ISSN 1230-7483
e-ISSN 2720-5983

Problems of Forensic Sciences 2024, vol. 137, 47–67

DOI: 10.4467/12307483PFS.24.004.19860

A COMPARATIVE STUDY OF SECURITY FEATURES OF NATIONAL IDENTITY CARDS IN FIVE COUNTRIES: INDIA, BRAZIL, SOUTH AFRICA, MALAYSIA, AND THE PHILIPPINES

Mukti CHAVDA[1], Manisha MANN[2]

[1] *School of Forensics, Risk Management and National Security, Rashtriya Raksha University, Lavad, Dehgam, Gandhinagar, Gujarat – 382305, India*
[2] *National Forensic Sciences University (Delhi Campus), LNJN-NICFS Campus, Near Jaipur Golden Hospital, Outer Ring Road, Institutional Area, Sector 3, Rohini, Delhi – 110085, India*

Abstract

This article discusses the security features of national identity cards of different countries in order to compare and help understand the application and uniqueness of these features. National identity cards are security documents provided with embedded security features to prevent their counterfeiting and misuse. These features include holograms, microprinting, anti-photocopying properties, QR codes, and ghost images. A security document is a medium necessary to prove a person's identity as an unique individual in the civil and legal sense. This article analyzes a comparative study of national identity cards used in five countries: India, Brazil, South Africa, Malaysia, and the Philippines. The study was based on a collective set of 22 security features, such as ghost images, QR codes, tactile engravings, microprocessor chips, guilloches, holograms, and anti-photocopying features. The results showed that the lowest number of security features appears in the Brazilian identity card (8), followed in increasing order by India (10), Malaysia (12), the Philippines (12), and South Africa (14). Moreover, the article discusses the prevalence of security features, along with the need for and the methods to implement their improvement. The study aims to identify a security feature or a combination of features that would make the security document in question safer. This could assist countries around the world in curbing the prevalence of fraud and identity theft by improving and strengthening their identification systems.

Keywords

Security documents; Security features; National identity cards; Identification system; Fraud; Identity theft.

Received 20 November 2023; accepted 7 February 2024

Civilization has long followed the process of documentation in the course of streamlining its legal, political, and social spheres. Documents are a durable tool for collecting, recording, and preserving events, memories, and information. With the modern age changing the nature of documentation, documents with a legal aspect are now considered the most important, concrete, and useful. This group includes identity cards, driving licenses, ration cards, and other documents, such as those functioning as court evidence and records.

Section 3 of the Indian Evidence Act of 1872 defines a *document* as "any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, which is intended to be used, or which may be used, for the purpose of recording that matter" [1]. In other words, any surface that bears marks, letters, or symbols – thus delivering a certain message or conveying information – is called a document.

Security documents

In legal terms, security documents are a type of security agreement that protects specific information for the owner of that particular instrument. The information in question is connected exclusively to the document holder and derived from the holder's details. However, counterfeiting or false alteration of documents that have legal standing is becoming an increasingly frequent problem that affects the security of individuals forming a particular nation or society. Hence, it has become imperative for the authorities responsible for ensuring this security to protect the individuals' information derived from their security documents. Consequently, such documents display certain features embedded during their manufacture and preparation.

In view of the above, a *security document* refers to an instrument that contains specific incorporated countermeasures against counterfeiting, tampering, or alteration. There are three categories of such countermeasures:

– elements present on the document's surface or in its substrate (e.g. paper),
– elements created by different printing techniques (e.g. intaglio, digital),
– elements created by different types of inks (e.g. optically variable ink).

Importantly, the security measures in question refer not only to financial aspects but also to the information contained within a particular instrument. There are numerous security documents which function in different domains, namely:

– education: grade sheets, certifications,
– banking: credit and debit cards, permanent account number (PAN) cards, bank passbooks,
– the judiciary: judicial stamp papers, postal papers,
– real estate transactions: agreements, powers of attorney, records of rights, tenancy, and crops (RTC), debentures,
– employment: job offer letters, employment authorization document (EAD) cards.

The most general of these include travel and identity documents, such as passports, national identity cards, and banknotes. The misuse of these documents occurs in criminal acts that range from forgery and identity theft to illegal transaction activities and trafficking. Hence, member states of international organizations like the United Nations work toward the enhancement of features in security documents and their examination so as to prevent related criminal activities [2].

In India, the requirements for security documents are met in their entirety by the India Security Press (ISP) in Nashik and the Security Printing Press (SPP) in Hyderabad. These security printing presses belong to the Security Printing and Minting Corporation of India Limited (SPMCIL). The presses print bonds, warrants, postal stamps, cheques, and travel documents, while their security features include microprinting, embossing, guilloche patterns, and designs with ultraviolet (UV) inks.

Security features

A *security feature* is designed to protect the security document against any act of misuse or counterfeiting (fraudulent imitation). As discussed above, security features can be present in the substrate or be created by the use of different inks or printing methods. Examples include bi-fluorescent inks, microperforations, holograms, guilloche patterns, chemically reactive materials, and die-cutting. Moreover, security features are classified into levels [3]:

Level 1: Overt features visible to any individual without special aids or support (e.g. tactile engraving, guilloche, rainbow printing).

Level 2: Covert features that can be visualized with such simple techniques as UV illumination or a magnifying glass (e.g. microtext).

Level 3: Forensic features that can be identified only with forensic knowledge and sophisticated examination techniques (e.g. digital watermarking).

Level 4: Hidden, confidential laboratory features that only experts or the manufacturers themselves can confirm (e.g. tagging).

The national identity card is a document that provides proof of a person's identity. Usually, only a citizen or resident can acquire such an identity document. However, in some countries, such as India, an identity card is not proof of citizenship [4]. Documents like national identity cards or birth certificates – and the biometric methods used in their production and issuance – indirectly confirm that their holder is a law-abiding citizen. National identity cards serve as valid proof of identity and a method of distinguishing between people in the event of national or international migrations. Moreover, identity cards facilitate enrollment in educational institutions, bank account opening, or the use of public healthcare services. Finally, identity cards allow the authorities to establish a national population database and keep car holders updated about resulting benefits and entitlements.

Common security features in national identity cards include [5]:

a. guilloche pattern: an ornamental engraving in the form of a complex geometric pattern consisting of thin, continuous lines. These lines are formed on the basis of mathematical rules, and their constantly changing curvature makes the feature difficult to copy. The pattern can consist of lines, rosettes, borders, parts of background design, an ellipse, or a polygon. Manufacturers can also use covert inks to create different color combinations.

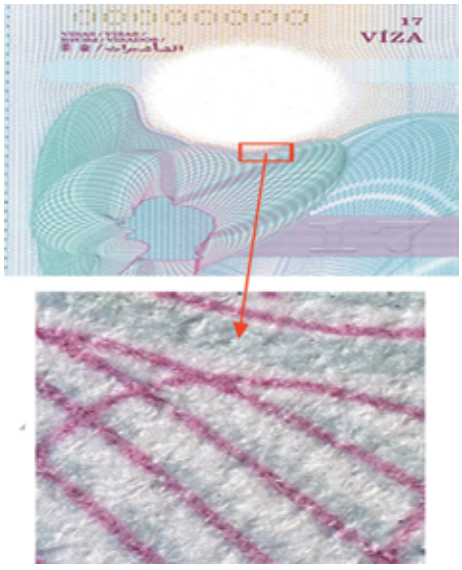


Figure 1. A magnified guilloche pattern on a Czech Republic passport from 2005.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g380

b. hologram: an optically variable feature that requires diffraction of light to visualize its unique optical properties and creates 3D virtual effects; it may appear to diffract different light beams at different angles. Holograms provide anti-photocopying protection, making them difficult to copy using a printer or photocopier. They can be customized using nano- and microprinting, microimages, or laser-readable images. These types are classified as reflected or transmitted holograms depending on the illumination technique applied to visualize the image [5].

