Global trends for document security

Identity is an integral part of the Human subsystem. All livings being struggle for their unique identity in the universe- It may be in the form of knowledge, Power or Wealth. In ordinary language, one can use the word "identity" to refer to characteristics or attributes that cannot naturally be expressed in terms of a social category. However, realizing its importance, worldwide all governments keep their Citizen in easy and quick access identity formats.

But today, Identity counterfeiting is a growing global menace that has turned our identities into highly valuable assets. The potential risks associated with fake identification documents can be high. With a fake identity, an individual can potentially gain illegitimate access, qualify for government benefits, defraud credit companies or make illegal purchases. Even though today's card printing technology delivers superior image quality and exceptional card durability at a surprisingly affordable cost, but with forgery and counterfeiting now a serious issue, what defense mechanism are solution providers putting in place to protect the end users?

This article outlines how to reduce the risk of counterfeiting with latest document security trends, paying particular attention to a system combining the most effective features.

Identity Cards:

ID Cards were introduced during the First World War as part of a statutory registration scheme. It ended in 1919. They were introduced in 1939 and remained in force for several years after the war until they were abolished by Churchill in 1952. Today, around a hundred countries have official, compulsory, national IDs that are used for variety of purposes.

In India, the recent national Unique Identification (UID) project launched by the Government of India, with the iconic technocrat, Mr. Nandan Nilekani at its helm is indeed a significant project. With this, India has embarked on an ambitious e-governance project which targets to provide a unique number to each citizen.

Authentication

In this era of heightened security concerns, we are keenly aware of the role that ID Documents, or credentials, play in our lives. **Whether a driver's license, passport, social security number, Unique Identity number, etc. these documents are used routinely not only to verify a person's identity but can also be used to protect rights to privacy, wealth and security.**

Today, governments worldwide are using e-Governance methods and realizing that national security has profound effects on the economy and our way of life. To optimize these issues, a diversity of security features is available. A brief overview of the most widely used features is given below.

Commonly used security features

Most people would agree that secure identification begins with a photo ID card, the most representative of which is the driver's license. While a good photo likeness and a legible signature remain the key features of a photo ID card, those features alone are inadequate today. **Issuing authorities now incorporate several additional features to deter counterfeiting, while at the same time making authentication easier and more reliable.**

The identity of a physical object is uniquely determined by a set of distinctive properties. Most ID cards are fabricated today by direct printing on composite CR-80 cards comprising layers of cross-oriented polyester with outer layers of PVC. Once printed, a tough 0.001" (1 mil) thick polyester laminate is typically applied to protect both sides of the card.

After the process, **companies used a variety of integrated security features, which can be classified mainly into three categories visible, invisible and forensic.** Finally, there are machine-readable magnetic stripes, bar codes and programmable devices (smart cards) that can provide even more security, plus the means for automatic data checking and database connectivity.

Level 1 (Overt features)

