The profiling of false identity documents: a promising method to fight identity fraud

S. Baechler[1´2], E. Fivaz[2], O. Ribaux[1], P. Margot[1] – [1]Institut de Police Scientifique, University of Lausanne, Switzerland / [2]Police Neuchâteloise, Switzerland

1. Context and objective :

- **False identity documents** represent an important means used by **organized crime**
- **Forensic intelligence** can help distinguish organized from anecdotic frauds
- A general method for **profiling** false identity documents with the aim of **discovering existing links** based on **visual forensic characteristics** is presented

2. Postulates and hypotheses :

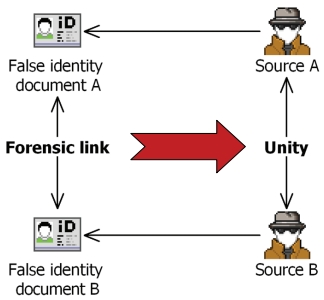
I. A false identity document is regarded as the **trace** left by the forger

II. Its material characteristics constitute **the forger's « signature »** and depend on :

- A particular technique
- A specific equipment
- Personal choices of production

➔ **profile**

III. Link inference : if documents share a **common profile** ➔ they come from a **common source** (forger or workshop)



3. Forensic profile :

Made of 20 **visual forensic characteristics** such as :

Printing techniques, reaction under UV light, typefaces codification, ways of imitating security features, alterations, etc.

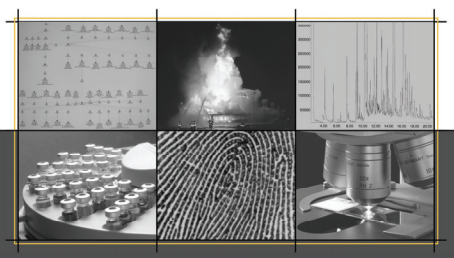
4. Materials and methods :

More than 220 false identity documents collected from 9 Swiss police departments **of three representative kinds** were analyzed :

- Stolen blank French passports
- Counterfeit Iraqi driver's licenses
- Falsified Bulgarian driver's licenses

The methodology was as follows :

1. **Description** of their characteristics in an *ad hoc* database
2. **Automatic** and **systematic detection of links** by the database
3. **Analysis** of links and **production of intelligence**



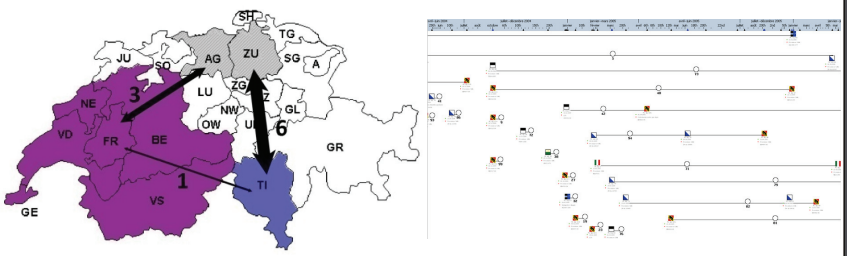
5. Computer database (*ProfID*) :

- Integrates **forensic** characteristics and **circumstantial** data
- Detects links **automatically** and **systematically**
- Provides **statistics** on false documents' **« security » features**

6. Results :

6.1 Strategic intelligence :

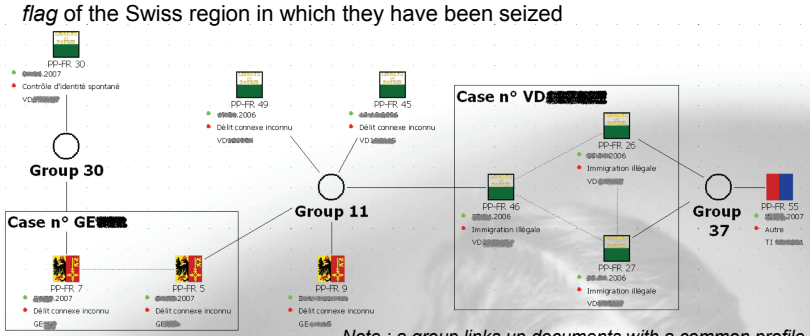
- Links are detected for **30% to 60%** of the documents ➔ proof of a **structured form of crime** and not an accumulation of isolated cases
- A **restricted number of forgers** is responsible for these considerable parts of the market ➔ **priority targets** identified through forensic intelligence
- Geographical and chronological analysis : groups of linked documents are **interregional** (>50% are trans-jurisdictional) and **long-lasting** (avg. 1.5 to 2 years)



Examples : Links for falsified Bulgarian driver's licenses between different parts of Switzerland (left) – Links for counterfeit Iraqi driver's licenses represented in time (right)

6.2 Tactical intelligence :

Forensic links point out potential **criminal interactions** or **undetected networks** and suggest **fusing inquiry teams** working on different cases *(boxes)*. In the example below, false identity documents are represented by the *flag* of the Swiss region in which they have been seized



Note : a group links up documents with a common profile

7. Conclusion :

Profiling based on **visual forensic characteristics** :

- Is **efficient** and **cost-effective** : requires minimum equipment, time and training
- Produces **relevant strategic** and **tactical intelligence**
- Provides **objective knowledge** on a little studied form of crime

➔ Suggests **targeted** and therefore more efficient **actions** to fight fraud :

- *Preventive* : training, identity document designers consulting, alerts, …
- *Repressive* : objective dispatch of resources, new leads in criminal and terrorism investigations, tracing back the networks up to the forgers, …

Contact and questions **: Simon.Baechler@unil.ch**

ESC école des sciences criminelles

UNIL | Université de Lausanne

Ecole des Sciences Criminelles, Batochime, 1015 Lausanne - info.esc@unil.ch - www.unil.ch/esc

16th International Forensic Science Symposium, October 2010, Lyon