Figure 2. A hologram from different angles on a special passport from Iraq, 2011.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g383

c. microprinting/microtext: a very tiny (0.15–0.30 mm high) text, symbol, or figure that requires magnification to be seen with the naked eye. It is mainly used as anti-photocopying protection as it is difficult to reproduce. This feature enhances the security properties of holograms and security threads. Microprinting includes two types: positive – dark letters on a light background, and negative – light letters on a dark background.

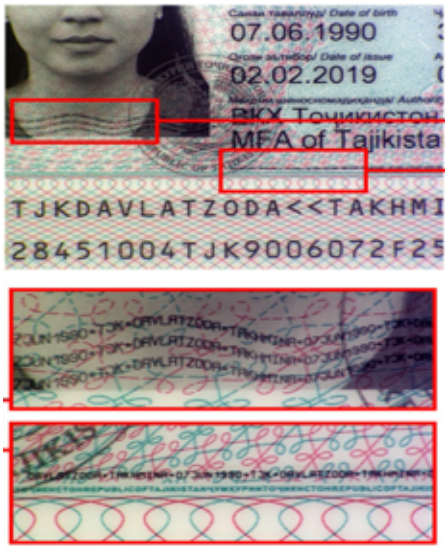


Figure 3. An identity card from Tajikistan.
Source: https://platform.keesingtechnologies.com/micro-printing-3/

d. secondary image and ghost image: found on the personal information page of a security document. This is a repeated image with a reduced or contrasting size, applied using the same or different techniques as the holder's main image. Examples include the use of laser engraving to plot the image on paper or a polymer substrate or the use of a hologram-like formation to view the secondary image in oblique light. This printing technique uses covert ink for ghost images. The image can be reproduced multiple times on the document using techniques such as UV light visualization.

Figure 4. A secondary image on a Korean passport plotted with UV-transparent fluorescent ink.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g428

e. QR code: an array of machine-readable matrix of black and white squares that stores information related to the document. The digital signature generated by a QR code is highly secure, and the credibility of the information it conveys can be readily verified.

Figure 5. A QR code on an Indian *Aadhaar* card.
Source: https://www.scribd.com/document/427789751/Aadhaar-card-sample-300x212-pdf

f. bar code: a set of lines or rectangles with varying thickness, arranged as a sequence and containing graphic information. A barcode may include UV luminescence or magnetic ink to enhance security. The encoded information is read by special devices. This feature is available as a linear barcode, encoded and read in one direction, and a 2D barcode, encoded and read in both the horizontal and vertical direction.

Figure 6. A barcode in a Brunei passport from 2008.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g460

g. embedded microprocessor chip: an encrypted microprocessor chip used to store, receive, and transfer data. The user needs to place the chip under a reader or scanner to read the encrypted data.

Figure 7. A Finnish identity card.
Source: https://hmong.in.th/wiki/Smartcard

h. background pattern: a type of image or decorative design visible below the main printed information and other security features. It prevents attempts to alter or erase the text, images, or marks present on the document's surface, as any such attempt damages the background pattern. The techniques used to produce this feature include offset printing, where an offset cylinder with a rubber blanket transfers ink from the printing plate to the receiving surface; Orlov printing, in which separate color printing plates transfer ink to a single plate and then to the receiving surface, creating a sharp change of color with each stroke; and rainbow printing, in which colors merge gradually. The pattern can consist of microtext/microprinting, designs with solid colors, lines of varying thickness creating an illusion of

a three-dimensional element, guilloches, or anti-copying features.

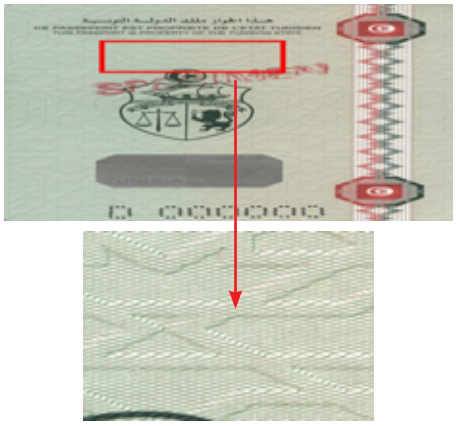


Figure 8. A background pattern with 3D elements on a Tunisian diplomatic passport from 2003.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g452

i. optically variable ink: also called color-shifting ink because it shifts color depending on the viewing angle as well as the angle of illumination and the thickness of the dielectric layer used. It consists of two reflective layers: a bottom metallic layer and a surface translucent metallic layer – a transparent dielectric layer (MgF2) with nontransparent and colorless pigments. The surface and bottom layers partially reflect white light, and the interference, along with a series of multiple reflections, results in the selective absorption of waves, producing the visible color.

Figure 9. A Greek passport from 2004.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g457

j. embossing: blind embossing involves deforming the substrate under pressure or heat, or both, depending on whether the substrate is made of paper or polymer. The resulting relief is concave or convex and permits visualization in oblique or sliding light. Embossing can also be used in combination with optically variable ink to print an image as a background for a second image to be applied by blind embossing.

Figure 10. A New Zealand identity card from 2016 with embossing.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g374

k. fingerprint: a graphic reproduction of the holder's fingertip friction ridges on the document's surface. Fingerprints are an excellent tool in biometrics due to their individuality, permanency, and universality.

Figure 11. A passport from Kosovo.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g420

l. multilayer image: a composite image created using multiple initial images. It is applied via lenticular technology, namely under lenticular lenses using laser engraving that embosses the layers onto a polymer substrate. The initial images, cut into stripes to form the composite image, contain personal data. The result is a layered image with an illusion of depth or the ability to show different characteristics at different viewing angles.

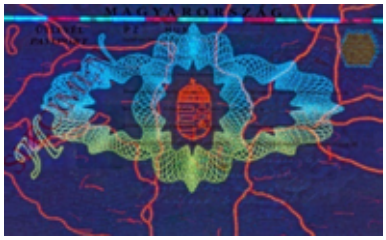
holder's portrait at a 45º | date of birth at a 135º | horizontal array of lense

Figure 12. Multiple laser layering of images on a Swedish emergency passport from 2012.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g412

m. features applied using UV fluorescent ink: this type of ink contains luminophores – atoms of the compound's functional group responsible for luminescent properties. When exposed to UV light at a particular wavelength (250–380 nm), luminophores produce fluorescence of different colors.

Data page on hybrid substare

UV light of 365 nm



UV light 254 nm

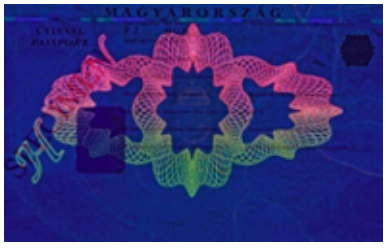


Figure 13. A service passport from Hungary: rainbow print in UV light.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g449

n. anti-photocopying features: these features consist of patterns and elements forming a background design that prevents forgery by scanning or photocopying. A scanned or copied document bears the text 'copy' or 'void', which is invisible to the naked eye in the original document. The text appears, for example, as rainbow lines or colored strips.

Figure 14. A special passport from Egypt (1999) with 'copy' appearing as rainbow lines.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g372

o. rainbow printing: a printing method that uses one color box with multiple colors separated by plates. In this method, one color merges into another while forming a symbol or pattern.

Figure 15. A passport from Belarus with a rainbow-print background.
Source: https://regulaforensics.com/explore/expert-hub/glossary/documents/#g395

Materials and methods

Materials

The following section presents the national identity cards used in the countries included in the comparison – India, Brazil, South Africa, Malaysia, and the Philippines.

