Authentication of travel and breeder documents

Henri Bouma [1*], Armin Reuter [2], Patrick Brouwer [3], Martin George [3], James Ferryman [4], Jonathan Boyle [4], Alfonsas Juršėnas [5], Anni Karinsalo [6], Raimon Pruim [1], Arthur van Rooijen [1], Johan-Martijn ten Hove [1], Jelle van Mil [1], Damjan Gicic [2], Gabriel Goller [2], Eimantas Ledinauskas [5], Julius Ruseckas [5], Ben Kromhout [7], Hans de Moel [8], Niels Dolstra [8].

[1] TNO, The Hague, The Netherlands
[2] Veridos GmbH, Munich, Germany
[3] OVD Kinegram, Zug, Switzerland
[4] University of Reading, Reading, UK
[5] BPTI, Vilnius, Lithuania
[6] VTT Research, Oulu, Finland
[7] Immigration and Naturalization Service IND, Zwolle, The Netherlands
[8] Royal Netherlands Marechaussee, Schiphol/Ter Apel, The Netherlands

ABSTRACT

Authentication of travel documents (e.g., passports) and breeder documents (e.g., birth certificates) is important to facilitate legal movement of passengers and to prevent cross-border crime, such as terrorism, smuggling, illegal migration and human trafficking. However, it is time consuming and difficult to verify all security features, the border guards differ in experience and expertise, and it is hard to stay alert every minute of a working day. New (artificial-intelligence based) technologies can assist in the automated fraud detection in travel and breeder documents, which may lead to faster and more consistent checks.

This paper presents five categories of new technologies in automated document authentication to overcome the limitations of current document analysis systems in automated and non-automated border control scenarios. The first category consists of techniques related to the verification of visual security features on the holder page of travel documents. This category includes the verification of *KINEGRAMs* and other Optically Variable features under different light sources and lighting angles, and the analysis of printing techniques. The second category consists of techniques related to the analysis of breeder documents. This analysis can be at detail level (e.g., investigation of stamps) and at tactical level (e.g., verification of a check digit in a document number). The third category concerns the analysis of travel patterns, using information from the visa pages in passports. The stamps on these pages can be used to extract a travel pattern to support risk assessments and to detect anomalies. The fourth category is an analysis of the border-guard inspection history based upon a distributed ledger and blockchain technology that enables secure storage and prevents undesired manipulations. The last category analyzes the electronic chip of a passport. The software analyses document signer and country signer certificates on the chip to detect vulnerable cryptographic keys and tactical anomalies.

Keywords: Artificial intelligence, travel documents, breeder documents, border guards, immigration services.

[*] Henri.Bouma@tno.nl; phone +31 6 5277 9020; www.tno.nl

H. Bouma, A. Reuter, P. Brouwer, M. George, J. Ferryman, J. Boyle, A. Juršėnas, A. Karinsalo, R. Pruim, A. van Rooijen, R.J.M. ten Hove, J. van Mil, D. Gicic, G. Goller, E. Ledinauskas, J. Ruseckas, B. Kromhout, J. de Moel, N. Dolstra, "Authentication of travel and breeder documents," Proc. SPIE, vol. 11869, (2021). https://doi.org/10.1117/12.2598143

1. INTRODUCTION

Document fraud is indicated as one of the main serious and organized crime activities in the EU [Europol, 2021]. Document fraud entails the production of complete counterfeits, partly forged documents, altered genuine documents, or stolen genuine documents. Document fraud is an enabler for most criminal activities, which includes all types of cross-border crime, such as migrant smuggling, trafficking in human beings as well as the trafficking of drugs, weapons or stolen vehicles. [Europol, 2021]. In 2017, border guards detected 6,700 individuals travelling with fraudulent documents upon entry to the EU/Schengen area [FRONTEX, 2018], although the amount of actual fraud is likely to be significantly higher due to non-detection of the identified vulnerabilities.

Travel documents are documents issued by a government for the purpose of entering another country (e.g., passports). Breeder documents are used to support the application for identity, residence and travel documents (e.g., certificates for birth, marriage, divorce, death, living, residence, government). Since breeder documents can be used to obtain travel documents, it is important to authenticate both. However, it is time consuming and difficult to verify all security features of such documents. Furthermore, the border guards and immigration services differ in experience and expertise, and it is hard for them to stay alert every minute of a working day. New artificial-intelligence (AI) based technologies can assist in the fraud detection in travel and breeder documents, which may lead to faster and more consistent checks.

D4FLY is a European H2020 research and innovation project. The project focuses on enhancing the quality and efficiency of identity verification at border crossings by providing faster and more secure border control solutions. This paper aims to give an overview of the document analysis techniques developed in the D4FLY project.

This paper presents five categories of new technologies in automated document authentication to overcome the limitations of current document analysis systems in automated and non-automated border control scenarios. The first category consists of techniques related to the verification of visual security features on the holder page of travel and identity documents. This category includes the verification of *KINEGRAMs*® (Sec. 2) and other Optically Variable features (e.g., *MagicID*®) in different light sources and lighting angles (Sec. 3), and the analysis of printing techniques (Sec. 4). The second category consists of techniques related to the analysis of breeder documents. This analysis can be at detail level – e.g. by investigation of stamps (Sec. 5) – or at tactical level – e.g., by verification of a check digit in a document number (Sec. 6). The third category concerns the analysis of travel patterns, using information from the visa pages in passports. The stamps on these pages can be used to extract a travel pattern to support risk assessments and to detect anomalies (Sec. 7). The fourth category is an analysis of the border-guard inspection history based upon a distributed ledger and blockchain technology that enables secure storage and prevents undesired manipulations (Sec. 8). The last category analyzes the electronic chip of a passport. The software analyses document signer and country signer certificates to detect vulnerable cryptographic keys and tactical anomalies (Sec. 9).

2. KINEGRAM ANALYSIS

Diffractive Optically Variable Image Devices (DOVIDs), of which the *KINEGRAM*® is a widely used example, are visible security features originally designed to protect personalized data such as a face photo or biographics in secure identity credentials so human inspectors can ascertain if a document is genuine and has not been tampered with. The *KINEGRAM* is contained in a foil whose proprietary materials and design structures remain unchanged under the high temperatures and pressures applied as the layers of the card or datapage body are fused during manufacturing. *KINEGRAMs* differ from other DOVIDs in that they have continuous vector lines in their diffractive structure, rather than discrete pixel or patch segments [Peters, 2020]. With document security being a high concern worldwide, many visually sophisticated security feature designs have emerged, making it very difficult even for the trained human inspector to recognize which feature is appropriate to which document. Further, sophisticated holographic production tools are now available to forgers, so they attempt to recreate a fake card or datapage whose security features look visually similar to the genuine article. Alternatively they try to harvest features, or to mill out areas behind personalization, so that an impostor's data or photo can be substituted. These attempts result either in damage to the minutiae of security features, or to creating a fake or altered security feature whose microscopic properties no longer match the specific image "fingerprint" of the original.

The *KINEGRAM* analysis method is developed by OVD-Kinegram in the D4FLY project. It comprises a set of analytic checks across multiple images and data fusion of the results obtained. The checks are performed across the high-resolution images, typically at 400dpi, acquired from the document reader scanner in multiple light sources (Visible, Near Infra-Red and Ultraviolet). These checks investigate features of the *KINEGRAM* under test, mostly by a knowledge-based decision process that compares against values and combinations contained in a template, combined with specific company know-how about the *KINEGRAM*, derived from known originals and the original design [Peters, 2017]:

- The size and position of the *KINEGRAM* relative to the complete holder data page
- The shape of the *KINEGRAM* by comparing the measured shape on a holder page with a predefined shape that is known for the holder page of the document under inspection.
- The colors and structures in the measured *KINEGRAM* (e.g. metallization and registration revealed in NIR)
- Various position, contrast, texture and intensity properties, and their relationship across images

Some checks follow a decision tree, enabling the check process to be terminated as soon as a critical check fails. To give some examples of how the *KINEGRAM* analysis aids detection of a suspect document, unsophisticated fakes – such as cards produced by commercial color print methods – will not exhibit the same color, contrast and reflection intensities expected from a genuine *KINEGRAM* (Figure 1). More sophisticated fakes, for example using dot matrix holographic origination – if they do not fail on color, contrast and reflection intensity – are likely to fail on positional measurements, and on detection of metallization features. Attempts to harvest Kinegrams from an original document result in micro-destruction of the metallized features which – although perhaps not immediately visible to the naked eye – are detected from the measurements made on the combinations of NIR and Visible light images.

All images for analysis purposes can be produced from the current generation of commercial multiple light source document scanner used in kiosks, check-in desks, e-gates and border control points so that the only upgrade necessary is a software update. The *KINEGRAM* Optical Machine Authentication (OMA) checks are then directly integrated in the graphical user interface (GUI) of the document scanner. The set of checks is conducted in less than 1 second using processors already present in the document scanner devices themselves, or in the computers and networked systems typically used in border management IT systems.

Future work in the D4FLY project is extending the range of documents that can be checked, setting out guidelines for creating future document designs that are much more amenable to machine verification and investigating simple design enhancements to document reader scanners that will also improve the machine checking of documents.

