Securing ID credentials

Selecting the right secondary portrait

IN GROUPE

Creating fraud-resistant ID documents using innovative security features

Identity documents play a crucial role in today's connected world. They enable citizens to prove who they are, in person or online, and to securely access essential services. Yet, over the past decades, document fraud has evolved at an alarming pace, driven by the growing availability of advanced printing tools, image editing software, and, more recently, artificial intelligence.

Today, AI-powered technologies make it easier than ever to manipulate portraits, generate synthetic faces, or alter existing photos with near-perfect realism. This surge in sophistication has turned the portrait into the most targeted feature of identity documents, as fraudsters focus on the element that most directly connects the document to its rightful holder. Whether the attack involves replacing the portrait, overlaying a new image, or exploiting resemblance between individuals, the goal remains the same: to deceive verification systems and human inspectors alike.

The portrait is the essential bridge between the document and its owner, and when compromised, the entire trust chain collapses. To ensure reliable authentication, the portrait must remain clear, genuine, and tamper-proof, while being easily readable both by the human eye and by inspection systems. Strengthening its protection is therefore essential.

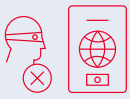
One of the most effective ways to achieve this is through secondary portraits, additional, embedded portraits that act as a visual checkpoint, confirming that the primary portrait is authentic and unchanged. Ultimately, an identity document must strike the right balance: highly secure and difficult to reproduce, yet simple to verify.

Five different types of fraud

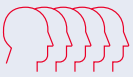
Counterfeit
The complete fake reproduction of a genuine document made with non-genuine materials or using parts of genuine documents.

Stolen blank documents
Genuine blank documents that have been stolen in order to personalize them with false information.

Forgery
Falsification of personalized or affixed data on an ID document for example using morphing or photo replacement.



Impostor
Use of a genuine document that does not belong to the holder, because the fraudster resembles the legitimate document bearer.



FOG
Fraudulently Obtained but Genuine document with false data and/or morphed portrait.

When Physical Meets Digital: Protecting Identities in Both Worlds

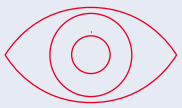
Fraud is constantly adapting. While counterfeit or altered ID documents remain a threat, the rise of digital services has opened new opportunities for identity misuse. From online banking and eGovernment services to remote onboarding, more and more interactions rely on digital identity verification—making trusted ID documents the first line of defense.

The challenge is clear: it's harder to verify someone online than face-to-face. Fraudsters exploit this gap by using fake or stolen IDs to access benefits, open accounts, or impersonate others across borders. As digital transactions become routine, the line between the physical and digital worlds has blurred, and both must now be protected with equal rigor.

This is where the secondary portrait plays a decisive role. By embedding a secure, tamper-evident duplicate of the holder's image directly into the document, it provides an additional layer of visual and digital trust. It helps confirm that the main portrait, and therefore the identity, is genuine, whether the document is checked in person or through a digital capture.

Three levels of inspection

To combat the five types of fraud, the security industry advocates a three layered approach for ID documents:



1. Manual inspection
To make inspection a straightforward process, a large number of security features are visible to the naked eye—feel, look and tilt is the motto. You can try it yourself!

2. Inspection with basic tools
Inspection is conducted with basic tools such as a UV lamp to see fluorescent elements, or a magnifying glass to see microelements.

3. Forensic analysis
At this stage, state-of-the-art equipment and forensic experts are required to analyze the document in depth.

IN Groupe is committed to creating ID documents that are hard to reproduce, yet easy to inspect.

A truly robust security concept to create fraud resistant ID documents

Aspects to be considered are:

- **Document authentication** needs to be unambiguous using the detailed portrait
- **Examination conditions** such as the type of lighting (daylight, artificial light or backlight), and the time available for document authentication
- **The level of knowledge necessary** for the person inspecting the document (trained professionals or untrained civilians)
- **Types of equipment needed** to inspect the document
- Possibility of authenticating the document using **Optical Machine Authentication** (OMA)

IN Groupe's security concept consists of three main pillars:

1. Portrait Protection
2. Data Interlinking
3. Optical Machine Authentication

Secondary portraits: Protecting the main portrait and adding an extra layer of security

Secondary portraits play a critical role in modern identity documents. Their primary function is to protect the main portrait—the element most frequently targeted by fraud attempts. By adding a second, independent representation of the document holder, they make it significantly harder to alter or replace the primary portrait without leaving visible traces. Secondary portraits also help create a more reliable link between the document and its rightful holder, supporting secure verification both in person and in digital processes.

Using different personalization technologies for the primary and secondary portraits is especially effective. Any attempt to manipulate one portrait would require replicating multiple, highly specialized techniques, greatly increasing the difficulty of tampering. For this reason, the secondary portrait has become a central layer of modern document security.

Advanced secondary portraits integrated with high-security features

Color portrait on a DOVID with LASINK™ Helios technology

LASINK™ Helios enhances document security by combining laser-engraved color personalization with a Diffractive Optical Variable Image Device (DOVID). DOVIDs are well-established security features known for their dynamic optical effects, which naturally attract attention during inspection. With LASINK™ Helios, the secondary portrait appears polychromatic when viewed at specific angles, while displaying various monochromatic representations when the angle changes.