India: Aadhaar Card

The *Aadhaar* card contains a 12-digit unique identity number that acts as proof of residence and identity for both adult and underaged citizens of India. This group also includes resident foreign nationals who spent more than 182 days in the past 12 months in India. The card's issuer is the Unique Identification Authority of India (UIDAI), a statutory authority of the Ministry of Electronics and Information Technology in the Government of India, established in 2009. *Aadhaar* is the world's largest biometric system. The system establishes identity using demographic information – such as name, date of birth, gender, and address – and biometric information, namely ten fingerprints, two iris scans, and a facial photograph. The *Aadhaar* card is not proof of citizenship. However, other identity-based applications and services in India – like the ration card or the passport – can use the Aadhaar card to verify identity, which confirms the card's usefulness. Morever, one must use the *Aadhaar* number while filing an income tax return or applying for a PAN card [6].

The new *Aadhaar* cards, introduced in 2020, are plastic-based (made of PVC) and contain better security features, such as invisible logos and holograms.

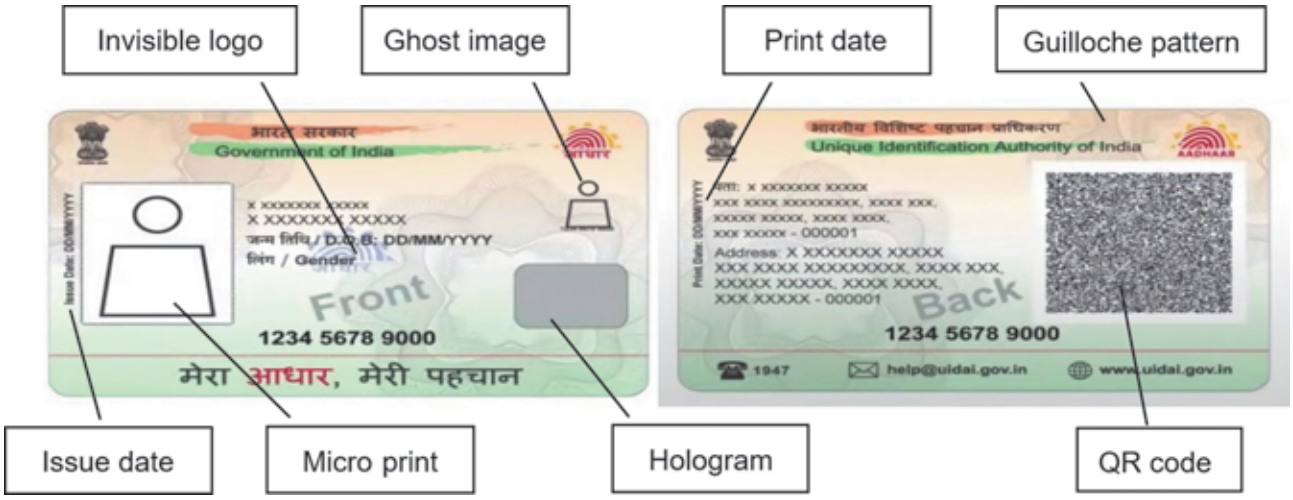


Figure 16. An *Aadhaar* card from India.
Source: https://www.indiatvnews.com/technology/news-aadhaar-pvc-card-how-to-order-online-708738

The cards include concealed data to safeguard data privacy: only the last four digits of the unique number are visible, and the rest is concealed by blocks of the letter 'X' in the e-Aadhaar [7].

Brazil: Cédula de Identidade

The Brazilian identity card is known as *Cédula de Identidade* or, informally, as *Carteira de Identidade Nacional* (CIN). It has replaced the General Registry (*Registro Geral*) in 2022, although the old identity card will remain valid until 2032. The replacement was free of charge, and the new document was initially introduced only in a few states. Brazilian citizens obtain the card as soon as they become teenagers. Therefore, most citizens are in possession of their cards, although the document is just one of the many proofs of identity that function in Brazil. Nonetheless, experts rank it among the safest identification documents in the world [8].

Brazilian nationals with a taxpayer number – an 11-digit long unique number known as CPF (*Cadastro de Pessoas Físicas*) – are eligible to file a request for an identity card. The authorities may use the birth certificate, marriage certificate, or naturalization certificate to produce the card. Its common features include the issue date, the date and place of birth, the CPF number, the coat of arms, a signature, and a thumbprint. The new identity card will be available as a modern plastic ID-1 card, a classic paper-based card, or a digital e-card. It will also contain a QR code for better readability [9].

Figure 17. The new Brazilian identity card.
Source: https://www.fronteiralivre.com.br/como-tirar-o-novo-rg-digital-com-qr-code-rg-unico/

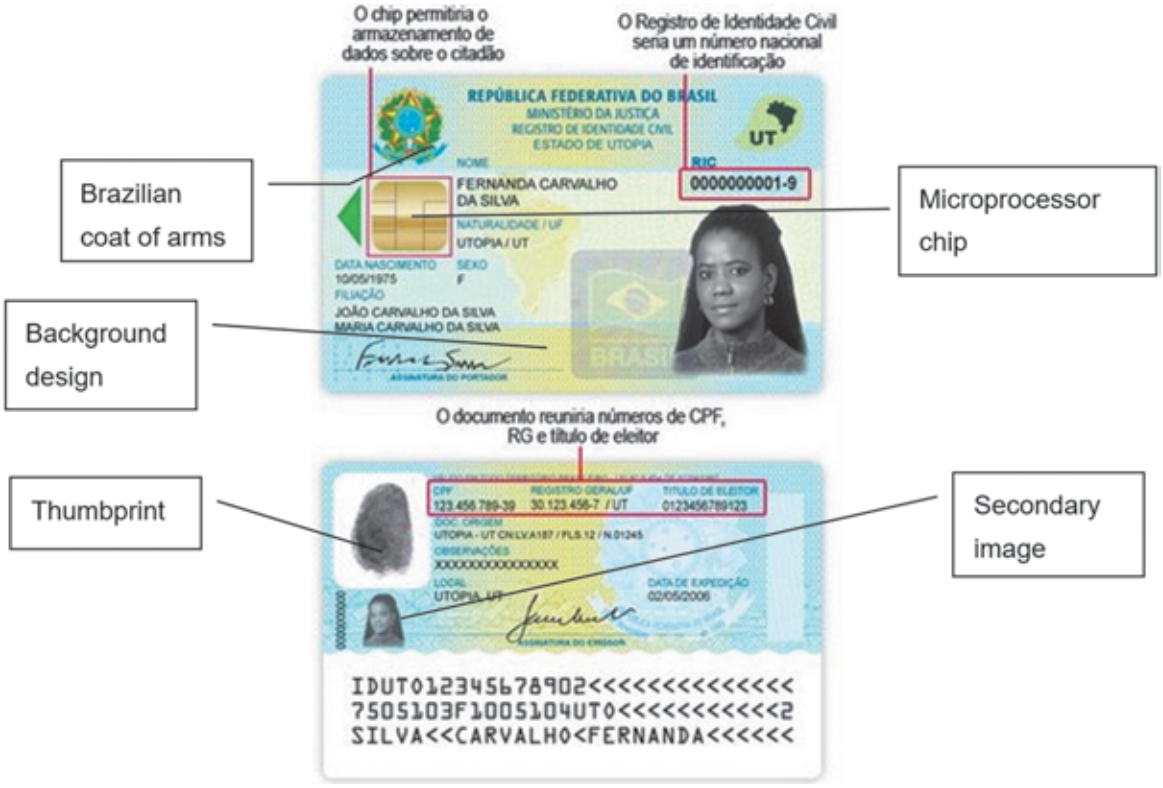


Figure 18. The old Brazilian identity card from 2009.
Source: https://ubisurv.net/2009/01/21/the-new-brazilian-id-system/

South Africa: Smart ID Card

South African citizens and permanent residents need a Smart ID Card, which has replaced the original green bar-coded identity book. The card is mandatory for all persons aged 16 years and above. It was first introduced in 2013, and people could initially apply for it in local banks. Afterward, the authorities launched a web portal for the application process to facilitate registration for older people. By 2018, the government had issued 5.5 million cards.

