. (2024). *Decoding the EU's most threatening criminal networks*. Publications Office of the European Union.

Fahrmeir, A. (2001). Government and forgers: Passports in nineteenth-century Europe. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity*. Princeton.

Friedrich, E. (2001). Fälschungskriminalität und Prävention – Sicherungstechnische Anforderungen an Ausweisdokumente. *Kriminalistik*, *55*(4), 271–277.

Fritz, T. (2007). Questioned documents – A review: 2004 to 2007. Paper presented at the 15th international forensic science symposium, Lyon, France.

Fritz, T. (2010). Examination of questioned documents/handwriting – Review: 2007 to 2010. Paper presented at the 16th international forensic science symposium, Lyon, France.

Frontex. (2019). Risk analysis for 2019. Warsaw, Poland. https://frontex.europa.eu/publications/risk-analysis-for-2019-RPPmXE

Fürbach, M. (2013). La contrefaçon de billets de banque face à l'évolution des technologies d'impression. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, *66*(3), 321–340.

Girelli, C. M. A. (2015). Laterally reversed fingerprints detected in fake documents. *Journal of Forensic Identification*, *65*(1), 1–17.

Girelli, C. M. A. (2016). The use of fingerprints available on the web in false identity documents: Analysis from a forensic intelligence perspective. *Forensic Science International*, *262*, 84–96. https://doi.org/10.1016/j.forsciint.2016.02.041

Gordon, G. R. (2003). Identity fraud: A critical national and global threat. In N. A. Willox (Ed.), *Economic Crime Institute, Utica*. LexisNexis.

Groebner, V. (2007). *Who are you? Identification, deception, and surveillance in early modern Europe*. Zone Books.

Guéniat, O., & Esseiva, P. (2005). *Le profilage de l'héroïne et de la cocaïne. Une méthodologie moderne de lutte contre le trafic illicite*. PU POLYTECHNIQU.

Hammond, D. L. (2013). Overview of forensic document examination. In J. A. Siegel, P. J. Saukko, & M. M. Houck (Eds.), *Encyclopedia of forensic sciences* (2nd ed., pp. 391–394). Academic Press.

Harrison, W. R. (1958). *Suspect documents: Their scientific examination*. Sweet & Maxwell.

Hilton, O. (1979). History of questioned document examination in the United States. *Journal of Forensic Sciences*, *24*(4), 890–897. https://doi.org/10.1520/JFS10920J

Hilton, O. (1993). *Scientific examination of questioned documents*. CRC Press.

Hochholdinger, S., Marvin, L., Arnoux, M., Esseiva, P., & Delémont, O. (2019). Elemental analysis for profiling counterfeit watches. *Forensic Science International*, *298*, 177–185. https://doi.org/10.1016/j.forsciint.2019.03.006

Huber, R. A. (1972). The philosophy of identification. *RCMP Gazette*, *34*(7-8), 9–14.

Huber, R. A., & Headrick, A. M. (1999). *Handwriting identification: Facts and fundamentals* (1st ed.). CRC Press.

INTERPOL. (2019). Identity and travel document fraud. https://www.interpol.int/ar/content/download/10479/file/Identity%20and%20travel%20document%20fraud.pdf

Ioset, S., Esseiva, P., Ribaux, O., Weyermann, C., Anglada, F., Lociciro, S., Hayoz, P., Baer, I., Gasté, L., Terrettaz-Zufferey, A. L., Delaporte, C., & Margot, P. (2005). Establishment of an operational system for drug profiling: A Swiss experience. *Bulletin on Narcotics*, *57*(1–2), 121–147.

Jorna, P., & Smith, R. G. (2017). *Identity crime and misuse in Australia 2017*. Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr10

Kelly, J. S., & Lindblom, B. S. (2006). *Scientific examination of questioned documents* (2nd ed.). CRC/Taylor & Francis.

Kephart, J. (2015). Assuring identity against the growing terrorist travel threat. *Biometric Technology Today*, *2015*(6), 5–7. https://doi.org/10.1016/S0969-4765(15)30096-5

Leaver, W. L. (2006). Introduction to forensic document examination. In A. Mozayani & C. Noziglia (Eds.), *The forensic laboratory handbook: Procedures and practice* (pp. 223–248). Humana Press.

Leaver, W. L. (2011). Forensic document examination. In A. Mozayani & C. Noziglia (Eds.), *The forensic laboratory handbook procedures and practice* (pp. 369–383). Humana Press.

Levinson, J. (1984). Passport examination. *Journal of Forensic Sciences*, *29*(2), 628–632.

Lewis, J. (2014). *Forensic document examination: Fundamentals and current trends*. Elsevier Science & Technology.

Locard, E. (1920). *L'enquete criminelle et les méthodes scientifiques*. Ernest Flammarion.

