International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/8
13/9/05
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Sixteenth Meeting

(Montreal, 26 to 28 September 2005)

Agenda Item 1: Development of specifications for MRTDs
Agenda Item 1.3: Report of the Document Content and Format Working Group
Agenda Item 2.2: Report of the New Technologies Working Group

INTEROPERABILITY OF STEGANOGRAPHY AND DIGITAL WATERMARKING

(Presented by the Document Content and Format Working Group in cooperation with the New Technologies Working Group)

1. INTRODUCTION

1.1 With the embedding of chips into passports, biometric data will provide additional support to help border officials in their work. The chip is only a support, and the printed and personalised security features on the data page are even more important and need to be sophisticated in order to avoid criminal damaging of the chip and then manipulating the visual data by conventional, or emerging forgery methods.

1.2 NTWG initiated research about steganography and digital watermarking in 2004. The key target was to find out if digital watermarking techniques are globally interoperable, so that they may consequently be recommended as a security feature by ICAO.

2. TERMS OF REFERENCE

2.1 The photo, being the main biometric identifier in current passports, is the major target for criminal attacks. Therefore it must be especially well protected. ICAO is looking for ways of protecting

the photo against manipulation by storing information in a digital watermark with the following being the crucial requirements:

a) the Information in the photo shall at least refer to the visual alphanumeric data, which will be an asset in addition to the data from the MRZ, the photo itself and the chip;

b) the Information must not be possible to reproduce by scanning and printing or colour copying;

c) the Information must be rendered illegible or a warning message must be displayed, if parts of the photo are manipulated or tampered with;

d) the Information must be protected in such a way that it cannot be extracted from the photo and inserted into another photo; and

e) the Information must be readable by interoperable software throughout the world which is not the property of a sole supplier.

2.2 Having surveyed the suppliers of watermarking technologies, it became obvious that each of the suppliers have developed their own string of software tools to reach their targets. Some use cryptographic mechanisms as a basis; others leave their implementation in the existing watermarking technology to the customer. Consequently, the degree of customisation for ID and passport applications vary between them, as well as the levels of user-friendliness.

3. KEY FINDINGS

3.1 Digital watermarks definitely add to the security of the document, but the implementation of the interoperability concept needs thorough planning. Since all the decoding software packages are proprietary systems (i.e. “Sole supplier” sourced) the most apposite application would seem to be national identity or travel documents for only a limited number of countries/regions.

3.2 However, interoperability as interpreted by ICAO stands for worldwide travel, of all nationals, from all countries, with any kind of passport. As ICAO promotes the facilitation of international travel, the sole supplier proprietary reading softwares do not lend themselves to this facilitation process. Thus, a solution to this interoperability problem is the key to a successful globally-accepted system.

3.3 The research paper mentioned in para. 1.2 above was issued in the Keesing’s Journal of Documents & Identity, issue 10, as agreed by TAG/MRTD-15.

3.4 At the end of 2004 the non-interoperable reading platforms were a major deterrent to continued investigation by ICAO into wider use of this technology. However as a result of last year’s research by the NTWG, the two market leaders Digimarc and Jura Group have recently announced a cooperative effort to produce and make available by the end of this year a single reading platform that can read both the IDMarc digital watermark from Digimarc as well as the Digital IPI digital watermark from Jura Group. It has also been indicated that this platform could be expanded to include other digital watermark variations from other companies.

3.5 Since digital watermarks add highly to the security of the data page and is a key security feature to protect the photo against manipulation, digital watermarking must not be neglected in any considerations for future recommendations concerning ID and passport documents.

4. ACTION BY THE TAG/MRTD

4.1 The TAG/MRTD is invited to:

a) support the continued market survey about technical cooperation between different suppliers with the target to decide, depending on the outcome, the eventual recommendation of steganographic techniques as globally interoperable security feature, if the interoperability can be technically guaranteed.

— END —