The Smart ID Card stores biometric information and details such as full name or date of birth. An embedded microprocessor ensures that the information about every card holder is easy to read and matches digitally at any authentication point. The card eliminates the requirement of having multiple identity documents and assists in quick security checks, the registry of citizenship, and the use of various governmental service schemes [10]. Two types of the document are in use: type A accommodates names of regular length, while type B is intended for holders whose names are long [11].

Malaysia: MyKad

The Malaysian identity card is known as *MyKad* (*Kad Pengenalan Malaysia*). The government introduced it in 2001 as a means of identification for citizens aged 12 years and above. The sample card shown here is the ordinary model that the general public uses. Permanent residents, police officers, and military persons receive special identity cards – for example, *MyPR* is the residents' document – but these have similar features. Malaysia was the first country in the world to introduce an identity card with an embedded microprocessor containing the necessary biometric information [12].

MyKad's issuer is the National Registration Department, and the application process occurs online. The card contains a unique number, which consists of 12 digits arranged in three blocks separated by hyphens according to the following pattern: YYMMDD-PB-###G. The first block of digits stands for the holder's date of birth, the second block represents the code denoting the place of birth, and the third block is computer-generated by the National Registration Department [13].

The Philippines: PhilSysID

PhilSysID, the national identity card of the Philippines, was introduced in 2018. The applicant has to produce a government-approved document containing their name, photograph, and signature. A legal guardian must be present for minors below 18 years of age. The card contains a 12-digit permanent identification number called the *PhilSys* Number (PSN) that is given to every citizen. After an online application, clerks in registration centers verify the supporting documents, and the card is issued after a certain period. Since the PSN is confidential, another number – the *PhilSys* Card Number (PCN) – protects it during public transactions. The card contains full demographic and biographic information about the holder, along with a digitally signed QR code [14].

Figure 19. The national identity card used in South Africa.
Note: OVD – optically variable device. OVI – optically variable ink. *Source:* http://www.dha.gov.za/index.php/id-smart-card

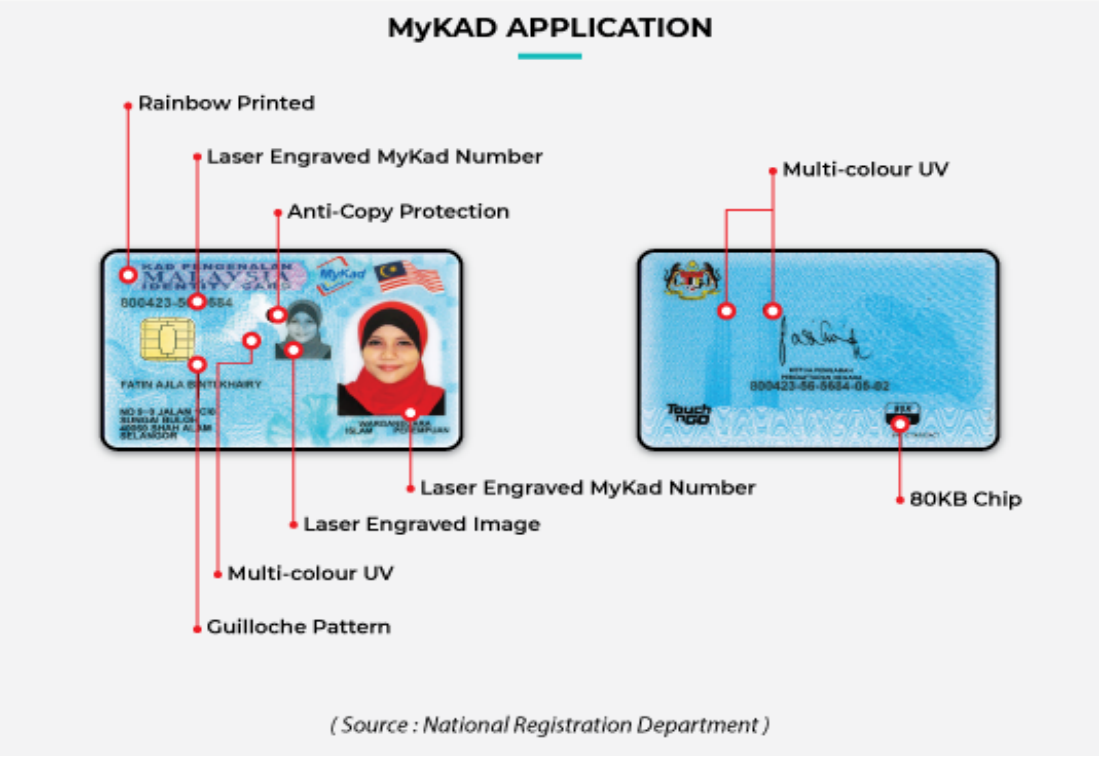


Figure 20. *MyKad* Malaysia. *Source:* https://www.techarp.com/facts/readable-mykad-vote-election/

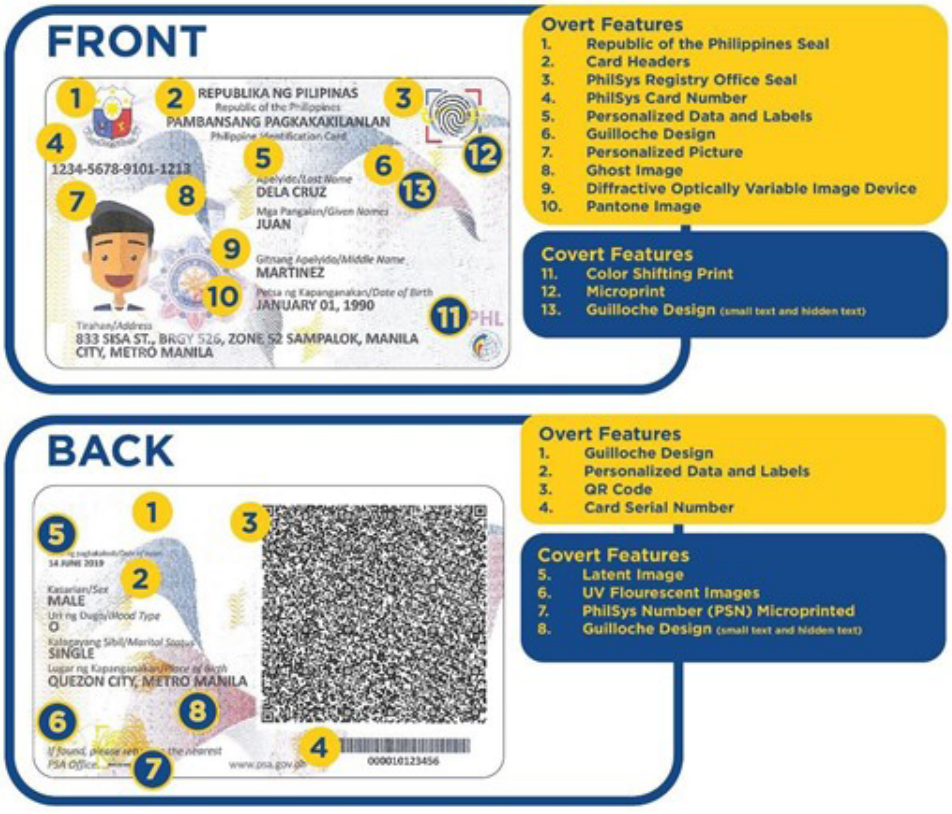


Figure 21. The identity card used in the Philippines. *Source:* https://philsysonline.com/philippine-national-id-parts/

Methods

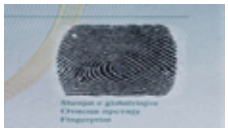
The study employed a qualitative approach, with data collected from secondary and tertiary sources (the observations made about the security documents are backed by already existing reports, texts and review articles). The obtained data enabled a comparison of the relevant security documents. An inductive approach governed the use of the collected data while identifying topics, phenomena, and patterns to create a conceptual framework. The resulting specific observations served as the basis for a generalization.

