Document security in the age of fully automated border control systems

Michael Gschwandtner[1], Svorad Štolc[2]

Austrian Institute of Technology
Safety & Security Department
[1]michael.gschwandtner@ait.ac.at
[2]svorad.stolc@ait.ac.at

Abstract: Automated checking of identity documents is heavily used in border checks all over Europe. In the conventional scenario, document scanners are only assisting devices operated by trained border guards. In such a configuration the operator can compensate for classification mistakes made by the document verification subsystem, which is not possible in fully autonomous border control setting. In this paper we show possible risk scenarios in currently used optical security feature verification methods as well as electronic security feature verification.

***Keywords*:** optical security features, electronic security feature, security documents, counterfeit detection, security analysis

INTRODUCTION

With the ever increasing number of travelers, border checkpoints are confronted with the necessity to increase the number of people to be processed. One popular solution to cope with such increased demand in almost any part of our daily lives is the automation. The same holds true for border checkpoints. Rise in demand is increasingly solved by putting automated border control systems in place. However, automating a process usually means that some steps have to be simplified. This can lead to a checking process which might be more vulnerable to certain attacks, when compared to a normal human-led border control [1].

In current border control scenarios, document scanners along with the document verification subsystem are mainly used as assisting devices. This configuration does not pose any serious security issue, as the final decision remains with the border guard operating the device. Therefore the document authentication can be tuned for maximum throughput even with the knowledge that some documents might slip through the automated check. On the other hand, in fully autonomous systems, such a bias towards acceptance of a document even if it might be forged or manipulated would have serious security implications. The tests in [1] show that current systems are already leaning towards accepting forged documents. In this paper we show that it is a non-trivial task to authenticate a document even if the automated document checks would be configured to be cautious and more likely reject a genuine document (false rejection) than accept a fake document (false acceptance).

OPTICAL SECURITY

Checking of optical security features is typically implemented by using special metrics (i.e., image quality metrics), which compare parts of the document against a reference stored in a database. This reference usually contains several numerical values such as mean and standard deviation, feature vectors characterizing certain areas within the document, reference image data like image patches, or even a sample of the whole document. The underlying assumption of those checks is that a counterfeiter cannot produce a document so that it would match the reference close enough to be accepted as genuine. However, in reality even the genuine document does not match the reference completely due to variations in the production process, aging, wear and tear, dirt, etc. Therefore the system has to allow for slight deviations from the reference, which in turn increases possibility to accept non-genuine documents.Image quality metrics are a thoroughly researched field in computer vision with a continued development of new methods to adapt to special requirements [4]. However, such metrics are not necessarily suited for detecting forgeries or document fraud.

In order to demonstrate problems which may arise from straightforward application of standard image metrics in the document authentication process, we conducted an experiment with the simulated modification of an Austrian passport. The original image patch extracted from a certain region of the genuine passport (see Figure 1a) was manipulated by using an image editing software and afterwards compared with the original unmodified image by means of commonly used image metrics. The image in Figure 1b was derived from the original image patch by a

clockwise rotation by 0.3 degrees and a slight increase in brightness. The second manipulated image in Figure 1c has a faint text spelling “FRAUD” overlaid over an otherwise untouched image.

(a) Original (b) Rotated by 0.3 degrees, increased brightness (c) Text overlaid

Figure 1. Three versions of the same image patch of a genuine passport.

It is clear, that even an untrained human observer can immediately recognize the overlaid text in Figure 1c, even without any reference image available. On the other hand, the difference between Figures 1a and 1b may not be visible even for a trained border guard. However, with respect to many standard image similarity metrics, the image in Figure 1c is closer to the original than the one in Figure 1b. As a consequence of this, the underlying document of Figure 1c would be considered as more authentic than the document in Figure 1b (see Table 1). The biggest difference between the human observer and an automated method is that the human does not simply compare some values somewhat characterizing the document, but instead automatically reasons about the content of what he sees. Although a comparison of acquired images with the reference data based on image metrics is highly applicable in quality inspection tasks, if applied to the document authentication, where tailored attacks against a system must be expected, more sophisticated checks are inevitable.