Marquis, R., Weyermann, C., Delaporte, C., Esseiva, P., Aalberg, L., Besacier, F., Bozenko, J. S., Dahlenburg, R., Kopper, C., & Zrcek, F. (2008). Drug intelligence based on MDMA tablets data: 2. Physical characteristics profiling. *Forensic Science International*, *178*(1), 34–39. https://doi.org/10.1016/j.forsciint.2008.01.014

Mathyer, J. (1980). Quelques remarques sur le problème de la sécurité des pièces d'identité et des pièces de légitimation: Une solution intéressante. *Revue Internationale de Police Criminelle*, *35*(336), 66–79.

McMenamin, G. R., & Choi, D. (2002). *Forensic linguistics: Advances in forensic stylistics*. CRC Press.

Mireault, C., Baechler, S., Côté, R., Roy J. F., Daoust, B., & Crispino, F. (2017). What if counterfeit IDs could talk? Chemical profiling of identity documents. *Keesing Journal of Documents and Identity*, *53*, 9–13.

Morelato, M., Baechler, S., Ribaux, O., Beavis, A., Tahtouh, M., Kirkbride, P., Roux, C., & Margot, P. (2014). Forensic intelligence framework—Part I: Induction of a transversal model by comparing illicit drugs and false identity documents monitoring. *Forensic Science International*, *236*, 181–190. https://doi.org/10.1016/j.forsciint.2013.12.045

Morelato, M., Beavis, A., Tahtouh, M., Ribaux, O., Kirkbride, P., & Roux, C. (2013). The use of forensic case data in intelligence-led policing: The example of drug profiling. *Forensic Science International*, *226*(1), 1–9. https://doi.org/10.1016/j.forsciint.2013.01.003

Morelato, M., Beavis, A., Tahtouh, M., Ribaux, O., Kirkbride, P., & Roux, C. (2014). The use of organic and inorganic impurities found in MDMA police seizures in a drug intelligence perspective. *Science & Justice*, *54*(1), 32–41. https://doi.org/10.1016/j.scijus.2013.08.006

Morton, S. E. (1984). Counterfeits: Three groups, one source. *Journal of Forensic Sciences*, *29*(1), 310–316. https://doi.org/10.1520/jfs11665j

Moulin, S. L., Ertan, E., Martin, D., & Baechler, S. (2024). Cross-border forensic profiling of fraudulent identity and travel documents: A pilot project between France and Switzerland. *Science & Justice*, *64*(2), 202–209. https://doi.org/10.1016/j.scijus.2024.01.003

Moulin, S. L., Weyermann, C., & Baechler, S. (2022). An efficient method to detect series of fraudulent identity documents based on digitised forensic data. *Science & Justice*, *62*(5), 610–620. https://doi.org/10.1016/j.scijus.2022.09.003

Muehlberger, R. J. (1989). Class characteristics of Hispanic writing in the southeastern United States. *Journal of Forensic Sciences*, *34*(2), 371–376. https://doi.org/10.1520/JFS12646J

Ng, P. K., Hui, W. S., Chim, J. L. C., Li, C.-K., & Poon, N. L. (2004). Methods of forgery in counterfeit travel documents. *Journal of the American Society of Questioned Document Examiners*, *7*(2), 83–90.

Ojeda-Aciego, M., & Rodriguez-Jimenez, J. M. (2021). Formal concept analysis with negative attributes for forgery detection. *Computational and Mathematical Methods*, *3*, e1124. https://doi.org/10.1002/cmm4.1124

Ombelli, D., & Knopjes, F. (2008). *Documents: The developer's toolkit*. IOM-International Organisation for Migration Via Occidentalis Editora Lda.

Organisation for Security and Co-operation in Europe (OSCE). (2017). *Intelligence-led policing*. OSCE Secretariat.

Partouche, F. (2013). Questioned documents – Review 2010–2013. Paper presented at the 17th international forensic science managers symposium, Lyon.

Pfefferli, P. W. (2000). Forgery/counterfeits. In J. A. Siegel (Ed.), *Encyclopedia of forensic sciences* (pp. 580–584). Elsevier.

Pfefferli, P. W. (2001). Review 1998-2001 from the coordinating laboratory on questioned documents (other than handwriting). Paper presented at the 13th international forensic science symposium, Lyon, France.

Pfefferli, P. W., Steiner, J., Oneta, C., & Gahwiler, H. (1999). Bekämpung von Ausweis- und Visums-fälschungen: ein Lagebericht. *Kriminalistik*, *53*, 833.

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Willan Publishing.

Ribaux, O. (2023). *De la police scientifique à la traçologie* (2nd ed.). EPFL Press.

Ribaux, O., Baechler, S., & Rossy, Q. (2022). Forensic intelligence and traceology in digitalised environments: The detection and analysis of crime patterns to inform practice. In M. Gill (Ed.), *The handbook of security* (pp. 81–100). Palgrave Macmillan.