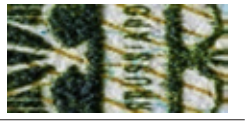
Results and discussion

The following table compares the security features present in the national identity cards of the five studied countries.

The list includes 22 security features. According to Table 1, the lowest number of security features is found in the Brazilian identity card (8), followed in increasing order by India (10), Malaysia (12), the Philippines (12), and South Africa (14). The most common features – those used in four or five countries – include security number series, photograph, signature, background design, and ghost image, with the last one absent only from the Brazilian card. Certain features, like barcode, multilayer image, and use of Braille, appear exclusively on South Africa's Smart ID Card. The embossed logo is unique to the Indian card, while the Philippine document is the only one with a latent image. Anti-photocopying features appear only on Malaysia's *MyKad*. The remaining security features display a moderate match among two or three countries; thus, one can consider them as vital emerging features in the domain of security documents. These include tactile or laser engraving, hologram, guilloche pattern, QR code, microtext, optically variable ink or optically variable devices, fingerprint, UV features, the presence of a seal or emblem, and microprocessor chip. South Africa, Malaysia, and Brazil use identity cards with a microprocessor chip, which makes them easy to convert into digital or virtual identity cards, reducing the risk of fraud or theft. Table 2 shows the numerical distribution of security features among the five countries' documents.

Table 1
A comparison of the security features of national identity cards

Security feature	India	Brazil	South Africa	Malaysia	The Philippines	Illustration
Security number series	Present	Present	Present	Present	Present	
Photograph	Present	Present	Present	Present	Present	
Microprocessor chip	Absent	Present	Present	Present	Absent	
Seal or emblem	Absent	Present	Absent	Absent	Present	
Fingerprint	Absent	Present	Absent	Present	Absent	

Security feature	India	Brazil	South Africa	Malaysia	The Philippines	Illustration
Barcode	Absent	Absent	Present	Absent	Absent	
Multilayer image	Absent	Absent	Present	Absent	Absent	
UV features	Absent	Absent	Present	Present	Present	
Embossed logo	Present	Absent	Absent	Absent	Absent	
Signature	Present	Present	Present	Present	Present	
Optically variable ink/ device	Absent	Absent	Present	Absent	Present	
Latent image	Absent	Absent	Absent	Absent	Present	
Background design	Present	Present	Present	Present	Present	
Braille	Absent	Absent	Present	Absent	Absent	
Microtext	Present	Absent	Absent	Absent	Present	
QR code	Present	Present	Absent	Absent	Present	
Ghost image	Present	Absent	Present	Present	Present	
Guilloche	Present	Absent	Absent	Present	Present	

Security feature	India	Brazil	South Africa	Malaysia	The Philippines	Illustration
Hologram	Present	Absent	Present	Absent	Absent	
Anti-photocopying features	Absent	Absent	Absent	Present	Absent	
Tactile/laser engraving	Absent	Absent	Present	Present	Absent	
Rainbow print/image	Absent	Absent	Present	Present	Absent	

Source: own elaboration.

Table 2
Numerical distribution of security features among the analyzed countries' identity cards

Country	Most common features	Moderately matched features	Least matched features	Total features
India	5	4	1	10
Brazil	4	4	0	8
South Africa	5	6	3	14
Malaysia	5	6	1	12
The Philippines	5	6	1	12

Source: own elaboration.

Conclusion

As discussed in the introduction, most security features belong to one of three levels: easily visible (overt) features, those requiring special techniques like UV visualization (covert features), and forensic features. Interestingly, the South African identity card includes the highest number of features [14] and the most technologically advanced features. First, the card has a durable polycarbonate body with visual protection against forgery. Second, the biometric information stored in the microprocessor and the encryption key for identification ensure contactless verification of card holders. Although the Brazilian card displays the lowest number of security features, the presence of a microprocessor chip both in the old document and the new digital version is an important aspect that considerably enhances security.

The need to use the maximum number of security features, along with their adequate complexity to serve the intended purpose, becomes evident when considering the potential of theft, fraud, or counterfeiting of security documents. The counterfeiting rate is directly related to the number of fraudulent use attempts and the percentage rate of identity theft in the countries concerned. In South Africa, for instance, identity theft from documents renders the victims more susceptible to a large amount of unrelated debts under their name [15]. In Malaysia, the National Registration Department determined 1047 cases of using a fake identity card between 1990 and 2013 [16]. In Brazil, the fraud rate reaches 37.5%, while in the Philippines, 55 million users are at risk of losing their information. In the case of India, six percent of the *Aadhaar* card fingerprint authentication procedures fail. Moreover, as of 2020, the authorities have canceled 40,955 *Aadhaar* numbers as fake.

There are two ways to remedy these problems:
– increasing the number of high-quality security features with a more complex technological structure and application,
– introducing appropriate punitive measures for the forgery and counterfeiting of security documents.

As regards the features themselves, Estonia is said to have the world's most advanced and sophisticated identity card. The document contains a chip that carries embedded files, a color photograph, a QR code, a secondary image visible only from a certain angle, and a 2048-bit public key encryption, making it easy to use in the electronic environment. The card was developed in December 2018 in collaboration between global experts and Estonia's national authorities, such as the Estonian Forensic Science Institute and Enterprise Estonia. Its characteristics can serve as improvements to the security features present in other national identity cards. In terms of punitive measures, each of the five countries uses both fines and an imprisonment term ranging from two to 10 years. While immigration in a country like Estonia remains limited, developing countries see large numbers of illegal immigrants, with India and Brazil ranked in the world's top ten. Hence, developing countries need improved identity cards for national security purposes. The document in question is important for the security of individuals and nations alike, as it significantly reduces the rates of illegal immigration, impersonation fraud, and identity theft – not possessing a necessary security document is related to a person being an illegal immigrant or a fraud. A security document or identity card is related to the citizenship of a country, a person not possessing the same will not be considered part of the genuine population. So, an identity card holder possesses a legal instrument, which confirms that they belong to the law-abiding part of the population.

Future prospects

The future of security documents lies in the evolution of advanced security features and associated services. From Malaysia as the first country to introduce an identity card with a computer-based chip, fingerprint biometrics, and photographic identification, to the Philippines as the country with over 75 million applications for the national identity card, the necessity of establishing a more secure and robust national identification system with a global outlook has only grown more complex.

The South African identification system followed technological advancements and produced a card with a microprocessor chip that serves as a source of single-point digital identification and authentication. Brazil also significantly improved its national identity card by providing its digital format in a government application and adding a QR code that can verify the card's authenticity at any point [17]. In India, the future looks promising with respect to the enhancement of the *Aadhaar* card's security features. The Deputy Director General of UIDAI believes that the card will soon receive a biometric locking/unlocking system to prevent unauthorized access in case of the card's misplacement or theft. Moreover, a virtual format will be introduced to mitigate the risk of theft. Finally, verification will also occur offline to increase *Aadhaar*'s accessibility [18].

Today, the future relies on implementing these efforts not only in developed or rapidly developing countries but also in countries that are underdeveloped. The latter states should establish their respective national identification systems and thus improve their own standing while contributing to global security.

