Optical Security Document Simulator for Black-Box Testing of ABC Systems

Michael Gschwandtner*, Svorad Štolc†, Franz Daubner‡

Intelligent Vision Systems, Safety & Security Department
AIT Austrian Institute of Technology GmbH
2444 Seibersdorf, Austria
Email: *Michael.Gschwandtner@ait.ac.at, †Svorad.Stolc@ait.ac.at, ‡Franz.Daubner@ait.ac.at

***Abstract*—Ever increasing passenger numbers have prompted the rise of automated border control (ABC) systems. Such systems are expected to perform the identity check of a traveler with the same or higher reliability as a human border guard. One important aspect of such a control is the authentication of the identity document provided by the traveler. To ensure a constant quality of the authentication process it is necessary to subject the ABC system to a thorough testing on a number of different document samples. Given the ever increasing number of eGates in operation all over the world, this testing becomes a technically infeasible task, which may have severe security implications. In this paper, we propose a system that can automate such quality assessments using an optical document simulator. Our simulator uses a similar principle as that of an active display attack, where a mobile device is used to trick automated document readers.**

***Index Terms*—security document authentication, document simulation, ABC system testing, automated border control, MRTD, passport**

I. Introduction

Asynergistic effect of the global adoption of automated border control (ABC) systems (commonly known as eGates) is the necessity to guarantee a constant quality of the document authentication subsystem, which is a very important subsystem of every eGate. This is an inevitable step in order to ensure a prescribed level of security in the automated border control scenario.

In this paper, we propose a system that can automate the testing of the optical document authentication, exploiting an intrinsic weakness of the underlying acquisition process.

Most modern document readers acquire an image of the document by illuminating it in multiple spectral ranges and taking pictures formed by the light either reflected or emitted by the inspected security document. Depending on the light source position with respect to the document and the camera, this process acquires both the diffuse and specular components of the reflected light. Most security documents are equipped with multiple optical security features that have diverse reflectance/emittance properties in different spectral ranges. In order to capture those properties, the scanner must acquire several images of the document under varied illumination and possibly by using multiple cameras equipped with special optical filters.

In a typical case, the document reader uses a single camera to acquire a sequence of three images taken under three different lighting conditions: (i) visible white, (ii) infrared, and (iii) ultraviolet (UV-A) light. Afterward, the document authenticity is verified by checking all the obtained images against predefined templates of the genuine document. The security of this approach originates from the assumption that it is very difficult or even impossible to forge a document, which would perfectly imitate a genuine document in all inspected security features without access to production mechanisms, materials, etc. Nevertheless, in [1] it was shown that this assumption does not hold true in the automated border control scenario, where an active display can be used to trick the scanning process itself rather than creating a counterfeit document. Such an attack is also know as a presentation attack. Furthermore, the whole automated document inspection needs to be carefully evaluated and tested on a regular basis in order to maintain the overall level of security. If this step is not done correctly or completely omitted, the actual security provided by the affected ABC system can be significantly lower than expected [2].

The paper has the following structure: Section II gives a brief overview of the prior art in this research area. In Sections III, the proposed document simulator for the black-box testing of ABC systems is described in detail. In Section IV, we provide several use cases for the proposed device and pay attention to possible countermeasures against the presentation attack. Finally, conclusions are drawn in Section V.

II. Prior art

In [1], an attack on security document readers has been shown that exploits the fact that most currently available document readers use a sequential scanning process to acquire images of the document in different spectral ranges.

A. Document specifications

Most identity documents that are used nowadays are based on the ICAO 9303 standard [3], which specifies the basic properties as well as commonly used security features. Guidelines and requirements for the automated verification of such documents can be found in [4] and [5].

B. Document authentication

In [6], a system for the automated authentication of security documents using generic spectroscopic methods is shown. This

work is based on the assumption that security inks and papers have very specific spectral properties which cannot be easily forged or substituted. In [7], a similar method for document authentication is presented where the spectral analysis is limited to a certain set of spectral ranges by acquiring a sequence of images of the document illuminated by a light with different wavelengths. A method to authenticate a security document through the detection of presence or absence of certain security features is described in [8]. Preventing the modification of individual parts of a document by adding invisible information using steganographic methods and watermarking methods is proposed in [9].

