Optic-id.com

Hologram authentication
The good practices

A hologram is a security device that one must be able to authenticate if it is to protect a product or document against counterfeiting. Otherwise, it is only decorative.

Several providers indicate that they authenticate holograms, but their methods are not effective, and put users at risk of identity theft or acquisition of counterfeit products, and all those who offer such authentication services of significant legal risks.

We therefore thought it useful to list these ineffective and dangerous methods on the one hand, and then to examine those which can allow quality authentication.

I. The ineffective and dangerous methods

A. Acquisition of a single image of the security device

This does not allow any verification of the device, which may be a photographic copy. If it is an identity document, the fraudster may have replaced the photograph of the holder with his own and have also modified other elements.

B. Acquiring a video of the security device in ambient light

1. Make a first photographic acquisition of the device,
2. and make a second one, from a different point of view or in a different light, to check that the appearance has changed.

This does not allow any verification of the security device, because the original hologram may have been replaced by another.

II. An acceptable method in certain cases

1. Make a first photographic acquisition of the device,
2. compare this acquisition with a reference corresponding to the same or a similar point of view,
3. and make a second one, from a different point of view or in a different light, to check that the appearance has changed.

This cannot be considered a valid authentication, as the hologram may have been replaced by a glossy varnish that will reflect any light source in the vicinity, or by an imperfect copy of the original hologram, which is within the reach of many counterfeiters.

Anyway, capturing images of a hologram without first measuring the position of the light sources is meaningless, since each light source causes different reflections from the hologram depending on its position.

Therefore, this method is only suitable for security devices that are not sensitive to ambient light, such as color-changing inks, and only works with holograms if flash is the primary source of illumination and ambient light is very dim.

III. The good practices

A. The "MINIMUM" authentication method

1. Make a first "double photographic acquisition" of the security device, from the same point of view, eliminating the effect of ambient light (this is done by calculating a so-called "differential" image, which is the subtraction of an acquisition made in ambient light from an image taken in the same ambient lighting, but with the illumination of the flash in addition),
2. compare this acquisition with a reference corresponding to the same or a similar point of view,
3. and make another photographic acquisition, from a different point of view, to verify that the appearance has changed.

B. The "STRONG" authentication method

In addition to the operations defined in the "minimum" method, use the same "double photographic acquisition" method for each of the two successive points of view.

C. The "USER-FRIENDLY" authentication method

To take the lead in the market, it is necessary to improve the "strong" method by not forcing the user to place his smartphone at a particular point of view, which requires:

1. the prior registration of a plurality of original descriptions of the authentication device corresponding to different points of view from each other, constituting a wide field of visibility and analysis (or the calculation of these aspects, which amounts to the same),
2. and the comparison of each acquisition with an original description corresponding to one or several neighboring points of view.

D. The "VERY STRONG" authentication method

To achieve an even higher level of authentication, the "strong" method can be improved by preventing a fraudster from replaying a previously recorded scenario (man in the middle, or Trojan horse in a smartphone) by asking him to make one or more successive acquisitions from one or more points of view that cannot be foreseen.

This method is essential for voting, for making financial transactions or for signing important contracts.

IMPORTANT: The use of artificial intelligence does not change anything, since it amounts to comparing not with a reference image, but with a set of reference images having been used to train the artificial intelligence.

3 mai 2023
Franck Guigan
f.guigan@optic-id.com
+33 6 14 63 93 36

Latest publications

- The essential evolution of identification procedures
- What future for identity businesses?

En français:

- L'évolution indispensable des procédures d'identification
- Quel avenir pour les métiers de l'identité ?
- Authentification des hologrammes - les bonnes pratiques