References

1. Ministry of Law and Justice of India. The Indian evidence act 1872. New Delhi: Ministry of Law and Justice of India; 1872. Available from: https://lddashboard.legislative.gov.in/actsofparliamentfromtheyear/indian-evidence-act-1872
2. United Nations Office on Drugs and Crime (UNODC). Security document examination. Vienna: UNODC; 2018. Available from: https://www.unodc.org/documents/scientific/Brochure_doc_kits.pdf
3. Thales Group. Levels of identity security and groups of secure features (2023). Paris: Thales Group; 2023. Available from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/security-features/levels-identity-security
4. Unique Identification Authority of India (UIDAI). Aadhaar is not a citizenship document. New Delhi: UIDAI; 2020. Available from: https://uidai.gov.in//images/Aadhaar_Press_Release_18Feb_2020.pdf
5. Regula. Glossary of documents Daugavpils: Regula; no date. Available from: https://regulaforensics.com/explore/expert-hub/glossary/documents/
6. Motiani P. Who can apply for Aadhaar card? Know the eligibility rules. The Economic Times. 2018 October 15. Available from: https://economictimes.indiatimes.com/wealth/personal-finance-news/who-are-eligible-to-apply-for-aadhaar-find-out/articleshow/59998036.cms?-from=mdr

7. Unique Identification Authority of India (UIDAI). What is Aadhaar? New Delhi: UIDAI; no date. Available from: https://www.uidai.gov.in/en/16-english-uk/aapka-aadhaar/14-what-is-aadhaar.html
8. Murakami Wood D, Firmino R. Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of "identity fraud". Identity in the Information Society. 2009;2(3): 297–317.
9. Goulard J, Hwang H, Ferreira R. Brazil – new identity card and passport models. Amstelveen: KPMG Global; 2022 July 13. Available from: https://kpmg.com/xx/en/home/insights/2022/07/flash-alert-2022-135.html
10. South African ID card: identity and citizenship. Paris: Thales Group; no date. Available from: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/south-africa
11. Republic of South Africa Department of Home Affairs (DHA). Know your new Smart ID Card. Pretoria: DHA; no date. Available from: https://www.dha.gov.za/index.php/id-smart-card/
12. 3 methods to read MyKad. Subang Jaya: Innov8tif; 2023 August 7. Available from: https://innov8tif.com/3-methods-to-read-mykad-2/
13. MyKad – Malaysia National Registration Identity Card (NRIC). Sydney: Employment Hero; no date. Available from: https://employmenthero.com/my/glossary/mykad/
14. Philippine Identification System. Manila: Government of the Philippines; no date. Available from: https://philsys.gov.ph/
15. Identity theft (2023, May 2). TransUnion South Africa. Available from: https://www.transunion.co.za/education/identity-theft
16. Radhi NA, Babulal V, Yusof TA. 1,047 arrested for involvement with fake MyKad syndicates. New Straits Times. 2019 November 12. Available from: https://www.nst.com.my/news/crime-courts/2019/11/537879/1047-arrested-involvement-fake-mykad-syndicates
17. Ministério da Gestão e da Inovação em Serviços Públicos (MGI). Perguntas e respostas sobre a nova Carteira de Identidade Nacional. Brasília: MGI; no date. Available from: https://www.gov.br/gestao/pt-br/identidade. Portuguese.
18. Patil P. Aadhaar gets new data privacy features, says UIDAI DG Sumnesh Joshi. Deccan Chronicle. 2023 August 3. Available from: https://www.deccanchronicle.com/nation/current-affairs/030823/aadhaar-gets-new-data-privacy-features-says-uidai-dg-sumnesh-joshi.html

Corresponding author
Mukti Chavda
School of Forensics, Risk Management and National Security, Rashtriya Raksha University, Lavad Dehgam, Gandhinagar, Gujarat – 382305, India
e-mail: mdchavda2000@gmail.com

Problems of Forensic Sciences 2024, vol. 137, 47–67

BADANIA PORÓWNAWCZE ZABEZPIECZEŃ W DOKUMENTACH OSOBISTYCH UŻYWANYCH W PIĘCIU KRAJACH: INDIACH, BRAZYLII, POŁUDNIOWEJ AFRYCE, MALEZJI I FILIPINACH

Od wieków standardem cywilizacyjnym jest prowadzenie dokumentacji w celu usprawnienia funkcjonowania prawnego, politycznego i społecznego. Dokumenty są narzędziem pozwalającym przez długi czas gromadzić, zapisywać i zachowywać wydarzenia, wspomnienia i różne inne informacje. Na skutek zachodzących obecnie zmian najważniejszymi, najprzydatniejszymi i najbardziej konkretnymi typami dokumentów stały się te związane z aspektami prawnymi, w tym dokumenty tożsamości, prawa jazdy, karty upoważniające do przydziału jedzenia czy dowody i akta sądowe.

Rozdział 3 indyjskiej Ustawy o dowodach z 1872 r. definiuje *dokument* jako „wszelkie informacje wyrażone lub opisane na jakimkolwiek materiale za pomocą liter, cyfr lub znaków bądź za pomocą wielu takich metod jednocześnie, których celem jest zapisywanie tychże informacji lub takich, które można w tym celu zastosować" [1]. Innymi słowy – dokumentem jest każdy materiał dostarczający jakichś informacji za pomocą znajdujących się na nim znaków, liter czy symboli.

Dokumenty osobiste

Z prawnego punktu widzenia dokument osobisty stanowi rodzaj umowy chroniącej szczegółowe informacje o jego posiadaczu – i tylko o jego posiadaczu. Narastający problem fałszowania i nielegalnej zamiany dokumentów o znaczeniu prawnym zagraża bezpieczeństwu osób należących do danego narodu czy danej społeczności. Priorytetowym zadaniem władz odpowiedzialnych za bezpieczeństwo staje się zatem ochrona informacji zapisanych w dokumentach osobistych. W tym celu dokumenty takie w trakcie produkcji i przygotowania zaopatruje się w różne zabezpieczenia.

Można więc zdefiniować *dokument osobisty* jako instrument zawierający określone zabezpieczenia przed fałszerstwem, manipulacją i zmianą. Wyróżnia się trzy typy zabezpieczeń:
- elementy znajdujące się na powierzchni dokumentu bądź jego substratu (np. papieru),
- elementy naniesione różnymi technikami drukarskimi (np. druk wklęsły, druk cyfrowy),
- elementy naniesione różnego typu atramentami (np. atramentem zmiennym optycznie).

Co istotne, wyżej wymienione środki stosuje się nie tylko ze względów finansowych, ale także po to, by zabezpieczyć zawarte w takich dokumentach informacje. W poszczególnych domenach funkcjonuje wiele różnych typów dokumentów osobistych, tj.:
- w szkolnictwie: arkusze ocen, dyplomy,
- w bankowości: karty kredytowe i debetowe, karty stałego numeru konta (*permanent account number*, PAN), książeczki oszczędnościowe,
- w sądownictwie: karty pieczęci sądowych, papier pocztowy,
- w obrocie nieruchomościami: umowy i rejestry pełnomocnictw sądowych, praw, dzierżaw i upraw (warzywa korzeniowe i bulwiaste), skrypty dłużne,
- w zatrudnieniu: oferty pracy, pozwolenia na pracę (*employment authorization document*, EAD).

Najpowszechniej stosowanymi dokumentami osobistymi są te używane w podróży i służące do identyfikacji osobistej, w tym paszporty, dowody osobiste, a także noty bankowe. Jest wiele przestępstw związanych z nadużyciem dokumentów osobistych – od fałszerstwa i kradzieży tożsamości po nielegalne transakcje i handel ludźmi. Dlatego aby zapobiec takim przestępstwom, państwa należące do międzynarodowych organizacji, w tym także do ONZ, dążą do usprawnienia zabezpieczeń w dokumentach osobistych oraz procesu potwierdzania ich autentyczności [2].