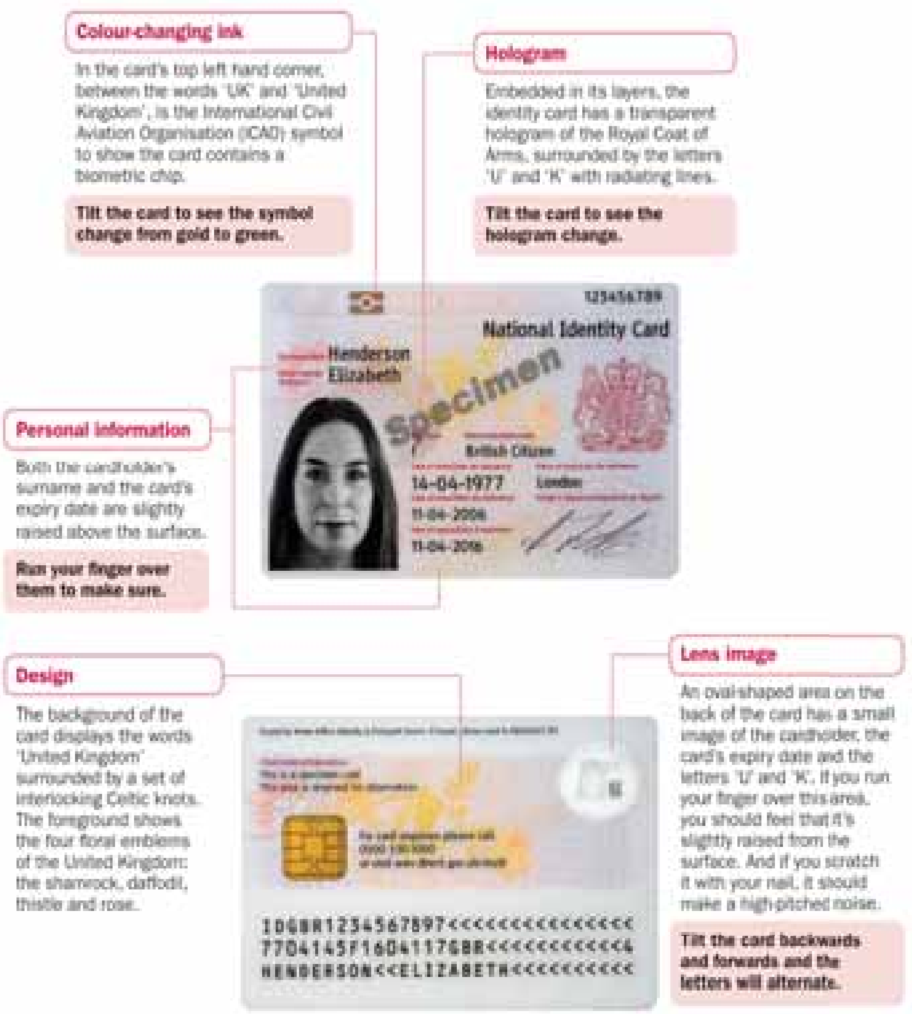
These are "first line" validation features, i.e. they can be seen without the use of equipment or special devices. The most frequently encountered Level 1 device is a High Refractive Index (HRI) hologram printed on either the card or, more commonly for drivers' licenses, on the underside of the protective laminate. Recently developed de-metallization and photo polymer holographic techniques now offer enhanced depth, transparency, and fine line detail which most would acknowledge being practically counterfeit-proof.

Level 2 (Covert features)

Level 2 features are verifiable by simple, inexpensive tests such as visual inspection under a lens or black light (UV), biometric scanning, digital scanning and data base checking. Examples of Level 2 features include: specialized bar codes, micro-printing, and covert background printing that is incorporated in the card design.

Level 3 (Forensic features)

The majority of these must be kept secret to remain useful. Analysis of a card having Level 3 features is essentially a post-mortem process, often requiring some dismembering of the card to determine its origin, and to minutely inspect the features for validity. Level 3 devices are images or physical objects that are hidden within the card structure or concealed by special graphic effects on the card surface. Typically, they can be fully validated only by specialized optical scanning devices, or other means of machine-reading data.



Colour-changing ink

In the card's top left hand corner, between the words 'UK' and 'United Kingdom', is the International Civil Aviation Organisation (ICAO) symbol to show the card contains a biometric chip.

Tilt the card to see the symbol change from gold to green.

Hologram

Embedded in its layers, the identity card has a transparent hologram of the Royal Coat of Arms, surrounded by the letters 'U' and 'K' with radiating lines.

Tilt the card to see the hologram change.

Personal information

Both the cardholder's surname and the card's expiry date are slightly raised above the surface.

Run your finger over them to make sure.

Design

The background of the card displays the words 'United Kingdom' surrounded by a set of interlocking Celtic knots. The foreground shows the four floral emblems of the United Kingdom: the shamrock, daffodil, thistle and rose.

Lens image

An oval-shaped area on the back of the card has a small image of the cardholder, the card's expiry date and the letters 'U' and 'K'. If you run your finger over this area, you should feel that it's slightly raised from the surface. And if you scratch it with your nail, it should make a high-pitched noise.

Tilt the card backwards and forwards and the letters will alternate.