This approach provides a clear visual link to the main portrait and makes fraud extremely challenging, as it merges optical variability with high-precision personalization. The color portrait is instantly recognizable and offers both intuitive human inspection and strong support for automated verification.

By merging high-resolution laser color engraving with optical variability, LASINK™ Helios protects the main portrait through unmistakable visual authenticity.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Color portrait in a transparent window creating a relief and depth effect with LASINK™ 3D technology

LASINK™ 3D leverages LASINK™ color laser engraving—a technology that produces secure, high-quality portraits using a cyan-magenta-yellow matrix engraved with perfect registration. Its distinctive linear pattern is immediately recognizable and extremely difficult to forge.

When combined with an SLI® lens structure in a transparent window, the secondary portrait produces a 3D relief effect when light shines through the document. This effect draws the verifier's attention naturally and makes it easy to compare the secondary portrait with the primary one or with the person presenting the document.

Because the technique requires both mastery of polycarbonate laser-engraving and precise engineering of window and lens structures, this type of secondary portrait creates a very high barrier to counterfeiting.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Other secondary portrait techniques on the market

Several other technologies are used globally to create secondary portraits. While they contribute to document security, they generally offer more limited resistance to sophisticated attacks.

Secondary portrait using a special ink

Some solutions rely on laser engraving beneath the document surface combined with a special ink that produces a gold appearance. When viewed in transmitted light, the portrait disappears and reveals a pre-printed symbol visible from both sides of the document. Although visually interesting, this method typically produces portraits with limited detail, reducing its authentication efficiency.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Secondary portrait engraved over an OVI® pattern

Another approach consists of engraving a ghost image over an Optical Variable Ink (OVI®) pattern. The color-shifting effect of OVI increases security, but the portrait must fit within the restricted shape of the printed pattern, resulting in low-resolution and low-sized portraits that are harder to compare reliably.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Secondary portrait within a transparent window using a specific material

Some documents feature a transparent window filled with a laser-engravable optical material. When examined under different light sources, the material changes color. While this provides useful optical variability, the complexity of portrait reproduction remains lower than in multi-layer laser engraving systems.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Secondary portrait using the same printing process as the main one, using encoded data

These solutions use the same printing technology as the primary portrait and embed invisible encoded information within the image. The information becomes visible only with a decoding lens. Although this adds a verification layer, the reliance on a single personalization method makes the feature less resilient to advanced alteration techniques.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Secondary portrait using a metallic optically variable window

Some solutions produce a secondary portrait inside a transparent window made from a metallic, optically variable material. It can shift from one color to another, for instance from golden to green, depending on the viewing angle; under transmitted light, the portrait becomes almost transparent. While the effect is visually striking, the achievable portrait detail is limited, offering less support for reliable face comparison.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Secondary portrait in a window combined with a decoder lens and hidden data

Another method combines a window-based secondary portrait with hidden information embedded directly into the image. The encoded elements become visible when viewed through a dedicated decoder lens, creating simple animated effects. Although this adds an additional verification layer, the resulting portrait typically offers lower resolution than multi-technology laser-based solutions.

Level 1
Level 2
Hard to Reproduce
Easy to inspect

Feature	Security	Level	Hard to reproduce	Easy to inspect
Color portrait on a DOVID with LASINK™ Helios technology	High	1 & 2	✓	✓
Color portrait in a transparent window with LASINK™ 3D technology	High	1 & 2	✓	✓
Secondary portrait using a special ink	Low	1	✓	–
Secondary portrait engraved over an OVI® pattern	Low	1	✓	–
Secondary portrait within a transparent window using a specific material	Medium	1 & 2	✓	✓
Secondary portrait using the same printing process as the main one, using encoded data	Low	2	–	✓
Secondary portrait using a metallic optically variable window	Medium	1	✓	✓
Secondary portrait in a window combined with a decoder lens and hidden data	Medium	2	–	✓

Key takeaways

Fraudsters are increasingly using sophisticated digital tools and artificial intelligence to manipulate images, reproduce patterns, and generate highly convincing counterfeit identity documents. In this evolving threat landscape, identity credentials must be designed to resist both physical and digital attacks, offering features that are technically complex to replicate yet simple to verify.

Secondary portraits play a critical role in this defense. By creating a second, independent representation of the holder, they reinforce the primary portrait, adding a robust layer of security that is difficult to alter or reproduce. When combined with multiple high-security personalization techniques, optical effects, and verifiable patterns, secondary portraits create a multi-layered protection system that strengthens the integrity of the entire credential.

Such robust features ensure that identity documents remain trustworthy, reliable, and resilient, enabling both trained professionals and untrained civilians to authenticate credentials quickly and confidently, whether in face-to-face situations or online.

In an age of rapidly evolving fraud, organizations must work with partners who combine experience and foresight to deliver identity solutions that are robust, reliable, and ready for the challenges of tomorrow.

Securing ID credentials

ingroupe.com

IN GROUPE