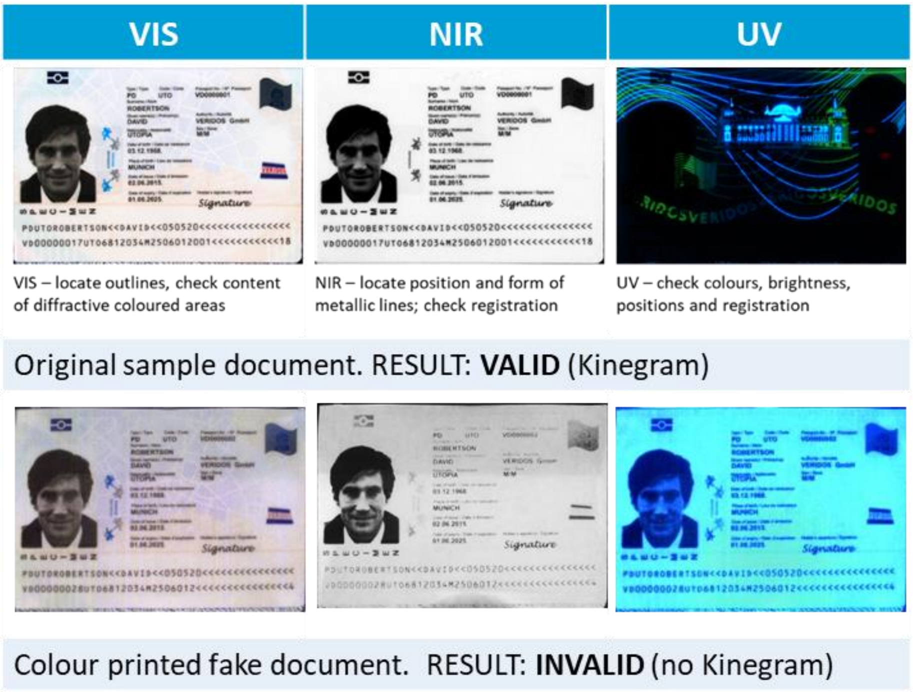

VIS
NIR
UV
VIS – locate outlines, check content of diffractive coloured areas
NIR – locate position and form of metallic lines; check registration
UV – check colours, brightness, positions and registration
Original sample document. RESULT: **VALID** (Kinegram)
Colour printed fake document. RESULT: **INVALID** (no Kinegram)

Figure 1: Documents with valid (top) and invalid (bottom) Kinegrams.

3. ADVANCED DOCUMENT ANALYSIS MODULE (ADAM)

The goal of the Advanced Document Analysis Module (ADAM), developed by the University of Reading, is to enhance the reliability of automatic document inspection. Specifically, the development of computer-vision algorithms to analyze specific document security features of passports that are not detected automatically by current generation software and optically variable features (other than Kinegram above) such as Multiple Laser Images (MLIs) and Changeable Laser Images (CLIs).

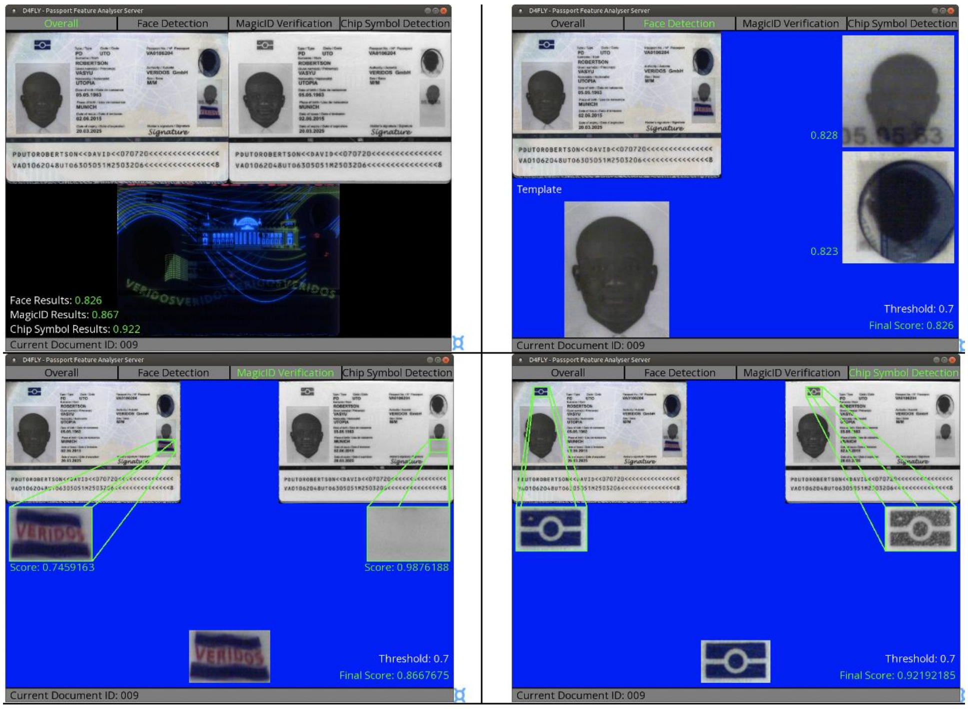
ADAM has been developed with extensibility in mind – it represents a plug-and-play architecture for different detection modules and supports multiple imaging modalities. The module is easily extensible to add new security features exhibiting different positions, scales, shapes, color etc. properties across different document types. There are two areas of research that has been the primary focus for ADAM to date:

1. The development, evaluation and integration of security feature detection within the D4FLY system based on a standard (low-resolution) *Regula* 7024M.111 document scanner. This scanner contains several light sources: white, infrared (870nm), ultraviolet (368nm) and coaxial white.
2. A preliminary study using the higher-resolution *Regula* 8850M scanner to determine its suitability for enhanced authentication of security features. This scanner contains more light sources, more wavelenghts and more illumination angles.

For the *Regula* 7024M.111 scanner, three detection modules were implemented as defined below. The exact selection and specification of features for a given document is provided by the document model:

1. Chip symbol
2. *MagicID*® feature
3. Secondary and further faces on the main data page

A first version of ADAM has been integrated into the overall D4FLY architecture and system as a plug-in component. The graphical user interface (GUI) can be seen in Figure 2 with examples of the abovementioned 3 security features.



Face Results: 0.826
MagicID Results: 0.867
Chip Symbol Results: 0.922
Current Document ID: 009

0.828
0.823
Threshold: 0.7
Final Score: 0.826
Current Document ID: 009

Score: 0.7459163
Score: 0.9876188
Threshold: 0.7
Final Score: 0.8667675
Current Document ID: 009

Threshold: 0.7
Final Score: 0.92192185
Current Document ID: 009

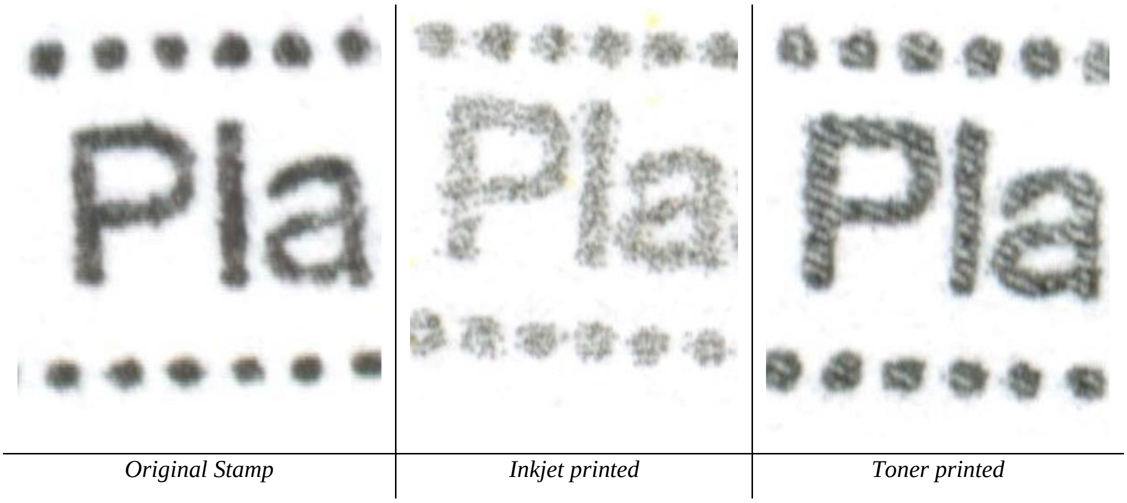
Figure 2: GUI of ADAM showing the detection of chip symbol (bottom right), MagicID (bottom left), and further facial images (upper right).

For the Regula 8850M scanner, a preliminary study has been performed using a starting point of 15 documents. This analysis has revealed how enhanced authentication of selected security features could be achieved using different light sources and directions. In particular, lenticular effects in security features can be measured using an 8850M scanner whereas they cannot using a 7024M scanner. Another additional benefit of the 8850M scanner is the higher resolution potentially enabling further additional automated authentication.

There are multiple aims for further work: the development of a tool to calibrate unseen passports to the 7024M.111 version of ADAM, and the integration of the information gained from the 8850M study into a usable software/hardware form. This will add onto the extensibility of the overall ADAM module to demonstrate that further automation of passport security feature detection is not only possible but within the realms of current technology.

4. PRINTING TECHNIQUES

Travel and breeder document may contain different printing techniques (e.g., offset, inkjet, laser). Recognition of the printing technique may assist in the detection of forged documents, because the forgeries are often generated with different printing techniques. An example of a stamp created with three different printing techniques is shown in Figure 3.



Original Stamp *Inkjet printed* *Toner printed*

Figure 3: Examples of a stamp created with three different printing techniques, which show differences in texture.