Figure 1: Security features in currently release UK National ID Card

SOLUTIONS TO IMPROVE SECURITY OF ID'S- ADDING EXTRA SECURITY

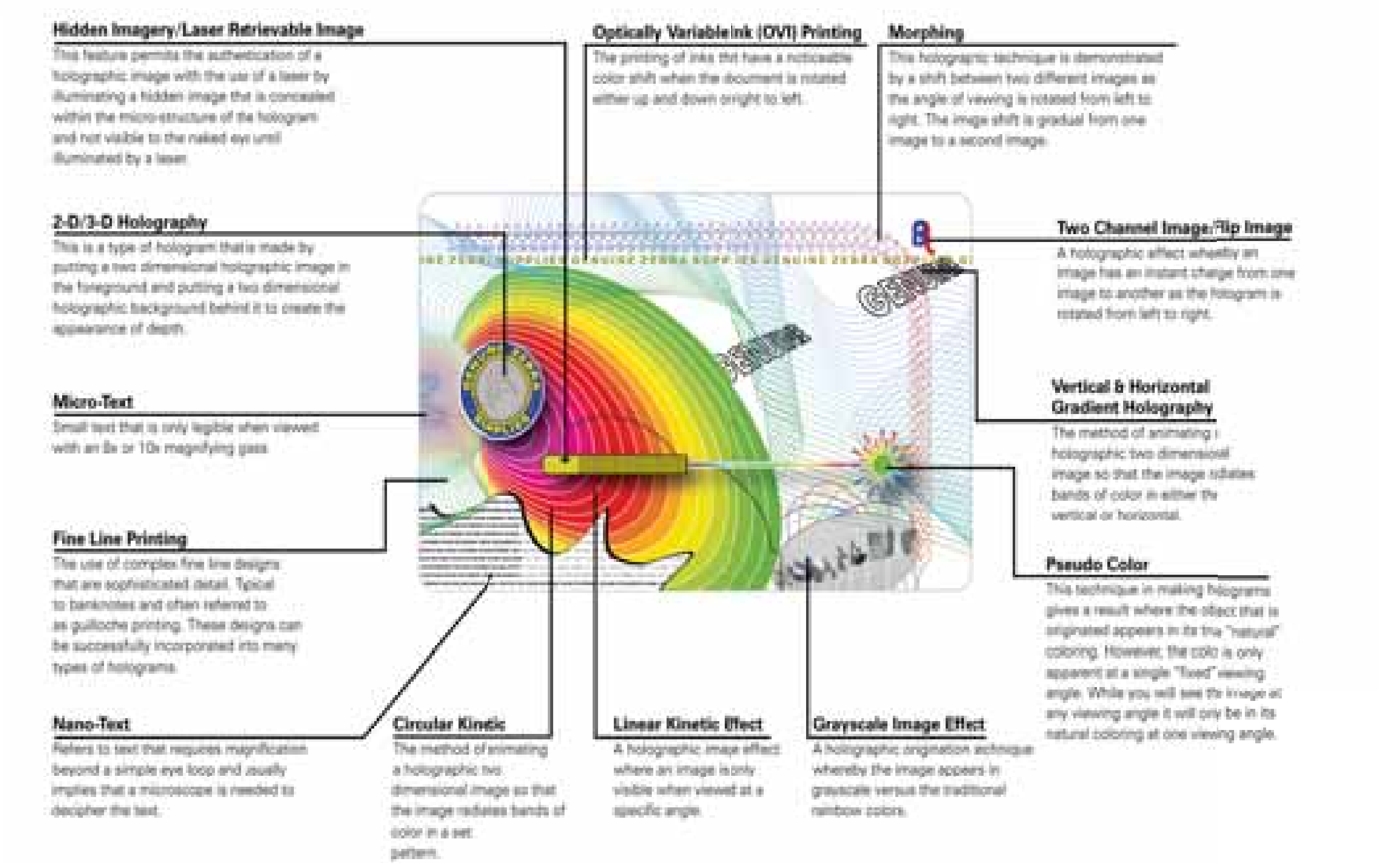
ID card security comes from a combination of features inherent to the card media (like overt, covert and forensic), together with variable features printed at the time of issuance. To add security, growing use is made of security features with integrated personal data.

