



COVECTRA
Multi-Layered Brand Protection

StellaGuard™ Security Label

CONVERGING SMART TECHNOLOGIES
TO PROVIDE UNIVERSAL BRAND PROTECTION

Viewpoint: Anti-counterfeit features – should public be aware?

Petr Hampl and Libor Sustr, *23-Feb-2018*



There have recently been several crimes committed by criminals impersonating policemen in the Czech Republic. In one particularly serious case a young woman was kidnapped by a group of men with fake police badges, while others have involved the theft of money and products. Just recently, a crime ring of fake environmental inspectors was convicted.

The Czech Republic is no exceptional country in this respect, as can be seen from news reports in other countries. In Cheltenham, UK, a man impersonating a policeman stole £6,000 pounds from an old lady, while in the US state of Texas another fake policeman has committed series of burglaries. And there is an uncountable number of such cases in third world countries.

Fake policemen often do not wear uniforms, which makes sense because walking in uniform may be risky and the criminal can always claim to be undercover. However, the use of fake credentials – something that reportedly can be acquired easily from online retail platforms – means it can be easy to dupe unsuspecting victims.



police have published only the very basic information and some protective elements. Other national police do not communicate even such elementary information.

When a victim hears “come with me now,” he/she has no chance to be sure whether the other person is a real policeman or a fake policeman.

At Optaglio, we have had several discussions with law enforcement experts from different European countries in recent months, and time and again we meet the same argument: if anti-counterfeit features were published, it would help attackers because they could concentrate on these features. It is better to release nothing and invest more time and efforts into hunting for fake producers and abusers.

The same question can be asked more broadly – from driving licences through alcohol to drugs and luxury brands. Should be the protection features made public? If the answer says halfway, what does this exactly mean?

It is no surprise that there are different answers for different situations. The following factors need to be taken into account.

- Who will inspect the ID card/ document /item;
- What protective elements can be afforded, which is dependent on the value of the protected item?;
- Is there a chance that the information stays confidential? There is little chance to keep it secret if thousands of people are involved, but we should understand that number of inspectors is more important than the number of users.

People

Motivation is the critical factor also in this area. Are users motivated to check authenticity? Police ID cards are a simple case. Nobody wants to be seized by a faked policemen. However, some studies show that significant proportion of customers buy counterfeited luxury brands intentionally. If they don't care, of course, it makes no sense to publish features.

The capabilities of users are also relevant. Only such information should be published that will be utilised by users during their inspection of ID cards /brands /other items. Moreover, too many protection elements lead to user confusion instead of security enhancement. It is usually recommended that ID cards should include not more than three distinctive elements, but ID cards are mostly inspected by law enforcement staff with at least a basic level training. For inspection by untrained users, one element is sufficient, but this element must be distinctive and easy to recognise.

For holograms, it means that, e.g. visual effect of switching between letters and digits or switching between black and grey is almost useless. Such element could be replaced with another one without user noticing. In fact, if you want something that really works, you might choose more complex holograms with objects such as statesmen portraits that redden with hologram tilting or an animated animal. It is useful to publish such elements in these cases because people will understand and will be able to identify them. Luxury brands can even embody such holograms into an overall design.

Adding other elements that are known only to experts is not excluded.



the feature cannot be imitated at all, it is pretty secure to release all details. It can even contribute to deterring of attackers, which is often the case for the banknotes. On the other hand, publishing elements that are not very strong creates too high risks.

We never recommend publishing details of simple protection elements such as watermarks or out-of-date holograms. It is really an instruction for counterfeiters. On the other hand, it may be useful to publish details of advanced holograms created on high-resolution lithographs using sophisticated mathematic algorithms that cannot be derived from ready holograms. Such holograms often include a specific change of colours, move of illusion objects in unexpected directions, special 3D effects etc. It is critical to design the hologram so that principal visual object is based on these unique features.

Does it make any sense to add cheap protection elements that can be imitated? Any protection should meet three requirements:

- Recognisability;
- Non-imitability; and
- Self-destructiveness, which should guarantee that any attempt for removal of an element results in its destruction.

Does this mean that only first-class elements should be applied? It is a matter of proportionality. It is not reasonable to protect tickets for local cinema with high-resolution holograms. The business case would not work. On the other hand, even minimal protection barrier can be relevant so that an application of a cheap dot matrix hologram can be the solution for this local cinema. The same principle should be applied to the publishing of information about features.

So, to publish or not to publish? Security based on transparency is stronger than security based on secrecy, but you need to be sure that your technology is resistant against imitation and that users are motivated and skilled. It is the reason why central banks can publish almost everything about their banknotes. Moreover, lack of information creates suspicion that protection is not very strong. We are afraid it is the case for most of the police badges and ID cards.

Petr Hampl and Libor Sustr are consultants from Czech hologram company Optaglio.