W Indiach o spełnianie wszystkich wymogów dotyczących takich dokumentów dbają dwie instytucje: India Security Press (ISP) w Nashiku oraz Security Printing Press w Hajdarabadzie. Obie drukarnie należą do organizacji Security Printing and Minting Corporation of India Limited. Powstają w nich obligacje, zabezpieczenia pieniężne, znaczki pocztowe, czeki i dokumenty podróżne, a stosowane w nich zabezpieczenia obejmują mikrodruk, wytłaczanie, wzory giloszowe i nadruk wzorów wykonanych w sposób widzialny w świetle ultrafioletowym.

Zabezpieczenia

Celem zabezpieczeń jest ochrona dokumentu osobistego przed fałszerstwem i nadużyciem. Jak wspomniano powyżej, zabezpieczenia mogą występować w podłożu lub być nań nanoszone różnymi atramentami i metodami drukarskimi. Przykładami są atramenty bifluorescencyjne, mikroperforacje, hologramy, wzory giloszowe, materiały reaktywne chemicznie i zastosowanie sztancowania. Dodatkowo zabezpieczenia dzielą się na poziomy [3]:

Poziom 1: Jawne zabezpieczenia widoczne bez specjalnych przyrządów, np. grawerowanie dotykowe, giloszowanie, druk tęczowy.
Poziom 2: Ukryte zabezpieczenia uwidaczniane prostymi technikami, takimi jak światło UV czy szkło powiększające (np. mikrotekst).
Poziom 3: Zabezpieczenia kryminalistyczne, wykrywalne tylko za pomocą wiedzy specjalistycznej i zaawansowanych technik (np. cyfrowe znaki wodne).
Poziom 4: Ukryte, poufne zabezpieczenia laboratoryjne, które mogą stwierdzić wyłącznie eksperci lub sami producenci (np. znakowanie).

Dowód osobisty to prawomocny dokument potwierdzający tożsamość posiadacza. Dowód tożsamości mogą zazwyczaj uzyskać tylko obywatele lub mieszkańcy danego kraju. W niektórych krajach, takich jak Indie, dowód tożsamości nie potwierdza jednak obywatelstwa [4]. Dokumenty typu dowód tożsamości czy akt urodzenia, wraz z metodami biometrycznymi, za pomocą których są produkowane i wydawane, stanowią pośredni dowód, że ich posiadacz jest przestrzegającym prawa obywatelem. Dowody tożsamości to prawomocne potwierdzenie tożsamości oraz metoda identyfikowania osób w przypadkach migracji wewnątrz- i międzynarodowych. Mogą też służyć naborowi do placówek edukacyjnych, otwieraniu konta bankowego czy korzystaniu z państwowej służby zdrowia, a także pozwalają rządowi prowadzić krajową bazę danych ludności i na bieżąco informować posiadaczy samochodów o przysługujących im świadczeniach i uprawnieniach.

Do typowych zabezpieczeń stosowanych w dowodach tożsamości należą [5]:

a. Wzór giloszowy: dekoracyjny grawerunek w postaci skomplikowanego wzoru geometrycznego złożonego z cienkich linii ciągłych. Linie te są tworzone na podstawie zasad matematycznych, a ich zmienna krzywizna utrudnia kopiowanie wzoru. Wzór może składać się z linii, rozetek, krawędzi, elementów tła, elips i wielokątów. Za pomocą niewidocznych w świetle białym atramentów można też uzyskać różnokolorowe kombinacje;
b. Hologram: element zmienny optycznie. Jego niepowtarzalne właściwości optyczne uwidaczniają się na zasadzie dyfrakcji światła, w wyniku której powstaje efekt trójwymiarowy. W zależności od kąta patrzenia hologram może sprawiać wrażenie uginania promieni świetlnych pod różnymi kątami. Hologram zabezpiecza przed kserowaniem, utrudniając kopiowanie za pomocą drukarki czy kserografu. Można go dostosować za pomocą nano- i mikrodruku, mikroobrazów czy obrazów odczytywalnych laserowo. Uzyskane w ten sposób hologramy dzieli się na odbite i transmitowane – w zależności od techniki naświetlania stosowanej do wizualizacji obrazu [5];
c. Mikrodruk/mikrotekst: bardzo drobny (wysokość 0,15–0,30 mm) tekst, symbol lub kształt, którego nie można dostrzec gołym okiem, bez powiększenia. Za względu na trudność kopiowania stosowany jest głównie w celu zapobiegania kserokopiowaniu. Ta cecha zwiększa skuteczność hologramu i nitek zabezpieczających. Mikrodruk dzieli się na dwa typy: mikrodruk w pozytywie – ciemne litery na jasnym tle – i w negatywie – jasne litery na ciemnym tle;
d. Obraz dodatkowy i obraz widmo – znajdują się na stronie dokumentu z danymi osobowymi. Są to obrazy mniejsze bądź o wyróżniającym się rozmiarze, naniesione tą samą lub inną techniką niż właściwy wizerunek posiadacza. Przykładowymi technikami mogą być: stosowanie grawerunku laserowego do nanoszenia obrysu na papier lub podłoże polimerowe, użycie układu holograficznego pozwalającego zobaczyć obraz dodatkowy pod odpowiednim kątem naświetlania. Obrazy widma są nanoszone atramentami niewidocznymi w świetle białym, również techniką grawerunku laserowego. Obraz można nanieść na dokument wielokrotnie za pomocą technik, których zastosowanie umożliwi jego wizualizację w świetle UV;
e. Kod QR: mozaika złożona z czarnych i białych kwadratów przeznaczona do odczytu maszynowego i służąca przechowywaniu informacji związanych z dokumentem. Podpis cyfrowy generowany przez kod QR jest bardzo bezpieczny, a prawdziwość informacji w nim zawartych można z łatwością sprawdzić;
f. Kod kreskowy: zestaw linii lub prostokątów o różnej szerokości, ułożonych w określonej kolejności i zawierających informacje graficzne. Bezpieczeństwo kodu kreskowego można zwiększyć, dodając luminescencję UV lub atrament magnetyczny. Zakodowane informacje odczytuje się specjalnymi urządzeniami. Kody kreskowe dzielą się na liniowe, tj. kodowane i odczytywane w jednym kierunku, i dwuwymiarowe, tj. kodowane i odczytywane zarówno w pionie, jak i w poziomie;
g. Wbudowany układ mikroprocesorowy: zaszyfrowany czip mikroprocesorowy używany do przechowywania, odbierania i przesyłania danych. Użytkownik odczytuje dane, umieszczając czip pod czytnikiem lub skanerem;
h. Wzór tła: typu obrazu lub dekoracyjnego wzoru, widoczny pod właściwymi danymi i innymi zabezpieczeniami. Zapobiega próbom zmiany i usunięcia tekstu, obrazów czy znaków znajdujących się na powierzchni dokumentów, ponieważ próby takich działań kończą się uszkodzeniem wzoru. Wzór tła uzyskuje się różnymi technikami, na przykład: drukiem offsetowym, polegającym na przenoszeniu tuszu na docelową powierzchnię z płyty drukowej za pośrednictwem cylindra offsetowego z gumowym obciągiem; drukiem Orłowa, w którym podzielone kolorami płyty

drukarskie przenoszą tusz najpierw na pojedynczą płytę, a następnie na docelową powierzchnię – każde pociągnięcie powoduje intensywną zmianę koloru; oraz drukiem tęczowym, w którym kolory mieszają się stopniowo. Wzór tła składa się z mikrotekstu (mikrodruku), jednokolorowych kształtów, linii o różnej grubości dających złudzenie trójwymiarowości, giloszy lub elementów zapobiegających kopiowaniu;.