a) UV-Ink Personalization

One example is on-demand UV ink personalization, which allows cardholder's photograph or personal data to be printed in high-resolution gradient UV ink. Pre-printed features are very difficult to duplicate. User defined text, with deliberate random font changes and misspelling if desired, may be micro-printed as an added security features. Character height of the micro-printing is five thousand of an inch. Other printed security choices include Guilloche patterns, serial numbering and micro-graphics.

b) Holographic Laminate

Since their use in 1989, holograms were historically hard to copy; they were used to provide cloning resistance to products. Holographic laminate may be used to extend the useful life of a card while simultaneously protecting it against data manipulation. To combat document tampering and counterfeiting, the holographic industry is developing and implementing new security features such as nano-text and images (very small text and graphics including entire city maps) created using special diffractive techniques. Other enhanced diffractive methods also exist.



Hidden Imagery/Laser Retrievable Image

This feature permits the authentication of a holographic image with the use of a laser by illuminating a hidden image that is concealed within the micro-structure of the hologram and not visible to the naked eye until illuminated by a laser.

Optically Variableink (OVI) Printing

The printing of inks tht have a noticeable color shift when the document is rotated either up and down orright to left.

Morphing

This holographic technique is demonstrated by a shift between two different images as the angle of viewing is rotated from left to right. The image shift is gradual from one image to a second image.

2-D/3-D Holography

This is a type of hologram that is made by putting a two dimensional holographic image in the foreground and putting a two dimensional holographic background behind it to create the appearance of depth.

Two Channel Image/Flip Image

A holographic effect wheby an image has an instant change from one image to another as the hologram is rotated from left to right.

Micro-Text

Small text that is only legible when viewed with an 8x or 10x magnifying gass.

Vertical & Horizontal Gradient Holography

The method of animating i holographic two dimensioal image so that the image rdiates bands of color in either the vertical or horizontal.

Fine Line Printing

The use of complex fine line designs that are sophisticated detail. Typical to banknotes and often referred to as guilloche printing. These designs can be successfully incorporated into many types of holograms.

Pseudo Color

This technique in making holograms gives a result where the object that is originated appears in its tru "natural" coloring. However, the colo is only apparent at a single "fixed" viewing angle. While you will see the image at any viewing angle it will only be in its natural coloring at one viewing angle.

Nano-Text

Refers to text that requires magnification beyond a simple eye loop and usually implies that a microscope is needed to decipher the text.

Circular Kinetic

The method of animating a holographic two dimensional image so that the image radiates bands of color in a set pattern.

Linear Kinetic Effect

A holographic image effect where an image is only visible when viewed at a specific angle.

Grayscale Image Effect

A holographic origination technique whereby the image appears in grayscale versus the traditional rainbow colors.

Figure 2: Lamination Security features

c) Holographic Personalization Technology (HPT)

Database verification is an important element of ID card. To secure this, a more recent trend is to combine holographic laminates with personal data, photos and other information. One example is Identigram, as found on the German ID Card and e-passport. HPT allows unique or generic diffractive images to be coated on a card surface. The images incorporate unique optical effects that are extremely difficult to counterfeit.

Figure 3: German ID card using HPT

Think, for example, of the card holder's photo, biographic data, a logo, symbols, a coat of arms or a combination thereof. This technology, which is also available for desktop personalization, allows a much wider range of diffractive optical images to be designed, this effectively adding an additional level of security to ID cards.

d) Holographic Biometrics Security

The security of card can also be enhanced by encrypting and storing (biographic data) on high-capacity chips, possibly in combination with biometrics. Given the limited space available on an ID cad, especially compared to passport, the use of electronic ID cards- or – eIDs – likely to increase. **Moreover, eIDs can be used for various e-business and e-governance applications, including online banking, shopping, and user registration and with implementation of government schemes.** In this system, the holographic photopolymer is laminated to the plastic card, either as a strip or patch. It is laminated with a reflective layer and protected against wear of tampering. The designated biometric (e.g. an iris scan or fingerprint) is captured in the normal way (cameras, fingerprint scanner, etc), then encoded using a code mask.

e) Enhanced Security with Laser Engraving

A growing number of industry participants are calling for laser engraving technology to be used on a broader scale. **Laser engraving**