	MSE	Normalized cross-correlation	Structural similarity
Rotated and brighter	25.360	0.974	0.931
Text overlay	*6.320	*0.975	*0.973

Table 1. Distance between modified and original image patch of the passport image, using common image similarity metrics. The best values for each metric are marked with an asterisk.

In order to analyze the impact of an image manipulation on the real world document authentication, we conducted a second experiment with commercially available software that is nowadays in use at many borders worldwide. The first step was to acquire a scan of a valid genuine passport. In our case, we used again an Austrian e-passport which at the time of our experiment was approximately 6 years old. The document scanner acquired 3 images associated with different spectral ranges: (i) visible light, (ii) infrared (IR), and (iii) ultraviolet light, denoted to as V_0, I_0, and U_0, retrospectively.

(a) (b)

Figure 2. Example of an UV image from a genuine passport (a) and a modified version of the same image (b). Both images are part of a visible light, UV and infrared image set and were considered as genuine by a commercially available document authentication system. The genuine passport has a similarity of 87% to the template in the database, while the modified passport has a similarity of 94% to the template in the database.

In Figure 2, one can find the acquired UV image U_0 (a) and the manipulated image U_1 (b) derived from U_0 by overlaying the text “FRAUD” in big semi-transparent letters. The tuple (V_0, I_0, U_0) represents a genuine passport and the tuple (V_0, I_0, U_1) represents a passport with an obvious modification. Although the document authentication system is in principle a “black box”, it does provide a list of checks performed during the verification process

along with similarity scores and boolean flags signaling the decision for each individual feature. The similarity score, given in percent, determines how similar the acquired image is to the template stored in the database. The boolean value determines whether the similarity exceeds given threshold, meaning that the feature can be considered as genuine. The comparison of the genuine passport (V_0, I_0, U_0) against the template results in a similarity score of U_0 of 87%. The comparison of the modified passport (V_0, I_0, U_1) results in a similarity score of U_1 of 94%. Making decision just based on these numbers, one would consider the modified image U_1 (shown in Figure 2b) as significantly more authentic than the genuine image U_0 (shown in Figure 2a), even though any human observer would tell otherwise.

To increase the robustness against forgeries while maintaining the usability of a system, a number of security features are validated at once, where each feature has its own independent acceptance range. Correspondingly security documents should be designed so that a counterfeiter might be able to forge few isolated features, but it should be virtually impossible to produce a complete document falling within all acceptance ranges at the same time. In order to achieve this goal, security documents usually contain several security features operating in different spectral ranges [2]. Manufacturers of security documents use materials and inks that have special spectral properties very different from materials and inks available on a public market. Note that the precondition of this approach to the document security is that such materials are regulated by official authorities worldwide and cannot be bought through other than official channels.

Nevertheless, there exists a generic attack on optical security features, regardless of the spectral channel [3]. This attack utilizes electronic displays to simulate the expected responses of valid documents and exploits the fact that the document scanner has currently no way to perform the implicit task of ensuring that the presented document is in fact a real document. Such a task is performed by a border guard without even thinking about it.

ELECTRONIC SECURITY

The electronic part of an e-passport is often cited as the be-all and end-all solution for securing identity documents. Although it is, under some circumstances, possible to clone a valid e-passport, there is still no known attack that can create a forged document. Nevertheless, replacing the current e-passport, containing both the optical and electronic security features, by a chip-only solution would cause the electronic part of the current passport to become the sole security feature, which might result in additional security risks.

The schematic in Figure 3 shows the most important parts involved in the issuing and verification of an e-passport with basic authentication (BA). It starts with the initial creation of the country signing certificate authority (CSCA) through the embedding of the biographical data (BIO) to the verification of the signature and the extracted document signer key (DS). Even though cryptoanalysis has not yet found a practical weakness in the signing process of current e-passports, the whole process has several attack vectors that range from man-in-the middle attacks up to social engineering. The following is a list of a by far non-exhaustive list of possible attack vectors on the current security model of electronic passports:

- Point 1 in Figure 3 shows possible problems with the creation of the CSCA and the DS itself. If the quality of the random number generator is to low, the resulting certificates are prone to attacks. Weak random number generators have been found for example in some versions of OpenSSL and some versions of Microsoft Windows.
- Point 2 is the signature creation itself. An attacker does not need access to the private signing keys in order to create a valid signed passport. He needs to store data which has the same hash values (also called collision attack) as the original passport it is derived from. While the currently used hashing functions are designed to be robust against collision attacks, cryptoanalysis has already found weaknesses in cryptographic hash functions that have previously been thought secure (e.g., MD5, SHA-0). Fortunately, this does not yet include hash functions used in electronic passports.
- Point 3 shows the transmission of the CSCA public keys to the participating countries. Some countries prefer to download them directly from the official servers of other countries, but these official servers are reached through conventional (insecure) connections. Other possibilities to compromise the

transmission of the certificates are for example compromised webservers and DNS cache poisoning attacks.

- Point 4 shows the scanner itself which might get compromised by a malicious service technician. The simplest attack would be to introduce a fake CSCA certificate resulting in the ability to issue fake passports that cannot be detected.

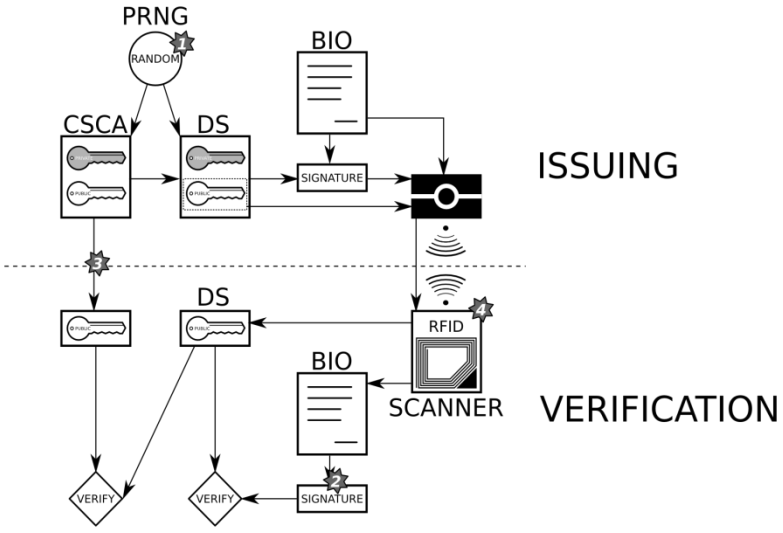

Figure 3. Schematic of the passive authentication. Gray stars mark a non-exhaustive list of possible attack vectors.

CONCLUSIONS

We have shown that current optical security checks are insufficient to authenticate secure identity documents and thus might pose a problem for fully automated border control. In addition, the obvious solution to rely solely on the electronic security of current e-passports should be handled with care, unless one can guarantee with absolute certainty that no part of the whole issuing-verification chain can be compromised, neither through technical attacks nor through a social engineering. As a result of this work the research in automated checking of optical security documents should be increased and based on academically researched and publicly verified methods rather than commercial “black box” systems. An example for public research in this field is shown in [4].

ACKNOWLEDGEMENTS

The work has been supported by the *FastPass* project. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 312583.

REFERENCES

1. Gariup, Monika and Soederlind, Gustav. ”Document Fraud Detection at the Border: Preliminary observations on human and machine performance”, in Workshop on Innovation in Border Control (WIBC), 2013.

2. Khan, Zohaib and Shafait, Faisal and Mian, Ajmal. "Towards Automated Hyperspectral Document Image Analysis", (to appear) in 2nd International Workshop on Automated Forensic Handwriting Analysis (AFHA), 2013.

3. Gschwandtner, Michael and Štolc, Svorad and Vrabl Andreas. “Active display attack on automated security document scanners”, (to appear) in Optical Document Security (ODS), 2014.

4. Ryu, Seung-Jin and Lee, Hae-Yeoun and Cho, Il-Weon and Lee, Heung-Kyu. “Document Forgery Detection with SVM Classifier and Image Quality Measures”, in Advances in Multimedia Information Processing (PCM), 2008.