The method to recognize printing techniques is developed by TNO and is applied in a region of interest (ROI) on the document. The ROI could consists of a foreground detail (e.g., stamp, signature, text) or a background detail (e.g., microtext, continuous curves/patterns). The detection of foreground details is implemented by means of a Faster R-CNN detector [Ren, 2017] with a ResNet-101 backbone [He, 2015], from the MMLab Detection Toolbox [Chen, 2019], which is a state-of-the-art deep-learning algorithm for object detection and classification [Boer, 2017]. For printing technique recognition of the details the following approaches are used:

- **Data-driven**: A data-driven approach for which each detail is divided into a set of small non-overlapping patches of size 128x128 pixels. A Convolutional Neural Network (CNN) determines the dominant printing technique used in each of the patches. The CNN used is the VGG16 network [Simonyan, 2015], which came out on top in a comparison with other state-of-the-art classification networks. A classification of the detail is obtained with majority voting of the separate patches.
- **Handcrafted:** The two handcrafted approaches (texture and contour) are classified with a binary decision tree.
  - **Texture:** A handcrafted design of a method for the recognition of printing techniques by measuring the filling pattern (texture). Figure 3 shows that the texture differs between printing techniques. One way to perform measurements on the texture is with the gray level co-occurrence matrix (GLCM) [Mikkilineni, 2005]. Several statistical features for the texture analysis are extracted from this matrix, such as: angular second moment (ASM), contrast, entropy, local homogeneity, dissimilarity, energy and correlation [Lee, 2019]. The printing techniques are classified with a binary decision tree.
  - **Contour**: A handcrafted design of a method by measuring the smoothness of a contour. This can be implemented with a binary segmentation between foreground and background and the extraction of a

binary contour. An example of the extracted contour is shown in Figure 4. This binary contour can be encoded with a chain-code, which allows the computation of curvature and bending energy [Sonka, 1999]. The printing techniques are classified with a binary decision tree.

The graphical user interface (GUI) of the tool is shown in Figure 5. The left part of the GUI shows the detected stamp on the whole document and the right part shows a magnification of this stamp. The label of the printing technique is automatically assigned by the system and it can be corrected by the human document expert in a drop-down menu.

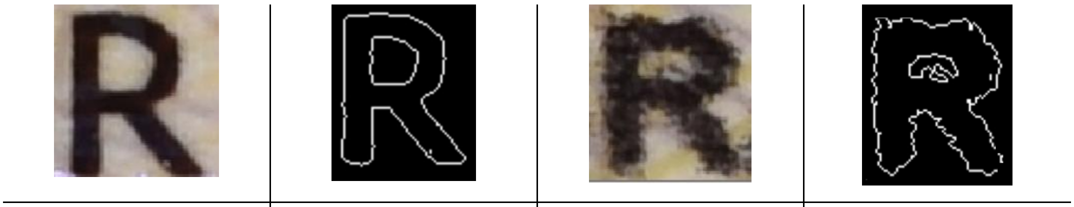
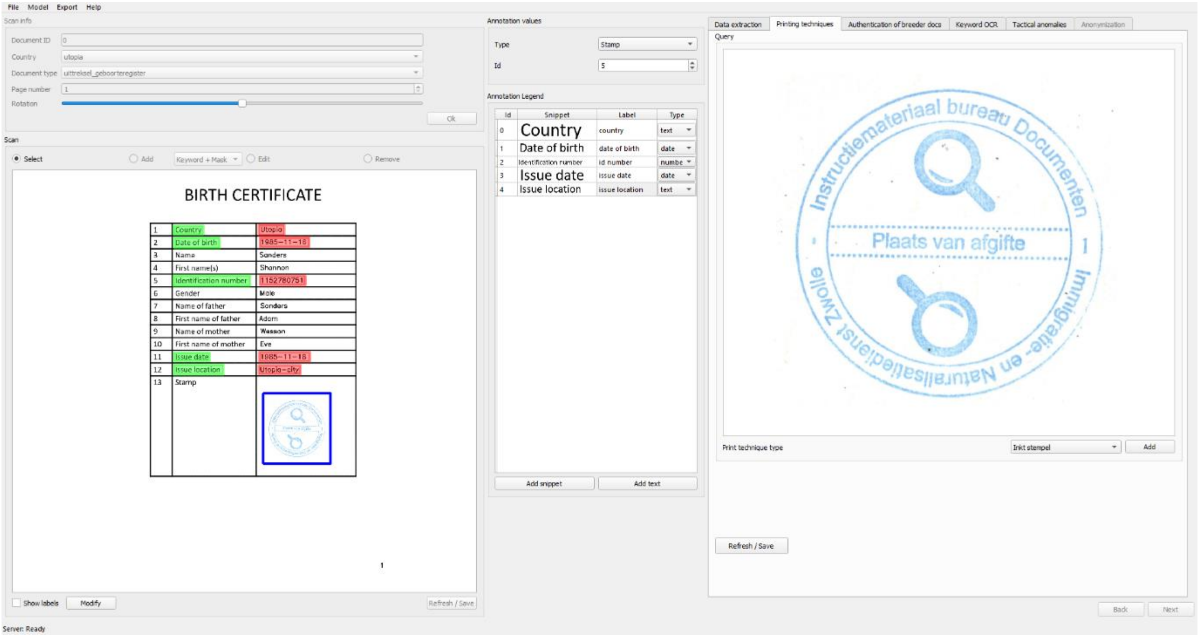


Image 1 | *Contour 1* | *Image 2* | *Contour 2*

Figure 4: Examples of text that is created with two different printing techniques, which show differences in the contour.



Document ID: 0
Country: utopia
Document type: uittreksel_geboorteregister
Page number: 1
Rotation
● Select
Keyword + Mask

BIRTH CERTIFICATE

1	Country	Utopia
2	Date of birth	1985–11–18
3	Name	Sanders
4	First name(s)	Shannon
5	Identification number	1152780751
6	Gender	Male
7	Name of father	Sanders
8	First name of father	Adam
9	Name of mother	Wesson
10	First name of mother	Eve
11	Issue date	1985–11–18
12	Issue location	Utopia–city
13	Stamp	

1

Type: Stamp
Id: 5

Id	Snippet	Label	Type
0	Country	country	text
1	Date of birth	date of birth	date
2	Identification number	id number	numbe
3	Issue date	issue date	date
4	Issue location	issue location	text

Print technique type: Inkt stempel

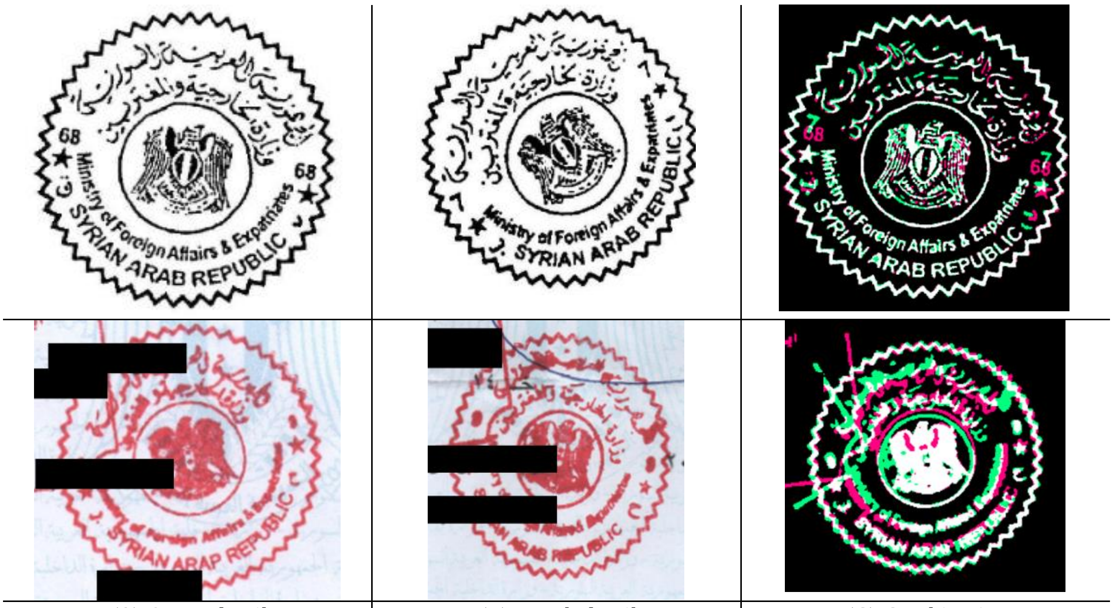
Figure 5: GUI with a detected stamp (left; blue box) and the print technique (right; drop-down menu).

5. FRAUD IN DETAILS

The security features included in breeder documents are limited. One of the most important security features is the stamp or the signature on a document. The current module assists in the authentication of such details.

The method is implemented by TNO and it consists of four components: detail detection, detail matching, detail registration and visualization. Detail detection was already described in Section 4 (printing techniques). The second component aims to match the query detail to similar details in the database to support comparison. Detail matching is implemented with Triplet-REID [Hermans, 2017], which is a state-of-the-art deep-learning algorithm for person re-identification [Rooijen, 2018]. The training set for the matcher was annotated by indicating whether two details are ‘same’ or ‘different’. A graph is created with these relations and the ‘same’ edges are used to create clusters based connected-components analysis and the ‘different’ edges are used to detect conflicts. The third component performs an alignment (registration) between one query and one match. Detail registration is performed to align the query detail (from the document scan) to a matching detail (a similar detail in the database). Detail registration is performed with multiple color transformations (to focus on the foreground object), AKAZE keypoints [Alcantarilla, 2011] and estimation of an affine transformation matrix with RANSAC [Fischler, 1981]. The transformation matrix with the highest Structural Similarity Index (SSIM) score [Wang, 2004] is used. After the coarse registration, it is refined with the Demons algorithm [Thirion, 1998]. The fourth component visualizes the registered combination of query and match detail. A false-color visualization is generated with a color transform and RGB encoding, where the query is encoded in the R-channel, the match is encoded in the G-channel and the mean is encoded in the B-channel. As a consequence, the combined image is red (for query), green (for match), black (none) or white (both).