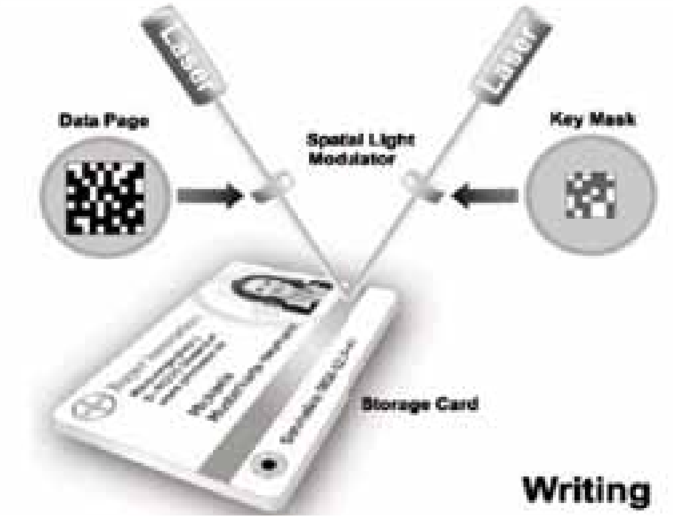


Figure 4: Phenostar, a holographic photopolymer storage medium for plastic cards, invented by Bayer Material Science

involves 'burning' data into the substrate of an ID card or polycarbonate biographic data page. The data may consist of text, images and graphics (including security features such as micro text).

As such, laser engraving is a technology rather than a security feature. The actual security is derived from the application method used. If properly applied, laser engraving provides protection against alteration and reproduction. In fact, laser engraving provides unsurpassed security. The application of heat (in the form of a laser beam) creates a chemical reaction inside the core of the card, causing molecules to move to the surface. The resultant characters or images are virtually impossible to modify - any attempt to alter or remove laser engraved data invariably destroys the substrate surface. Another advantage of laser engraving is that the data does not fade or deteriorate due to UV light or surface abrasion.

f) Advanced Laser Engraving

Laser engraving facilitates the creation of Multiple Laser Images (MLI) and Changeable Laser Images (CLI), which cannot be produced using othertechnologies. The process used to integrate CLI/ MLI images into the card body is highly specialised. CLI/MLI images are similar to holograms in that alternate images are produced, albeit using direct laser engraving. The alternate images are positioned close to each other and engraved at different angles. In contrast with holograms, CLI/MLI data forms an integral yet unique part of the card body (it is applied during personalisation). CLI/MLI allows personal data to be engraved on individual cards. Think, for example, of the document ID number or expiration date in combination with non-standard 'flipping' images of the cardholder's photograph or signature. **As the data cannot be copied or tampered, advanced laser engraving offers an additional level of security.** It also creates a much higher entry barrier for counterfeiters compared with other personalisation techniques. The result is a highly tamper-resistant card.

g) Creating Uniform Security Standards:

With the lack of consistent standards across identification documents today, it is often difficult to give reasonable assurance of a given document's authenticity. For e.g. MasterCard and Visa addressed the counterfeiting problem by mandating a uniform security feature in the form of a hot stamped hologram in the same place on each card, while leaving the rest of the design up to the discretion of the member banks. This resulted in a dramatic reduction in the incidence of credit card counterfeiting. This solution works because each layer of the security chain: consumer, issuer and law enforcement official alike, know where and what to look for to authenticate a given card.

In the end, no single security feature is able to provide adequate protection. Instead, security is optimized if several features are combined.

A clear laminate can be used to extend the card's life. If the laminate also contains holographic images, security is improved at the same time. Holographic laminate is therefore highly recommended for national IDs.

Conclusion

Improving the security of identity documents is a matter of urgent national security. Most identity documents in use today were not designed as secure documents, and there are no uniform security standards in place to assist the public and law enforcement in the recognition of genuine versus counterfeit identity documents. Government should understand that counterfeiters will attempt to counterfeit the least secure document.

Although no-one can stop a counterfeiter from trying to modify or copy a document, the right combination of security features and technologies make it impossible for him to be successful. These security features must be practical for document issuers to implement, easy for the public to recognize and provide specific identifying features for law enforcement and forensic investigators.