Ribaux, O., Baylon, A., Lock, E., Delemont, O., Roux, C., Zingg, C., & Margot, P. (2010). Intelligence-led crime scene processing. Part II: Intelligence and crime scene examination. *Forensic Science International*, *199*(1–3), 63–71. https://doi.org/10.1016/j.forsciint.2010.03.011

Ribaux, O., Baylon, A., Roux, C., Delemont, O., Lock, E., Zingg, C., & Margot, P. (2010). Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Science International*, *195*(1–3), 10–16. https://doi.org/10.1016/j.forsciint.2009.10.027

Ribaux, O., Margot, P., Julian, R., & Kelty, S. F. (2013). Forensic intelligence. In J. E. Siegel & P. J. Saukko (Eds.), *Encyclopedia of forensic sciences* (pp. 298–302). Academic Press.

Riordan, W., Gustafson, J., Fitzgerald, M., & Lewis, J. (2012). *Forensic document examination*. John Wiley & Sons.

Romagna, M. (2014). The cyber-market of identities: Criminological analysis on the illegal market of identity documents within the surface web and Onionland (Masters thesis). Utrecht University, Utrecht.

Romagna, M. (2015). Cybermarket for forged identity documents: The illegal trade of identity documents on the surface web and in Onionland. *Keesing Journal of Documents and Identity*, *47*, 12–15.

Roux, C., & Weyermann, C. (2020). Can forensic science learn from the COVID-19 crisis? *Forensic Science International*, *316*, 110503. https://doi.org/10.1016/j.forsciint.2020.110503

Roux, C., Crispino, F., & Ribaux, O. (2012). From forensics to forensic science. *Current Issues in Criminal Justice*, *24*(1), 7–24. https://doi.org/10.1080/10345329.2012.12035941

Roux, C., Willis, S., & Weyermann, C. (2021). Shifting forensic science focus from means to purpose: A path forward for the discipline? *Science & Justice*, *61*(6), 678–686. https://doi.org/10.1016/j.scijus.2021.08.005

Schloenhardt, A. (1999). Organized crime and the business of migrant trafficking. *Crime, Law and Social Change*, *32*(3), 203–233. https://doi.org/10.1023/A:1008340427104

Schloenhardt, A., Douglas, F., & Lelliott, J. (2012). *Stop the planes! Document fraud and migrant smuggling by air in Australia*. The University of Queensland. http://www.abc.net.au/am/content/2012/s3465202.htm

Talbot-Wright, B., Baechler, S., Morelato, M., Ribaux, O., & Roux, C. (2016). Image processing of false identity documents for forensic intelligence. *Forensic Science International*, *263*, 67–73. https://doi.org/10.1016/j.forsciint.2016.03.054

Trubshoe, T., & McGinn, J. (2013). Forgery/counterfeits. In J. A. Siegel, P. J. Saukko, & M. M. Houck (Eds.), *Encyclopedia of forensic sciences* (2nd ed., pp. 360–366). Academic Press.

Turnbull, S. J., Jones, A. E., & Allen, M. (2010). Identification of the class characteristics in the handwriting of polish people writing in English. *Journal of Forensic Sciences*, *55*(5), 1296–1303. https://doi.org/10.1111/j.1556-4029.2010.01449.x

United Nations Office on Drugs and Crime (UNODC). (2010). *Report of observations and conclusions of the session on the use of forensic sciences to combat and prevent identity-related crime*. United Nations Office on Drugs and Crime.

United Nations Office on Drugs and Crime (UNODC). (2013). *Transnational organised crime in East Asia and the Pacific: A threat assessment*. United Nations Office on Drugs and Crime (UNODC).

Vieira, R., Antunes, M., Silva, C., & Assis, A. (2017). *Automatic documents counterfeit classification using image processing and analysis*. Springer.

Vieira, R., Silva, C., Antunes, M., & Assis, A. (2016). Information system for automation of counterfeited documents images correlation. *Procedia Computer Science*, *100*, 421–428. https://doi.org/10.1016/j.procs.2016.09.178

Weyermann, C., Marquis, R., Delaporte, C., Esseiva, P., Lock, E., Aalberg, L., Bozenko, J. S., Dieckmann, S., Dujourdy, L., & Zrcek, F. (2008). Drug intelligence based on MDMA tablets data: I. Organic impurities profiling. *Forensic Science International*, *177*(1), 11–16. https://doi.org/10.1016/j.forsciint.2007.10.001

Willox, N. A., & Regan, T. M. (2002). *Identity fraud: Providing a solution*. Economic Crime Institute and LexisNexis.

How to cite this article: Devlin, C., Morelato, M., & Baechler, S. (2024). Forensic intelligence: Expanding the potential of forensic document examination. *WIREs Forensic Science*, *6*(5), e1528. https://doi.org/10.1002/wfs2.1528