Figure 6 shows two examples of a query detail, a similar match that is retrieved from the database and the combination of both in the false-color visualization. The first row shows two stamps with only minor differences although they are from different regions (indicated by the numbers 7 and 68). The second row shows two stamps with major differences. Figure 7 shows an example of the graphical user interface to authenticate details. On the left, the user can select a query detail. On the bottom right, the user can select a good match (the current view shows 5 candidate matches). On the top-right, the user can select an enlargement of a query, match or false-color visualization.

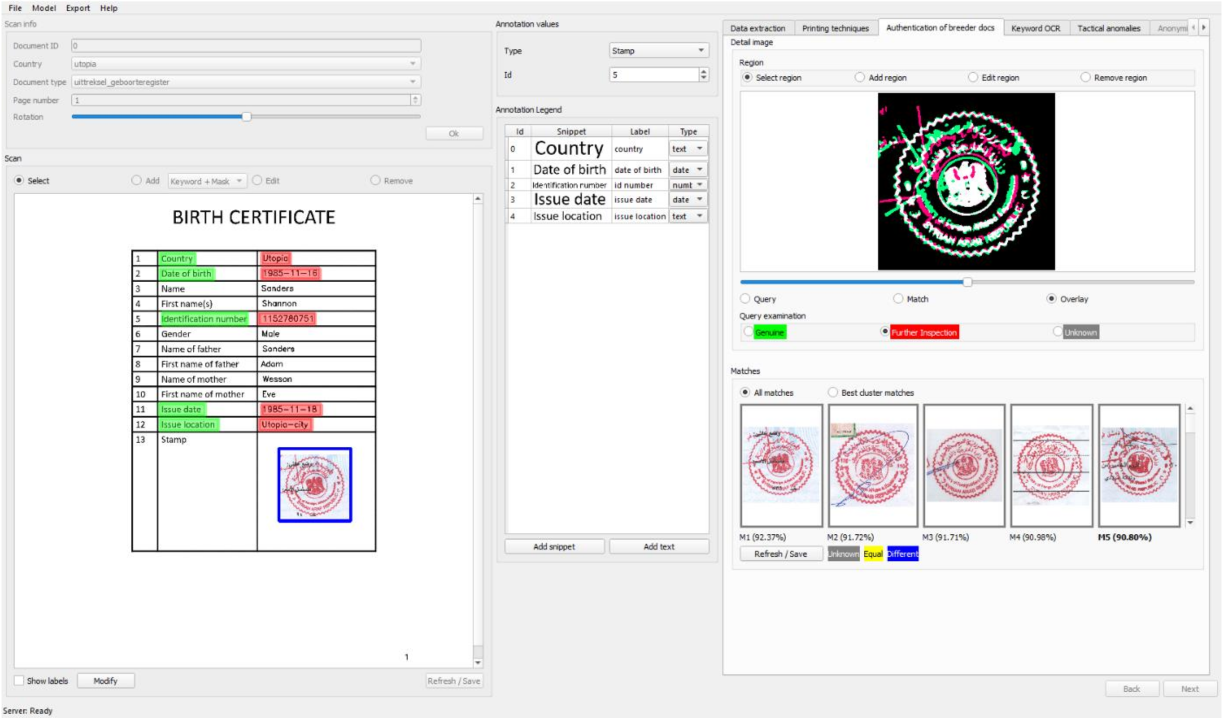


(A) Query detail | *(B) Match detail* | *(C) Combination*

Figure 6: Two examples of query stamp (left), stamp that matches the query (center), and combined overlay (right).

6. TACTICAL ANOMALY DETECTION

Fraud can be detected at the detail level or at tactical level. For example, at detail level a document seems unaltered, but the numbers or stamps or dates or names are not in the range of what is expected. A combination of top-down rules and bottom-up learning is used to recognize tactical anomalies.



Document ID: 0
Country: utopia
Document type: uittreksel_geboorteregister
Page number: 1
Rotation

● Select ○ Add Keyword + Mask ○ Edit ○ Remove

BIRTH CERTIFICATE

1	Country	Utopia
2	Date of birth	1985–11–16
3	Name	Sanders
4	First name(s)	Shannon
5	Identification number	1152780751
6	Gender	Male
7	Name of father	Sanders
8	First name of father	Adam
9	Name of mother	Wesson
10	First name of mother	Eve
11	Issue date	1985–11–18
12	Issue location	Utopia–city
13	Stamp	

1

Server: Ready

Annotation values

Type: Stamp
Id: 5

Annotation Legend

Id	Snippet	Label	Type
0	Country	country	text
1	Date of birth	date of birth	date
2	Identification number	id number	numt
3	Issue date	issue date	date
4	Issue location	issue location	text

● Select region ○ Add region ○ Edit region ○ Remove region

○ Query ○ Match ● Overlay

○ Genuine ● Further Inspection ○ Unknown

● All matches ○ Best cluster matches

M1 (92.37%) M2 (91.72%) M3 (91.71%) M4 (90.98%) **M5 (90.80%)**

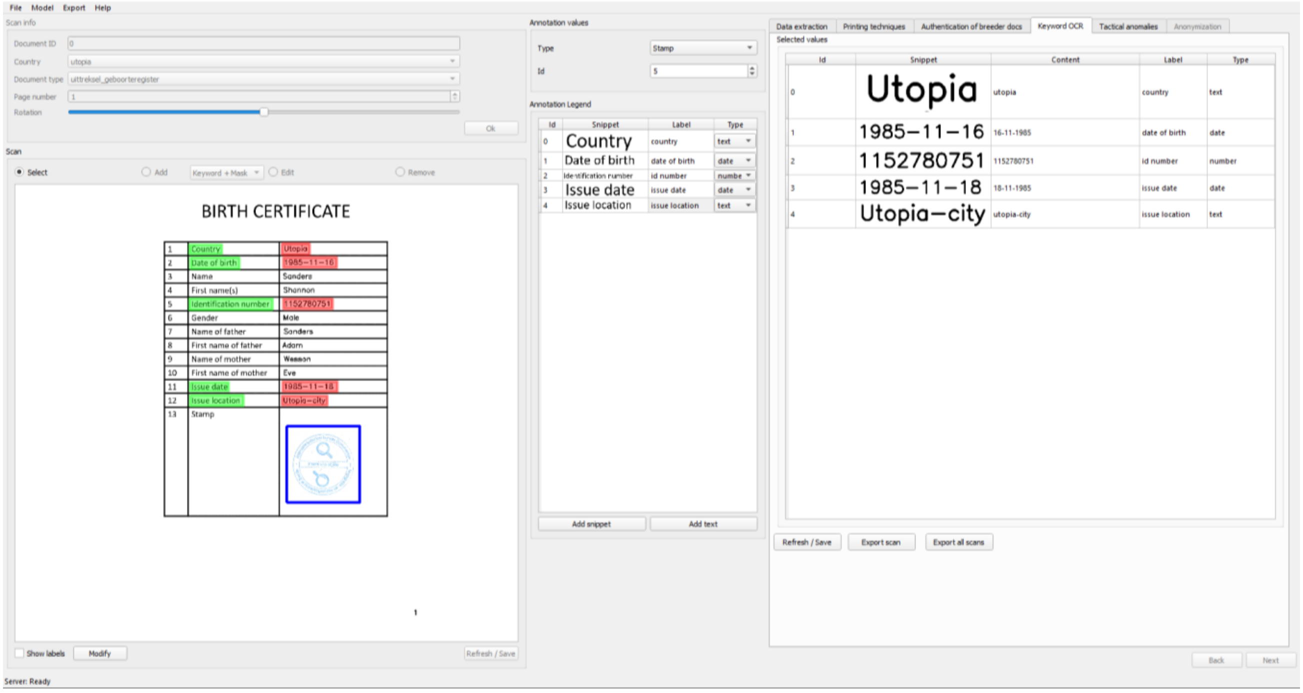
Figure 7: Query stamp (left), stamp that matches the query (center), and combined overlay (right).

The method is implemented by TNO and it consists of three main components: mask localization, text extraction and anomaly detection. The mask localization aims to find the data fields that contain the relevant information. The keywords (e.g., 'issue date') are used to localize the corresponding data field (e.g., '1985-11-18'). The implementation of mask localization is identical to the anonymization tool [Bouma, 2020]. The second component extracts text from the masks with an Optical Character Recognition (OCR) algorithm. The OCR implementation consist of two steps: 1) text detection using the CRAFT text detector [Baek, 2019], and 2) recognition of the text within a bounding box using a Convolutional Recurrent Neural Network (CRNN). Both are implemented using the open Keras-OCR engine [KERAS-OCR]. This Keras-OCR engine has the benefit of optional re-training of the model. For each data field mask, the recognized text of all bounding boxes overlapping with that mask are merged. The third component aims to make a separation between normal patterns and anomalies with two approaches: top-down rules and bottom-up learning. The top-down approach allows the user to express expert knowledge as rules in the system. Each rule consists of a short description, preconditions and conditions. The preconditions define when the rule can be applied (e.g., country = 'X' and issue date > '2020-01-01') and the conditions define which values are valid (e.g., document number has 8 characters). The bottom-up approach performs data-driven anomaly detection with Isolation Forest [Liu, 2008].

