



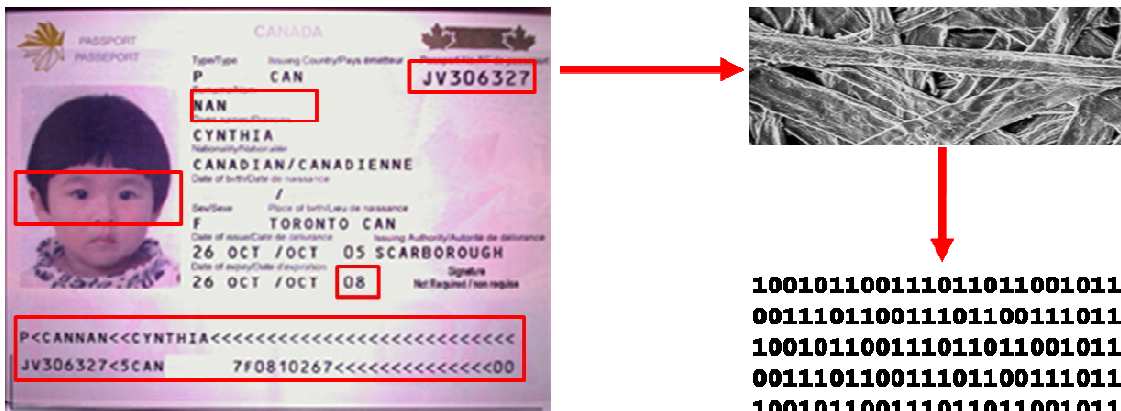
Rogue DNA Forensic Lab Document Authentication

Rogue DNA’s Forensic Lab suite (RFL) provides the following functions. Data can be seamlessly exchanged between each module:

- Face recognition & partial face recognition
- Fingerprint recognition and compliance with biometric standards
- Fingerprint & facial images – conversion of paper prints to electronic
- Biometric Application Server
- Document authentication

DNA is the ultimate means of identifying human beings. Similarly, Rogue DNA’s RDNA technology absolutely identifies a passport, bank note, cheque, ID card, and security materials. from their unique characteristics.

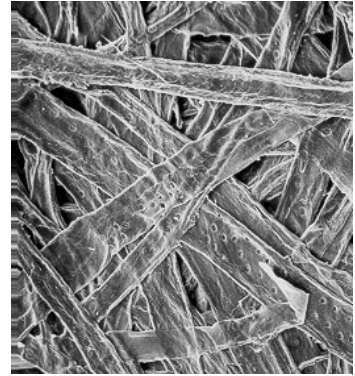
RDNA identifies the underlying characteristics of the document itself – the picture below shows the totally random fibre structure of a secure document such as a passport or banknote. If the pattern from any section or area is recorded when the document is produced, at any time in the future the same area can be rescanned and compared with the original. The process to do this involves processing light reflectances at multiple frequencies - Rogue DNA has five patents pending regarding this technology. Because nothing is added to the document, a counterfeiter has no means of knowing the locations of the areas being scanned, and because the fibre pattern is created when the security paper is produced, it cannot in any case be replicated.



The preselected areas are shown in red (although the document itself isn’t actually marked). Reflectances from the underlying fibre patterns of each section, plus any additional layers such as writing or special characteristics, are registered, encoded, converted to an encrypted digital string, and saved either in a database, on the chip, or printed in any selected format on the document

Rogue DNA's RDNA technology is a total solution combining hardware and software which scans, interprets, and matches the information retrieved. The core platform uses highly innovative optical/electronic technology to identify the three-dimensional composition of predefined areas of a document.

The technology can be used in two different ways. Firstly, if a credential such as passport or visa is registered when it's originally issued, at any time in the future it can be rescanned and the reflectances used to generate another DNA string. Comparing this with the original will determine whether the document is the unmodified original or not. For example, if selected areas on the passport details page are registered when a passport is issued to an individual, then when they subsequently present it on return to their home country it can be matched against the registration for this passport number in the database. Combining this with human biometrics such as face or finger recognition provides the strongest possible confirmation that an individual is who they claim to be, and that the identity document presented is the unmodified original. This offers the strongest possible closed loop protection.



The underlying fibre structure of a security document

Secondly, the RDNA process can determine whether the characteristics of a document are consistent with the generic characteristics of this type of document. For example, while the example above will compare the characteristics of the individual's passport against the original record, in the case of foreign passports this cannot be done. However each type of national passport has its own set of common characteristics, and these can be compared to determine if the passport being presented is consistent with them.

In summary, the Rogue RDNA process:

- Uses reflected light at multiple frequencies to confirm that any secure document is the original and not a counterfeit.
- It does this by scanning and identifying the unique characteristics (such as internal fibre patterns) of predefined areas of the actual piece of material of any document. These are stored as a digital string, or DNA, either in a database together with the Document ID, printed on the document (for example as a 2-D barcode), or stored in an RFID chip.
- At any time in the future the document can be rescanned and the resulting DNA compared with the original. Because any counterfeit will be on a different piece of material, it will have a different DNA and can always be identified.
- If the ink pattern on the paper is tampered with, e.g. the value or expiry date, this too will change the DNA of the document and generate a different DNA string.