Document security in the age of fully automated border control systems

Michael Gschwandtner
michael.gschwandtner@ait.ac.at

Andreas Kriechbaum
andreas.kriechbaum@ait.ac.at

Svorad Štolc
svorad.stolc@ait.ac.at
Automated document inspection

- ABC ≠ (manual) border control assisted by automated inspection
- The process is different – the document remains the same
- Same security features
- Should the documents have features that are designed for automated authentication (not just for reading)?
- Could electronic passport security replace the optical part completely?
Document security

- Optical security features
  - Microstructures
  - Special inks
  - Special printing methods
  - Security laminates
  - Optically variable devices (e.g., Holograms)
  - Watermarks
  - Security fibres
  - Special paper

- Electronic security features
  - Basic authentication
  - Passive authentication
  - Active authentication
  - Extended Access Control
Automated checking of optical security features

1. Acquire image of the passport in white, infrared, and ultraviolet light
2. Determine the type of the document (e.g., Austrian ePassport)
3. Compare patches extracted from the acquired images with the correct model stored in a database
4. If the patches and the model are similar enough, the document is considered authentic

- Two examples of such image patches:
  - However, those two are hard to verify reliably with existing document scanners
  - They were not designed with automated checking in mind

- Question: How to assess the similarity of image patches?

Microtext from an Austrian passport acquired with 1200dpi. Note that passport scanners have only around 400dpi.

Hologram (OVD) contained in the security laminate of an Austrian passport. It is intended for being viewed from different angles.
Common image quality/similarity metrics

- Determining the degradation or similarity of an image is a common task in computer vision and multimedia applications.
- Samples of commonly used similarity/quality measures:
  - Mean Squared Error (MSE)
  - Normalized Cross-Correlation (NCC)
  - Structural Similarity (SSIM)
- Using such metrics directly to authenticate optical security features may lead to unsatisfying/misleading results.

<table>
<thead>
<tr>
<th>Original image patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance between the original and the modified image</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Slightly brighter and rotated by 0.3°</td>
</tr>
<tr>
<td>Text overlay</td>
</tr>
</tbody>
</table>
What about real document inspection algorithms?

- **Commercially available document authentication systems**
  - Typically use more sophisticated metrics/checks
  - Currently used in manual checking to assist the inspection process
  - Counterfeiter MUST create a document that fools the human observer AND the document inspection system at the same time

- **Attacks on fully automated document inspection can be tuned to exploit weaknesses of a specific checking algorithm in use**
  - We demonstrated this problem on a modified UV page of a real passport:

  ![UV page of a real document. Similarity against ground-truth model: 87%](image1)
  ![Modified UV page. Similarity against ground-truth model: 94%](image2)
Advanced attacks on fully automated document inspection

- The border guard automatically and unwittingly checks if the document in his hand is actually a real document
- Document scanners imply this by checking the security features

- It is possible to create a device that simulates those security features but is not in fact a real document
  - Can simulate almost any security document
  - Production costs approximately 500€
Can electronic security fully substitute for optical security?

- Question: Should we create security documents that rely entirely on electronic security features?
- Public key cryptography used in electronic passports for signing (if done correctly) has not yet been broken
- Electronic passport security consists NOT ONLY of the public key cryptography
Possible angles for attack on electronic passport security

- Certificates have to be created, stored, managed → This is done by people
- Are the random number generators secure? Not always → OpenSSL (2008), Windows 2000, Windows XP
- Attacks targeted at gaining access to signing keys have happened before → recently Opera, Bit9
- Can the cryptographic hash algorithms be broken? Not yet but → MD5, SHA-0
- Can the scanner be compromised?
- Certificate distribution:
  - Compromised webserver?
  - Insecure connection (e.g., public internet)?
- Blackmail:
  - 105 ICAO member countries use ePassports
  - Each country must have several people with access to the signing keys
  - Only one is required to create an arbitrary number of passports
- Social engineering, etc.
Conclusions

- Optical document security in fully automated inspection needs an improvement
- Electronic document security is currently safe if we can assure that every step is 100% secure and no person, computer, connection, scanner, algorithm in all 105 participating countries can be compromised
- If electronic passport security is the only security feature and only one step can be compromised, there is no other line of defense left

Suggestions
- Consider electronic security features one (albeit very strong) security feature that supplements optical security features, but does not replace them
- Support OPEN research in the optical document checking
Questions?

- For detailed questions please contact the authors directly

**Michael Gschwandtner**  
michael.gschwandtner@ait.ac.at

**Svorad Štolc**  
svorad.stolc@ait.ac.at