The GUI for mask localization and text extraction is shown in Figure 8. The left part shows the keywords (green) and masks (red). The center part shows the list of keywords to obtain a consistent (automatic or manual) annotation in the documents of the same type. The labels are used for data analysis. The right part of the GUI shows the result of automatic text extraction in each of the masks. If the system makes an error, this can be manually corrected by the user.

Expert knowledge can be defined with the rule editor and the condition editor (Figure 9). The rule editor can combine multiple conditions with combinatory logic. The labels that were defined earlier are shown in the drop-down menus of the condition editor. The condition editor shows several building blocks that can be used to analyze the data, such as the verification of a check-digit. Figure 10 shows the top-down anomaly detection GUI with three example rules based on the issue date in 1985. The first rule contains a condition that the issue date should be before 1980, which is false and therefore indicated with the color 'red'. The second rule contains a condition that the issue data should be after 1984, which is true and therefore indicated with the color 'green'. The third rule has a precondition (not condition) that it should only be applied to documents after 2020, which is false and therefore indicated with the color 'gray'.

The data-driven data analysis contains visualizations with Streamlit [Streamlit] of statistics of variables over a set of documents, such as scatterplots, bar charts, correlation plots, and maps. Figure 11 shows an example of a visualization of variables, such as years and day-of-the-week. The visualization can be used for exploring the data and investigating normal ranges and relations of data values. In some cases, the visualization of the distribution of normal documents is hindered by the anomalies and therefore, they can be enabled or disabled (Figure 12). The GUI also allows a matrix representation with documents versus variables (similar to an excel sheet) where the normal values are shown in black and the anomalies are indicated in red (figure not shown).



Document ID: 0
Country: utopia
Document type: uittreksel_geboorteregister
Page number: 1
Rotation

BIRTH CERTIFICATE

1	Country	Utopia
2	Date of birth	1985–11–16
3	Name	Sanders
4	First name(s)	Shannon
5	Identification number	1152780751
6	Gender	Male
7	Name of father	Sanders
8	First name of father	Adam
9	Name of mother	Wesson
10	First name of mother	Eve
11	Issue date	1985–11–18
12	Issue location	Utopia–city
13	Stamp	

1

Annotation values

Type: Stamp
Id: 5

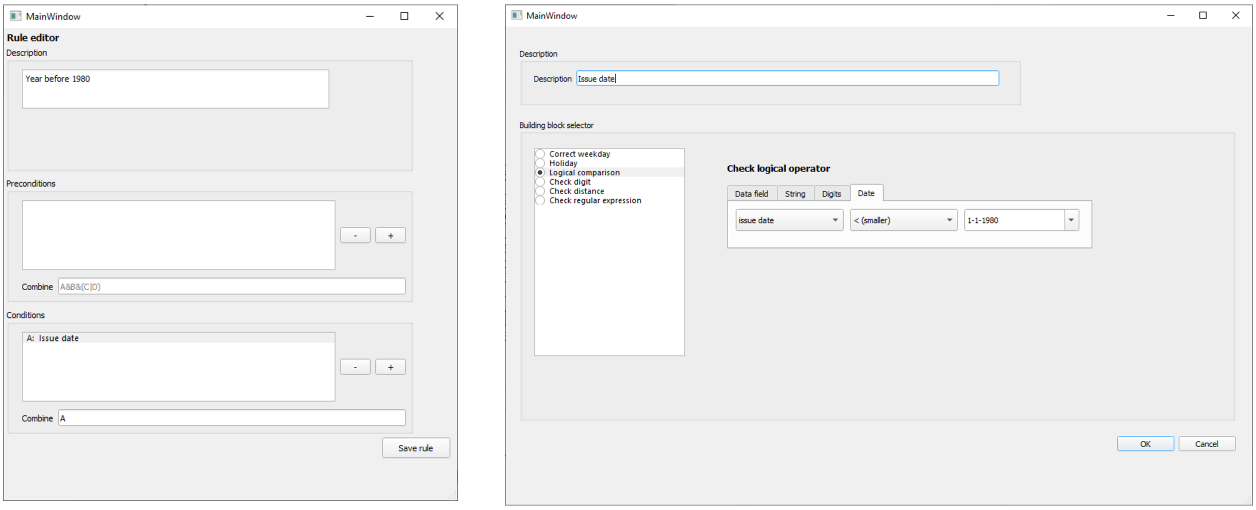
Annotation Legend

Id	Snippet	Label	Type
0	Country	country	text
1	Date of birth	date of birth	date
2	Identification number	id number	numbe
3	Issue date	issue date	date
4	Issue location	issue location	text

Selected values

Id	Snippet	Content	Label	Type
0	Utopia	utopia	country	text
1	1985–11–16	16-11-1985	date of birth	date
2	1152780751	1152780751	id number	number
3	1985–11–18	18-11-1985	issue date	date
4	Utopia–city	utopia-city	issue location	text

Figure 8: GUI for text extraction.



Rule editor

Description

Year before 1980

Preconditions

Combine: A&B&(C|D)

Conditions

A: Issue date

Combine: A

Description

Description: Issue date

Building block selector

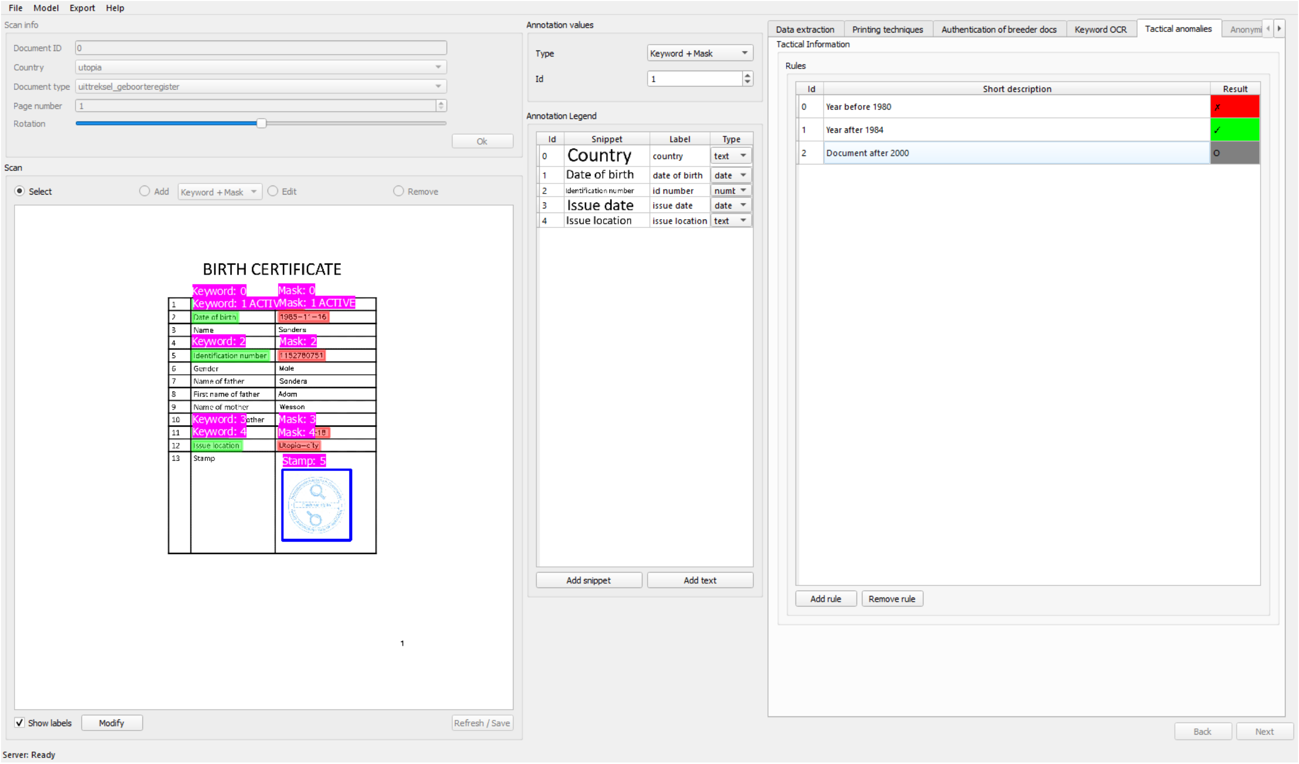
○ Correct weekday
○ Holiday
● Logical comparison
○ Check digit
○ Check distance
○ Check regular expression

Check logical operator

Data field | String | Digits | Date

issue date | < (smaller) | 1-1-1980

Figure 9: Rule editor (left) and Condition editor with several building blocks (right).