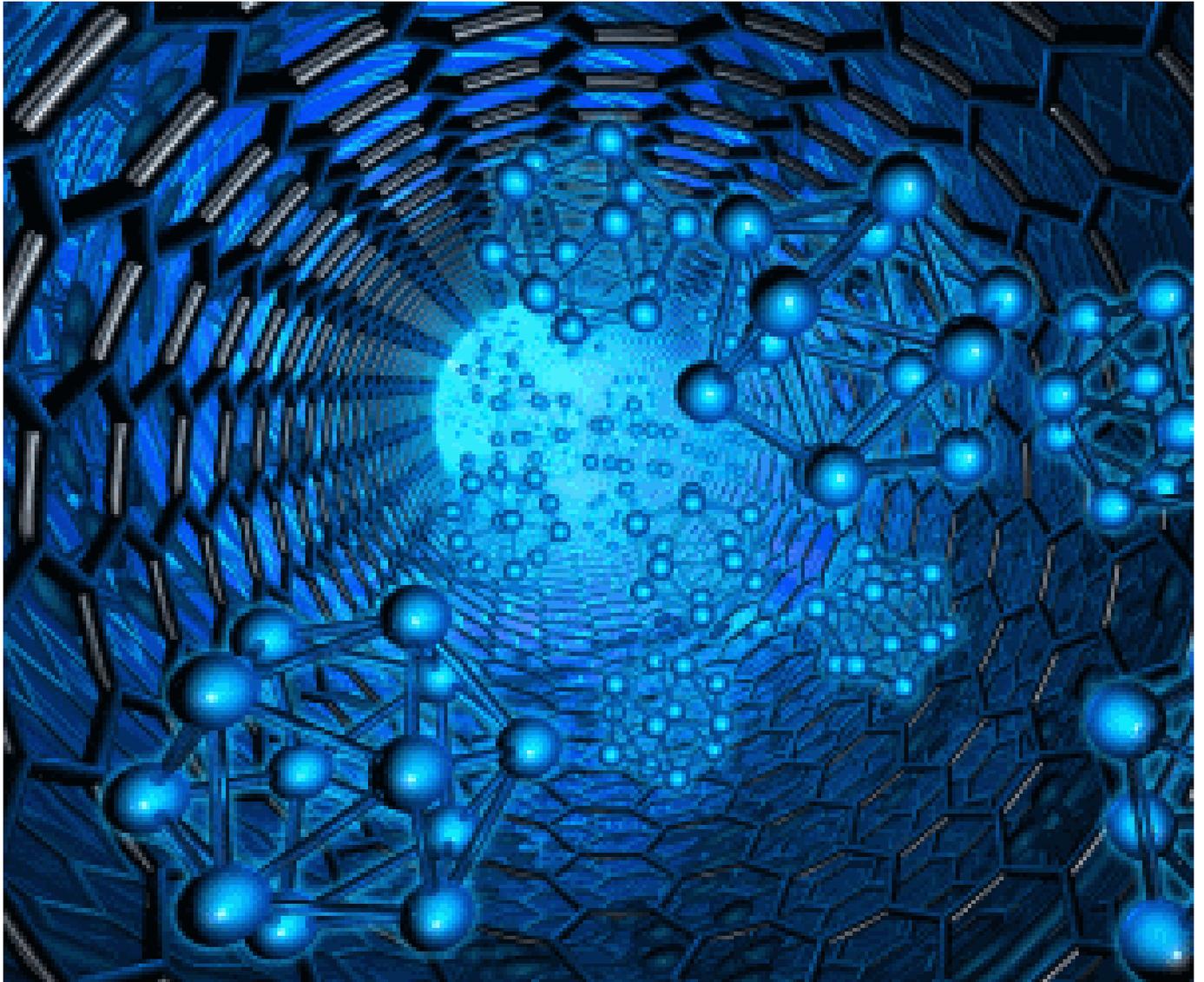
Related articles:

- [Fake FBI badges sold on Amazon](#)
- [US searches for CIA, FBI badge counterfeiter](#)
- [FDA warns again of extortion by bogus special agents](#)
- [FDA warns of bogus agents duping public](#)

Want our news sent directly to your inbox?



© 2018 SecuringIndustry.com



FREE Papers

Events

[Macallan Whisky picks Izon® Technology as part of a comprehensive anti-counterfeit solution \(De La Rue Authentication Solutions\)](#)

The Edrington Group, makers of world renowned The Macallan Highland Single Malt Scotch Whisky, faced a challenge when re-filled used bottles, intact with labels, began appearing on shelves under their brand name. This posed a serious consumer safety, as well as a global brand issue. For a solution, they turned to Authentication Solutions for the key overt component of a comprehensive solution.

[Epson builds market awareness of authentic product through implementation of layered AC tech \(De La Rue Authentication Solutions\)](#)



[Home](#) | [About us](#) | [Contact us](#) | [Advertise](#) | [Links](#) | [Partners](#) | [Privacy Policy](#) | | [RSS feed](#)  | [back to top](#)

© SecuringIndustry.com 2018