III. System description

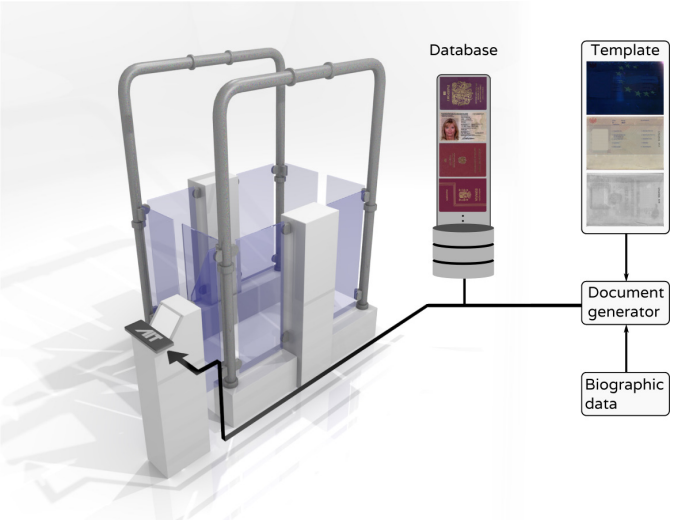

Figure 1. Overview of the document simulation in the ABC context.

A. Document simulator

A simulator can be any device with a high resolution active display that is big enough to cover the area of the document to be simulated. Furthermore, the device needs a means to detect changes in the illumination which is emitted by the document reader. In general there are two alternative hardware setups relevant for the proposed document simulator:

- *Simulator running on a smartphone* – One example of this all-in-one solution is the setup described in [1], where a smartphone with the Android operating system was used in the active display attack experiments. It is crucial that the brightness sensor of the employed smartphone is able to detect changes in the near-infrared spectrum;
- *Simulator running on a dedicated hardware* – In this paper, we devote to this setup as it provides more flexibility with a choice of hardware components in order to simulate security document as large as standard ePassports. The proposed setup consists of 7" full HD display, Raspberry Pi running a stock Debian Linux, Arduino with a photo diode, and a WiFi access point for a remote control of the simulator. The Hardware is housed inside a transport case. As shown in Figure 2, the virtual document – the display – can be taken out from the case and placed on the document reader.

Figure 2. The proposed document simulation setup running on a dedicated hardware. The display simulating a passport as well as the brightness sensor (red and black wires) are placed together on the document window of a reader device. The simulator is controlled via wireless network from a nearby laptop.

The work-flow of the simulation is shown in Figure 3. The simulation works in the following steps:

1) The simulator shows the first image that the document scanner expects. In the example shown in Figure 3 it is the infrared (IR) image, because the employed document reader acquires the IR image first. The simulator always displays the first image even before the scanning process has started. The reason is that the IR acquisition is typically very short, which makes it quite difficult to detect the initial IR flash and switch to the correct image on the fly.
2) The system tries to detect the IR flash signalizing that the IR acquisition has already started. This is done by means of the external brightness sensor or the on-board brightness sensor in the case of a smartphone-driven simulator.
3) Once the IR acquisition is detected the IR image is kept shown for a certain amount of time (so-called IR duration).
4) The second image to be displayed is the passport image acquired under the visible white light (so-called White image). The current version of the simulator assumes that the timing of the scanning process is constant throughout different acquisitions thus no additional detection of flashes is necessary.
5) The White image is also shown for a certain amount of time (so-called White duration).
6) Afterward, the ultraviolet (UV) image is displayed for a longer period since no further steps are left.