Scan info

Document ID: 0

Country: utopia

Document type: uittreksel_geboorteregister

Page number: 1

Rotation

Scan

● Select ○ Add Keyword + Mask ○ Edit ○ Remove

BIRTH CERTIFICATE

	Keyword: 0	Mask: 0
1	Keyword: 1 ACTIV	Mask: 1 ACTIVE
2	Date of birth	1985–11–16
3	Name	Sanders
4	Keyword: 2	Mask: 2
5	Identification number	1152780751
6	Gender	Male
7	Name of father	Sandera
8	First name of father	Adam
9	Name of mother	Wesson
10	Keyword: 3other	Mask: 3
11	Keyword: 4	Mask: 4-18
12	Issue location	Utopia–city
13	Stamp	Stamp: 5

1

☑ Show labels

Server: Ready

Annotation values

Type: Keyword + Mask

Id: 1

Annotation Legend

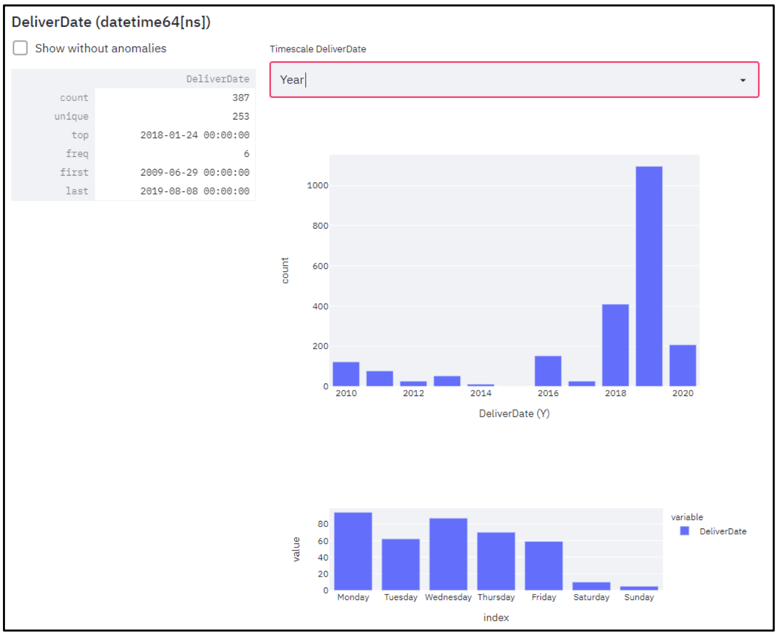
Id	Snippet	Label	Type
0	Country	country	text
1	Date of birth	date of birth	date
2	Identification number	id number	numb
3	Issue date	issue date	date
4	Issue location	issue location	text

Tactical Information

Rules

Id	Short description	Result
0	Year before 1980	✗
1	Year after 1984	✓
2	Document after 2000	O

Figure 10: Expert rule-based tactical anomaly detection GUI.



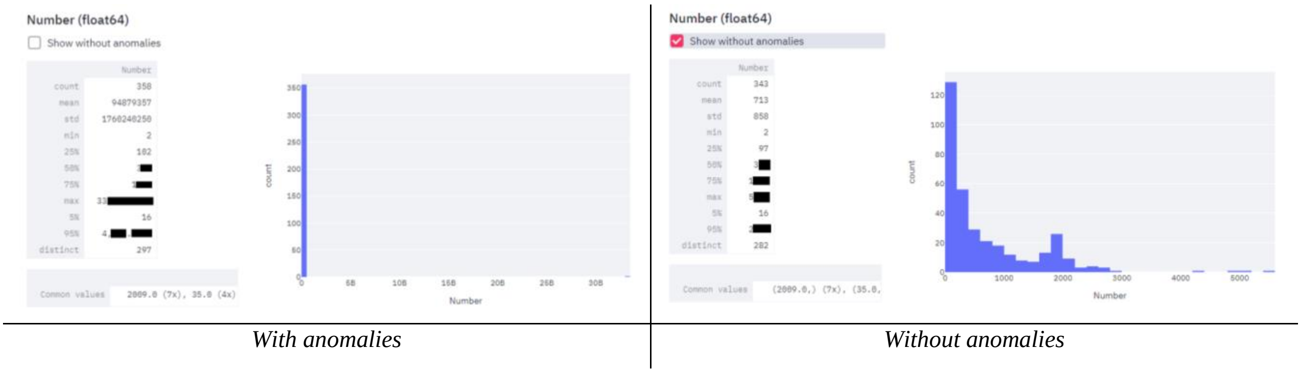
DeliverDate (datetime64[ns])

□ Show without anomalies

	DeliverDate
count	387
unique	253
top	2018-01-24 00:00:00
freq	6
first	2009-06-29 00:00:00
last	2019-08-08 00:00:00

Timescale DeliverDate: Year

Figure 11: GUI to visualize data over large sets of a specific types of documents, e.g., histograms are of variables such as years and day of month as shown here.



Number (float64)

□ Show without anomalies

	Number
count	358
mean	94879357
std	1760240250
min	2
25%	102
50%	[redacted]
75%	[redacted]
max	[redacted]
5%	16
95%	[redacted]
distinct	297

Common values	2009.0 (7x), 35.0 (4x)

With anomalies

Number (float64)

☑ Show without anomalies

	Number
count	343
mean	713
std	858
min	2
25%	97
50%	[redacted]
75%	[redacted]
max	[redacted]
5%	16
95%	[redacted]
distinct	282

Common values	(2009.0,) (7x), (35.0,

Without anomalies

Figure 12: GUI to show the histogram of a variable with and without anomalies.

7. TRAVEL PATTERN EXTRACTION

Passports include visa pages that may be stamped with entry and exit information of travelers. This travel information is commonly used as one of the indicators of risk (e.g., frequency of travel or duration of the visit), which may lead to more thorough inspection of the document. The travel pattern is defined as a sequence of exit and entry events. This section describes the automatic extraction of the travel patterns from stamps on the visa pages in passports.

7.1 Video-based travel-pattern extraction

The document analysis system that processes a real-time video stream of passport pages being flipped and reconstructs the travel pattern from detected stamps is implemented by BPTI. The implementation consists of a sequence of convolutional neural network models (CNNs) that form a pipeline for travel pattern extraction from a real-time video stream (Figure 13). Video frames are being sent into the pipeline which outputs the travel pattern in the form of a table. Each frame is sent to a classifier which recognizes the state of the passport (no passport, flipping, ready for processing). If the state is recognized as ready, the frame is further processed as follows: first, the page boundaries are detected, then the stamps are detected in the cropped image of the page and lastly the individual stamp images are being sent to models which extract date, stamp country and travel direction (incoming or outgoing). The current stamp detection and analysis pipeline is specialized for Schengen area stamps but could be extended by using more training data. The passport state classification model is based on ResNet18 architecture [He, 2016]. The page and stamp detection models are based on the single-shot detector YOLO [Redmon, 2016] with ResNet18 backbone. After detection of the stamp bounding quadrangles, the images of date, country code and direction symbols can be cropped. Country and direction recognition is implemented by using CNN classifiers with 5 convolutional layers followed by a global average pooling and a fully connected layer. Since the number of digits in the date is fixed, a specialized CNN architecture is used for date recognition: ResNet18 is used as a backbone to construct a feature map which is passed through two fully connected layers. The output is interpreted as a 10x6 matrix describing class confidence scores for the 6 date digits. Due to low amounts of available data, various data synthesis methods were employed to achieve the required amounts of training examples for the CNN models.

After training, the models achieved high accuracy on the validation data. We also qualitatively tested all models as a pipeline on a real-time video stream and it was concluded that all models demonstrate enough performance to be practical. Date recognition model works especially well and recognizes digits accurately even in the cases of blurry images, incomplete characters, and problematic backgrounds. Country and direction classifiers show a significant drop in accuracy on real data, but the developers believe that this could be fixed just by increasing the amount of training data. As all of the models are small compared to the state-of-the-art computer vision CNNs, they require significantly less computing resources and allow the processing of real-time video feed even on a laptop without GPU (graphical processing unit).

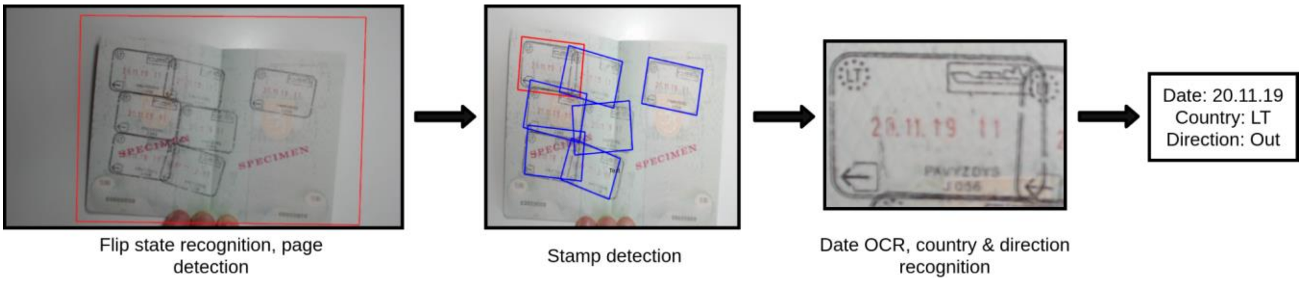
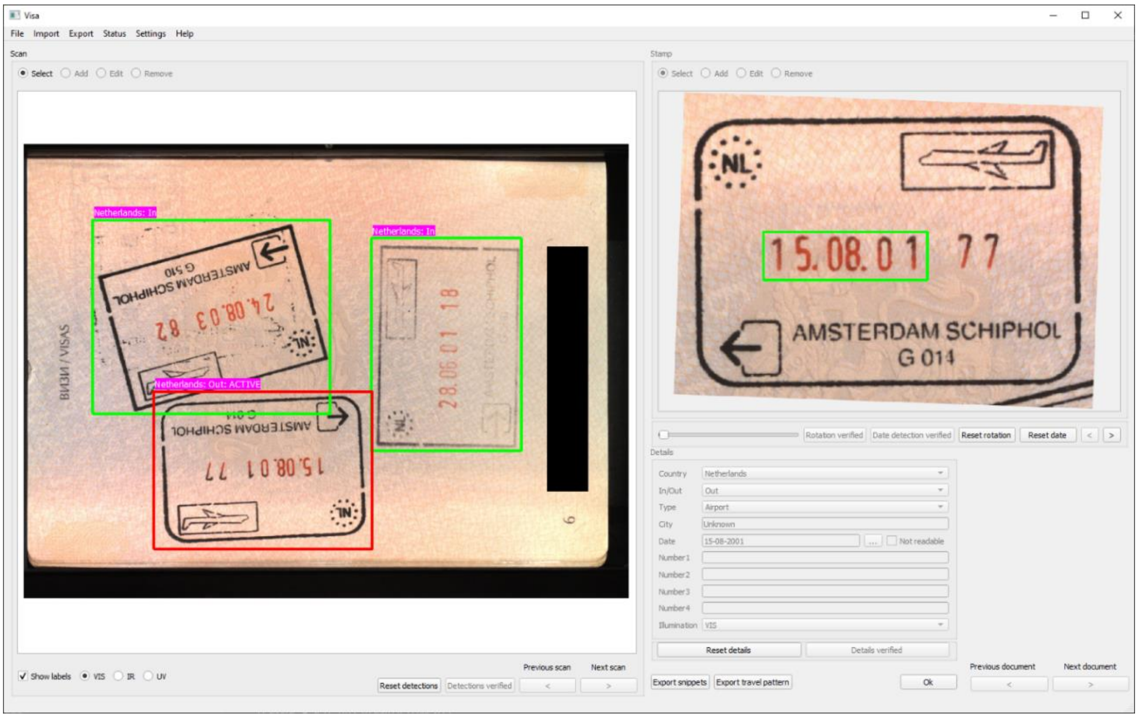

Flip state recognition, page detection
SPECIMEN
Stamp detection
Date OCR, country & direction recognition
Date: 20.11.19
Country: LT
Direction: Out

Figure 13: Video-based travel pattern extraction pipeline.

7.2 Image-based travel pattern extraction

The method is implemented by TNO and consists of five main components: stamp detection, stamp rotation, country + in/out + transport type recognition, date detection and date recognition. The Deep Neural Networks (DNNs) are trained to recognize stamps in challenging situations (with overlap and various backgrounds) for a wide variety of countries and characters. The stamp detection is identical to the detection that was described before (Section 4). The second component aims to recognize the country and the direction of movement (arrival or departure). It performs the recognition by means of finding the best match of the stamp within a database of stamps with known labels (country and departure/arrival and type of travel). This is implemented with Triplet-REID [Hermans, 2017] using a ResNet50 network [He, 2015]. The third components detects the orientation of a stamp using a ResNet18 network and rotates the stamp into an upright position. The fourth component performs date detection and its implementation is identical to the detection of the complete stamp. The fifth component extracts the date and it is implemented with Keras-OCR [KERAS_OCR].

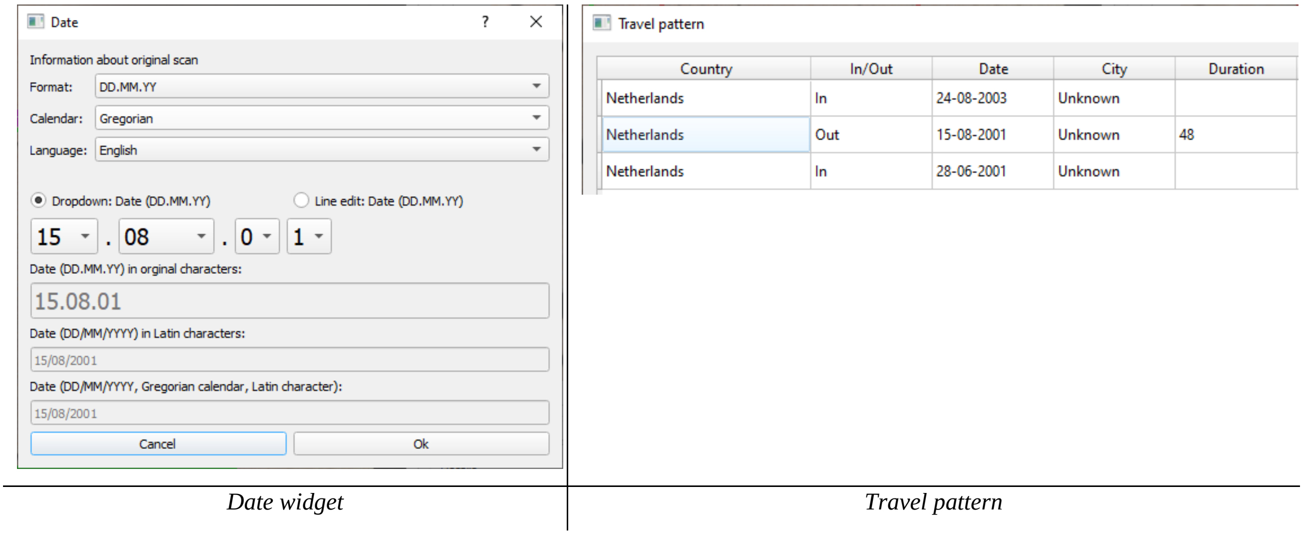
The GUI is shown in Figure 14. The left part of the GUI shows a visa-page with three detected stamps. The top-right shows one stamp with the detected date. The bottom-right shows meta-data that is automatically extracted from the scan. If one of the fields is incorrect, it can be modified by the user. For dates, a special date widget is used to keep the formatting consistent and to assist the user with different characters or calendars (Figure 15-left). Finally, based on the information extracted from all the stamps, the travel pattern of the document is visualized with the duration of stay (Figure 15-right).



Details

Country: Netherlands
In/Out: Out
Type: Airport
City: Unknown
Date: 15-08-2001 ... □ Not readable
Number1:
Number2:
Number3:
Number4:
Illumination: VIS

Figure 14: GUI shows detected stamps (left), detected date (top-right), and extracted data (bottom-right).



Information about original scan

Format: DD.MM.YY

Calendar: Gregorian

Language: English

● Dropdown: Date (DD.MM.YY) ○ Line edit: Date (DD.MM.YY)

15 . 08 . 0 1

Date (DD.MM.YY) in orginal characters: 15.08.01

Date (DD/MM/YYYY) in Latin characters: 15/08/2001

Date (DD/MM/YYYY, Gregorian calendar, Latin character): 15/08/2001

Country	In/Out	Date	City	Duration
Netherlands	In	24-08-2003	Unknown	
Netherlands	Out	15-08-2001	Unknown	48
Netherlands	In	28-06-2001	Unknown	

Date widget | *Travel pattern*

Figure 15: The date widget allows the user to correct the data that is automatically extracted by the system (left). Based on the stamps on all pages of the document, a travel pattern is generated (right).

8. BLOCKCHAIN FOR INSPECTION HISTORY

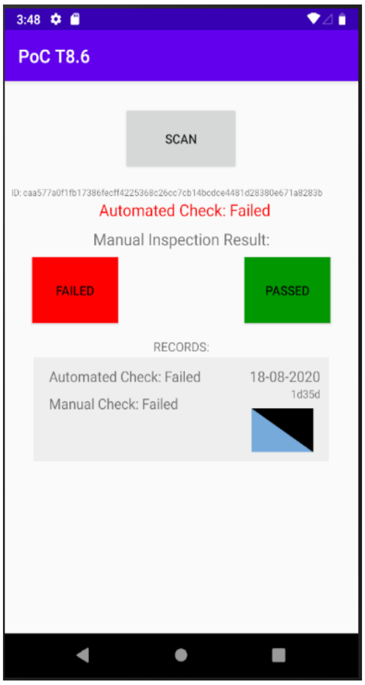
Blockchain is a cryptography-assured technique for storing information in an immutable manner. The technique is based on distributed ledger architecture, in other words, a distributed database containing replicated data [Sunyaev, 2020]. From the viewpoint of inspection history, blockchains ensure immutability and thus trust, that the record history remains unchanged. The immutability is based on the decentralized architecture and the cryptographic techniques used in the storage of the records.

The tool developed by VTT for the D4FLY project is an application allowing border guards to read previous inspection records of travel documents of the traveler crossing the border (Figure 16). The application also enables the border guard to insert new inspection records. All the records are stored in and read from the Ethereum [Wood, 2014] blockchain. In the scenario of the aimed use, the traveler presents the passport, for which the document scanner generates a unique document identifier, unambiguously defining the passport. The application then retrieves the verification history of the travel document. The identifier never contains any personal data, and is used to refer to all the records related to that particular travel document. Records contain information about authorities who have signed those records and possible comments from the border guard. The test process consists of the following steps:

1. Document is scanned,
2. History records are read,
3. (In case of failed automated verification of the travel document): The result of manual verification are chosen,
4. (In case of failed automated verification of the travel document): A comment about the check can be written.

If the travel document is automatically accepted, the result will be directly sent into the blockchain by the application without the need for any interaction.

The application was tested. The test process was performed 1) first with a virtual device in virtual environment and 2) second time with a physical device with printed documents over a local network connection. During the experiment, no failures were found, but the user interface was improved based on the results. However, there was some delay caused by the local network.



ID: caa577a0f1fb17386fecff4225368c26cc7cb14bcdce4481d28380e671a8283b

Automated Check: Failed

Manual Inspection Result:

RECORDS:

Automated Check: Failed 18-08-2020

1d35d

Manual Check: Failed

Figure 16: GUI for travel pattern inspection based on blockchain technology.