The result of such a simulation is shown in Figure 4, where the images of a genuine document (an Austrian ePassport) were first acquired by the system under test. Afterward, they

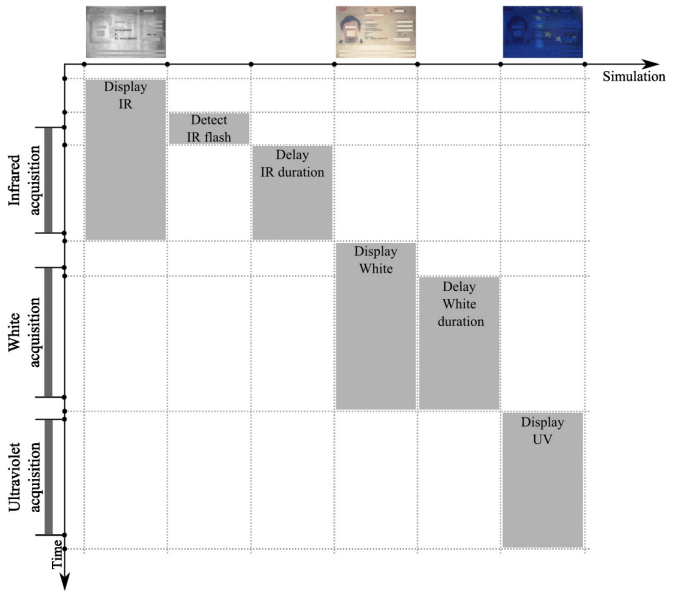

Figure 3. Simulation of an arbitrary security document by exploiting an intrinsic weakness of most currently available document readers.

were uploaded to the simulator and displayed without any further preprocessing. It can be seen that in this basic example, the simulated document renders slightly brighter than the genuine document. To account for such deviations, an image preprocessing step is required, in which different filters (e.g., contrast & brightness adjustment) would be applied to the images before their presentation on the display.

B. Document database

In this mode, the document simulator is either loaded with a previously acquired set of document images or the document database is stored on a remote machine and the passports are sent one-by-one to the simulator. The document simulator reliably reconstructs appearance of the provided documents as if they were physically present in the scanner. In the current version of the simulator, each passport is represented by a set of three images – IR, White, UV. An example of such a data set is shown in Figure 4 (a). By switching between data sets representing acquisitions of different documents, the document simulator can be used to test an arbitrary number of security documents in an automated or semi-automated way.

C. Document generator

Using empty unpersonalized document templates the simulator can generate an arbitrary number of passports, which can be compared to a virtual "printing". The information to be printed on the passport are configurable and can be controlled remotely. This mode has been successfully used to simulate different passports of the same type with varying personalized information. For printing texts the simulator uses the OCR-B font as it is required by ICAO 9303 [3]. For more advanced custom scenarios the method can be extended to simulate other effects, such as an UV security print. Since the personalization process of a passport is applied after the document has been created the personalized information is subject to spatial and appearance variations. Naturally, the proposed simulator is capable of printing the customized elements at arbitrary locations.

Figure 4. Side-by-side comparison of images obtained by a document reader for (a) an Austrian ePassport and (b) a simulated version of the same document. Rows comprise images associated with different spectral channels, i.e., IR, White, and UV, respectively. Images of the genuine document were used as templates in the simulation.

IV. Use cases

The document simulator can be either preloaded with the documents to be tested or the data can be sent to the simulator over WiFi. The simulator provides an HTTP interface which enables manual control of the operation through a web browser or in an automatic fashion directly from other software via a REST interface.

By using the REST interface the simulator can be easily integrated into already existing testing solutions.

A. Black box testing

Analyzing the document authentication back-end of an eGate could be done by interfacing with the authentication software directly. In such a case, the test images can be sent to the document authentication software directly without going through the image acquisition process. In some cases, this might be the right course of action but has several disadvantages:

- The vendor has to provide access to the document authentication system. Some vendors might not be willing to provide access to the core modules directly.

- The data has to be acquired by the document scanner under test. Otherwise the tests will not reveal problems specific to a certain document reader.
- The testing has to be adapted for each software individually. There is no common interface to the authentication system.
- The software has to be replicated exactly as it would be used in the eGate under test. There might be interaction between software components that produce side effects which are not reproduced correctly in a lab environment.

A solution to those problems is to test the eGate as a whole in the actual location where it is being operated. This is also useful for continuous reevaluation of the systems and a way to detect deviations, either deliberate or accidental, of the eGate operation without necessity to have an access to the eGate control software. The simulator can run a number of test cases automatically, either from a document database or by generating new documents on the fly.