9. ELECTRONIC PASSPORT VERIFICATION

Biometric passports or *ePassports* were introduced in the early 2000s, and are nowadays standardized by the International Civil Aviation Organization (ICAO) in Document 9303, Machine Readable Travel Documents [ICAO, 2021]. They contain a machine readable RFID (radio-frequency identification) chip that holds data about the passport and its authorized holder, organized in specified data groups. The chip can be read and verified according to protocols defined in Document 9303, Part 9 [ICAO, 2021].

To guarantee the authenticity and integrity of the data, it is secured by means of a public key infrastructure (PKI). This is designed to prevent fraudsters changing the data on the chip, cloning the data onto a different chip or creating a completely new chip. Additionally, each passport can be traced back to a root of trust. To achieve this, all the data on the chip is secured with a digital signature of a so called “document signer”, which is stored on the passport chip in the Document Security Object (EF.SOD). To verify this signature, the passport contains a certificate of the document signer, which itself is signed by a “country signer” (Figure 17). Many countries upload the public keys of their country signer and document signers into a public database which is hosted by the ICAO. These keys serve as a root of trust and can be used during passport verification.

By the end of 2020, some 150 countries and regions were issuing *ePassports* although as of 14 June 2021, only 78 countries were members of the ICAO PKD, and sharing public keys to their country and document signer certificates.

Traditionally, the cryptographic checks of passports check the mathematical correctness of the cryptographic primitives (e.g. if all signatures are correct, if the certificate chain is valid, if all hash values of the data is correct) as well as some checks of the metadata (e.g. if the signature date of the signature lies within the validity dates of the signing certificate). However, one aspect is currently missing in state-of-the-art verification systems: If one of the keys used for the signatures of the passport is susceptible to cryptographic attacks, the chain of trust could be compromised, and the passport should be further evaluated, because the authenticity and/or integrity of the data cannot be guaranteed anymore.

The ROCA (Return of Coppersmith’s Attack) was found by Nemec et al in 2017 [Nemec, 2017], and is due to a faulty implementation of the RSA key generation in a widely used library. RSA is a public-key cryptosystem developed in the 1970’s by Rivest, Shamir and Adleman [Rivest, 1978], which is until today one of the most used algorithms for cryptographic encryption and signatures. Currently, many countries still use it to sign their passports. If one of the cryptographic keys inside the PKI of the passport is susceptible to the attack, it is possible to calculate the secret (private) key from the public key, stored on the passport. While it is not trivial to perform this calculation, it is relatively easy to identify RSA keys that are susceptible to the attack. If an attacker would find a passport with such a weak key, it would be possible to change the data on the passport, or create a completely new passport with fraudulent data. Such an attack could then not be detected by systems implemented according to the ICAO protocol, because the certificate chain is valid.

To catch such passports, a module was created by Veridos that checks the cryptographic keys inside the passport using an open-source tool [ROCA, 2017]. If a passport is inserted into the reader, the system extracts the public keys stored on the passport, performs the ROCA check, and if the key is susceptible to the attack, the result is shown in the graphical output of the system. To check if the module works as expected, first some unit tests were developed where the module has to correctly identify several susceptible and non-susceptible keys. Additionally, a passport with a susceptible key was created, and checked in the complete system. All tests were successful and showed that the module works as expected. Additionally, the whole ICAO database of document signers and country signers was fed into the module to identify susceptible keys, however, no susceptible keys were found.

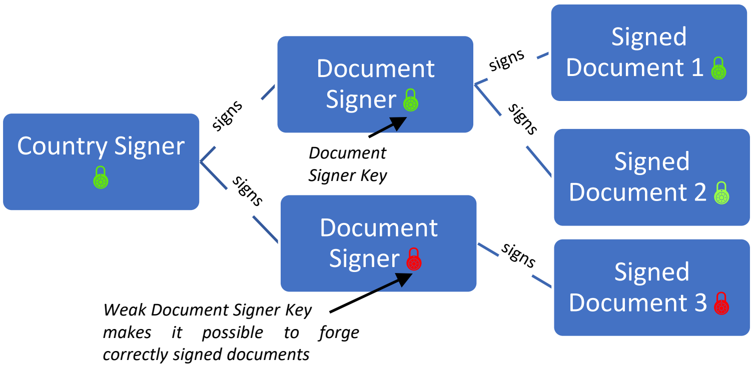


Figure 17: Relation between country/document signers and the signed document (green/red icons visible in color print).

10. CONCLUSION

This paper presented five categories of new technologies in automated document authentication to overcome the limitations of current document analysis systems in automated and non-automated border control scenarios. The first category consists of techniques related to the verification of visual security features on the holder page of travel and identity documents (Kinegram analysis, ADAM presence detection, printing techniques). The second category consists of techniques related to the analysis of breeder documents (detail level and tactical level). The third category uses information from the visa pages in passports (travel pattern extraction). The fourth category is an analysis of the border-guard inspection history in a distributed ledger (blockchain). The last category analyzes the electronic chip of a passport (detection of vulnerable cryptographic keys). The separate modules are integrated into two demonstrators: one for the analysis of breeder documents and one of the analysis of travel documents. The demonstrators are tested by end users in the D4FLY project and feedback is used to further improve the modules and the demonstrators.

ACKNOWLEDGEMENT

The work described in this paper is performed in the H2020 project D4FLY (“Detecting Document frauD and iDentity on the fly”). This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833704.

REFERENCES

[1] Alcantarilla, P., Nuevo, J., Bartoli, A., “Fast explicit diffusion for accelerated features in nonlinear scale spaces,” BMVC, (2013).

[2] Baek, Y., Lee, B., e.a., “Character Region Awareness for Text Detection,” IEEE CVPR, (2019).

[3] Boer M. de, Bouma, H., Kruithof, M., et al., “Automatic analysis of online image data for law enforcement agencies by concept detection and instance search,” Proc. SPIE 10441, (2017).

[4] Bouma, H. Pruim, R., Van Rooijen, R., Ten Hove, J., Van Mil, J., Kromhout, B., “Document anonymization for border guards and immigration services,” Proc. SPIE, vol. 11542, (2020).

[5] Chen, K., Wang, J., Pang, J., et al., “MMDetection: Open MMLab Detection Toolbox and Benchmark”, CoRR, http://arxiv.org/abs/1906.07155, (2019).

[6] Europol, “Serious and organized crime threat assessment (SOCTA),” Publications Office of the EU, (2021)

[7] Fischler, M., Bolles, R., "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography," Communications of the ACM 24(6), 381-395 (1981).

[8] Frontex, “Risk analysis for 2018,” Frontex report 2671/2018, (2018).

[9] He, K., Zhang, X., e.a., “Deep Residual Learning for Image Recognition,” arXiv:1512.03385, (2015).

[10] Hermans, A., Beyer, L., & Leibe, B., “In defense of the triplet loss for person re-identification,” arXiv:1703.07737, (2017).

[11] ICAO, “Machine readable travel documents”, ICAO Doc 9303, (Eighth edition, 2021).

[12] Lee, S., Tama, B., Moon, S., Lee, S., “Steel surface defect diagnostics using deep convolutional neural network and class activation map,” Applied Sciences 9(24): 5449 (2019).

[13] Liu, F, Ting, K., Zhou, Z., “Isolation forest,” IEEE int. conf. data mining, 413-422 (2008).

[14] Mikkilineni, A., Chiang, P., Ali, G., Chiu, G., Allebach, J., Delp, “Printer identification based on graylevel co-occurrence features for security and forensic application,” SPIE 5681, (2005).

[15] Nemec, M., et al., “The return of Coppersmith's attack: Practical factorization of widely used RSA moduli,” Proc. ACM SIGSAC Conf. Computer and Communications Security (2017).

[16] Peters, J., “Enhancing the reliability of automatic document inspection at our borders,” INFOSECURA 77, 13-15 (2017).

[17] Peters, J. Walter, H., Staub, R., Hoffmann, M., “Transforming DOVID’s for the emerging digital world,” Optical & Digital Document Security, 125 – 135 (2020).

[18] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A., “You only look once: Unified, real-time object detection,” IEEE CVPR, 779-788 (2016).

[19] Ren, S., He, K., Girshick, R., Sun, J., “Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks”, IEEE Trans. Pattern Analysis and Machine Intelligence 39, 1137-1149 (2017).

[20] Rivest, R., Shamir, A., and Adleman, L., “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM 21(2), 120-126 (1978).

[21] ROCA, https://github.com/crocs-muni/roca

[22] Rooijen, A. van, Bouma, H., Verbeek, F., “Fast and accurate person re-identification with Xception Conv-Net and C2F,” IberoAmerican Congress on Pattern Recognition CIARP, (2018).

[23] Simonyan, K., & Zisserman, A., “Very deep convolutional networks for large-scale image recognition,” ICLR, (2015).

[24] Sonka, M, Hlavac, V., Boyle, R., “Image processing, analysis and machine vision,” Brooks Publishing, (1999).

[25] Streamlit, https://github.com/streamlit/streamlit

[26] Sunyaev, A., “Distributed Ledger Technology,” Internet Computing Springer, 265-299 (2020).

[27] Tesseract-OCR, https://github.com/tesseract-ocr/

[28] Thirion, J. "Image matching as a diffusion process: an analogy with Maxwell's demons," Medical Image Analysis 2(3), 243-260 (1998).

[29] Wang, Zhou, et al. "Image quality assessment: from error visibility to structural similarity." IEEE Trans. Image Processing 13(4), 600-612 (2004).

[30] Wood, G., “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol 151, 1-32 (2014).