B. Document variations

Even though identity documents usually have very strict quality requirements, there are still some variations in the production process, especially associated with the personalized information that is added only at the end of the production process. Additionally there is aging of the document, dirt, scribbles, as well as wear&tear effects which may have severe impact on the optical properties of a document. The proposed simulator can efficiently emulate the mentioned effects and, therefore, allows for a systematic evaluation of how well a document authentication system copes with different types of document variations.

C. Presentation attack detection

The technique to simulate an arbitrary security document has been re-purposed from the active display attack presented in [1]. One important aspect of the document simulator is the use in the risk assessment of such a class of attacks. In order to guarantee a certain security level, the important question to be answered is, whether document authentication systems can have the ability to recognize the genuine document from the simulated one. This problem is also known as a presentation attack detection (PAD). If such attacks become widely used, there needs to be a way to certify and promote scanners that are able to withstand such attacks. Moreover, if future document scanners were able to detect the use of a dedicated simulator, they should be able to detect attacks performed by a less capable hardware, such as smartphones.

V. Conclusions

In this paper we presented a novel tool intended for the evaluation of automated document authentication systems such as those of eGates. The proposed simulator allows for the black-box testing of an eGate as a whole against an arbitrary number of specimens without the need for manual interaction. Besides testing the quality of the document authentication, the simulator can also be used for verifying the PAD robustness. The current version of the simulator supports basic document simulation functions which are useful for augmenting standard manual tests.

Our prototype of the proposed simulator was tested in combination with one commonly used document reader and an Austrian ePassport. In this configuration, the simulator proved to work reliably providing highly reproducible results (i.e., the reader accepted all generated virtual passports). In order to use the simulator with a wider range of documents and readers, a proper evaluation of the device will be necessary. Since there are currently no guidelines for security document authentication (that are explicit about security features to be inspected as well as methods for their verification, acceptable ranges, etc.), defining an evaluation process for the simulator is a non-trivial task. Nevertheless, we suggest that the first step in evaluating the simulator should be the verification of its functionality with a larger number of document readers and thus gain an understanding on how the state-of-the-art readers differ w.r.t. the proposed simulator. The development of requirements for future document readers should then go hand-in-hand with the evaluation of the simulator and extending its capabilities especially in the context of simulating the broad range of possible variations that arise from the production and personalization of security documents.

Acknowledgment

This work has been supported by the FastPass project and received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583.

References

[1] M. Gschwandtner, S. Štolc, and A. Vrabl, "Active display attack on automated security document readers," in *Optical Document Security, International Conference on*. San Francisco: Reconnaissance International, Jan. 2014.

[2] M. Gariup and G. Soederlind, "Document fraud detection at the border: preliminary observations on human and machine performance," in *Intelligence and Security Informatics (EISIC), European Conference on*, Uppsala, Aug. 2013, pp. 231–238.

[3] International Civil Aviation Organization (ICAO), "Machine readable travel documents - machine readable passports," 2006.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Maschinell gestützte dokumentenprüfung in hoheitlichen kontrollinfrastrukturen."

[5] Frontex, "Best practice technical guidelines for automated border control (abc) systems, version 2," Aug. 2012.

[6] M. Bart, "Spectroscopic methods for secure document authentication: An application to the automated handling of sheet-like objects," Ph.D. dissertation, Linnaeus University, School of Computer Science, Physics and Mathematics, 2010.

[7] R. B. Blair, "Systems and methods for spectral authentication of a feature of a document," Patent US 13/563,612, Feb., 2014. [Online]. Available: http://www.google.com/patents/US20140037196

[8] Y. Lei, "Document authentication using template matching with fast masked normalized cross-correlation," Patent US 8,485,559, Jul., 2013. [Online]. Available: http://www.google.com/patents/US8485559

[9] J. S. Carr, B. W. Perry, and G. B. Rhoads, "Identification documents and authentication of such documents," Patent US 8,280,101, Oct., 2012. [Online]. Available: http://www.google.com/patents/US8280101

[10] A. Sinha, "A survey of system security in contactless electronic passports," *Journal of Computer Security*, vol. 19, no. 1, pp. 203–226, Jan. 2011. [Online]. Available: http://dl.acm.org/citation.cfm?id=1971852.1971858