i. Atrament zmienny optycznie: nazywany również atramentem zmieniającym barwę, ponieważ zmienia on kolor w zależności od kąta widzenia, a także kąta oświetlenia i grubości zastosowanej warstwy dielektrycznej. Składa się z dwóch warstw odbijających: dolnej – metalicznej oraz powierzchniowej – przezroczystej, metalicznej warstwy dielektrycznej (MgF2) pokrytej nieprzezroczystymi i bezbarwnymi pigmentami. Obie warstwy częściowo odbijają światło białe. Interferencja w połączeniu z serią wielokrotnych odbić pozwala uzyskać wybiórcze pochłanianie fal, a co za tym idzie – widoczny dla człowieka kolor;
j. Wytłaczanie: wytłaczanie na sucho polega na odkształcaniu podłoża pod wpływem ciśnienia, ciepła bądź obu tych czynników w zależności od tego, czy podłoże jest wykonane z papieru czy polimeru. Powstaje w ten sposób relief wklęsły lub wypukły. Wizualizacja jest możliwa w świetle ukośnym lub przesuwanym. Wytłaczanie można również połączyć z nanoszonym na sucho atramentem zmiennym optycznie w celu wytworzenia tła pod inny obraz;
k. Odcisk palca: graficzne odwzorowanie na powierzchni dokumentu linii papilarnych z opuszków palców jego posiadacza. Ze względu na niepowtarzalność, trwałość i powszechność linie papilarne są znakomitym narzędziem biometrycznym;
l. Obraz wielowarstwowy: obraz złożony, powstający z wielu obrazów wyjściowych. Nakłada się go technologią soczewkową, tj. za pomocą soczewek i grawerowania laserowego, którym wytłacza się warstwy na podłożu polimerowym. Na obrazach wyjściowych, pociętych na paski i połączonych w obraz złożony, zapisuje się dane osobowe. Uzyskany w ten sposób obraz wielowarstwowy daje złudzenie głębi. Może też wykazywać różne właściwości w zależności od kąta patrzenia;
m. Elementy nanoszone atramentem wykazującym fluorescencję w świetle UV: atrament taki zawiera luminofory, tj. atomy jego grupy funkcyjnej, dające mu właściwości luminescencyjne. Pod wpływem światła UV o określonej długości fali (250–380 nm) luminofory świecą wielobarwnym światłem;
n. Zabezpieczenia przed kserowaniem: składają się ze wzorów i elementów tworzących tło chroniące przed skanowaniem i kserowaniem. Na zeskanowanym bądź skserowanym dokumencie pojawia się słowo „kopia" lub „nieważne", które na oryginale nie jest widoczne gołym okiem. Tekst może wyglądać np. jak linie w kolorach tęczy albo różnobarwne paski;
o. Druk tęczowy: metoda drukarska wykorzystująca pojemnik na atrament, w którym poszczególne kolory oddzielone są od siebie płytkami. Kolory mieszają się ze sobą, tworząc symbol albo wzór.

Materiał i metody

Materiały

Poniżej omówiono dowody tożsamości stosowane w porównywanych krajach – Indiach, Brazylii, Afryce Południowej, Malezji i Filipinach.

Indie: karta Aadhaar

Karta *Aadhaar* zawiera niepowtarzalny, 12-cyfrowy kod dowodzący miejsca zamieszkania i tożsamości obywatela Indii. Jest wydawana zarówno dorosłym, jak i nieletnim, a także obcokrajowcom, którzy w Indiach spędzili ponad 182 dni w ciągu ostatnich 12 miesięcy. Karta *Aadhaar* wydawana jest przez Unique Identification Authority of India (UIDAI), statutowy organ indyjskiego Ministerstwa Elektroniki i Informatyki, który powołano w 2009 r. *Aadhaar* to największy na świecie system biometryczny. Tożsamość jest ustalana na podstawie danych demograficznych, takich jak imię i nazwisko, data urodzenia, płeć czy adres, oraz biometrycznych, tj. dziesięciu odcisków palców, skanów obu tęczówek i fotografii twarzy. Sama karta *Aadhaar* nie stanowi dowodu obywatelstwa. Inne aplikacje i dostęp do usług w Indiach, takie jak karta upoważniająca do przydziału żywności czy paszport, korzystają jednak z karty *Aadhaar* w celu ustalenia tożsamości, co powierdza jej przydatność. Karta ta jest również wymagana do wypełnienia zeznania podatkowego i złożenia wniosku o kartę PAN [6].

Nowe, plastikowe (wykonane z PVC) karty *Aadhaar*, wprowadzone w 2020 r., zawierają lepsze zabezpieczenia, w tym niewidzialne logotypy i hologramy, oraz ukryte dane chroniące prywatność informacji: na karcie widać tylko ostatnie cztery cyfry niepowtarzalnego numeru. Pozostałe cyfry w karcie e-Aadhaar są ukryte pod literami „x" [7].

Brazylia: Cédula de Identidade

Brazylijski dowód osobisty znany jest pod nazwą *Cédula de Identidade* (Karta Identyfikacyjna) lub, nieoficjalnie, *Carteira de Identidade Nacional* (Krajowy Dowód Tożsamości). Wyparł on *Registro Geral* (Rejestr Generalny) w 2022 r., który pozostaje jednak ważny do roku 2032. Wymiana dowodów na nowe była nieodpłatna, a nowy typ wprowadzono początkowo tylko w kilku stanach. Większość obywateli posiada dowód osobisty,

ponieważ dokumenty te wyrabiane są już dla nastolatków. O ile w Brazylii funkcjonują również inne dowody tożsamości, o tyle eksperci uznają brazylijski dowód osobisty za jeden z najbezpieczniejszych tego typu dokumentów na świecie [8].

Brazylijczycy posiadający numer płatnika podatków – niepowtarzalny jedenastocyfrowy numer zwany *Cadastro de Pessoas Físicas* (Rejestr Osób Fizycznych, CPF) – są uprawnieni do składania wniosku o dowód osobisty. Urząd wydaje go na podstawie aktu urodzenia, małżeństwa lub świadectwa naturalizacji. Typowo zawiera datę wydania, datę i miejsce urodzenia, CPF, herb, podpis oraz odcisk kciuka. Nowy typ dowodu będzie dostępny w postaci plastikowej karty, tradyjnego papierowego dowodu oraz e-karty. Dla ułatwienia odczytu danych będzie też oznaczony kodem QR [9].

Południowa Afryka: inteligentny dowód tożsamości

Obywatele oraz stali mieszkańcy Południowej Afryki posługują się inteligentnymi dowodami tożsamości w postaci karty, które zastąpiły wcześniejszą zieloną książeczkę identyfikacyjną z kodem kreskowym. Dowód jest obowiązkowy dla wszystkich osób, które ukończyły 16 rok życia. Po raz pierwszy wprowadzono go w 2013 r., a wnioski o jego wydanie początkowo składało się w miejsowych bankach. Później, aby ułatwić składanie wniosków osobom starszym, rząd uruchomił specjalny portal internetowy. Do 2018 r. wydano 5,5 miliona dowodów.

Inteligentny dowód tożsamości przechowuje dane biometryczne i osobowe, takie jak imię i nazwisko czy datę urodzenia. Wbudowany mikroprocesor pozwala na łatwy odczyt informacji o jego posiadzaczu i jest cyfrowo kompatybilny z każdym punktem uwierzytelniającym. Dowód taki eliminuje potrzebę posiadania wielu różnych dokumentów osobowych oraz przyspiesza kontrole bezpieczeństwa, rejestrację obywatelstwa i korzystanie z programów usług rządowych [10]. W użyciu są dwa typu dowodu: typ A jest przeznaczony dla osób z imieniem i nazwiskiem standardowej długości, a typ B – dla osób z długim imieniem i nazwiskiem [11].

Malezja: MyKad

Malezyjski dowód tożsamości jest znany jako *MyKad* (*Kad Pengenalan Malaysia*) – Malezyjska Karta Rozpoznawcza. Rząd wprowadził ją w 2001 r. jako metodę ustalania tożsamości obywateli w wieku 12 lat i starszych. Przedstawiona w niniejszym artykule przykładowa karta to zwykły model, przeznaczony do użytku ogólnopopulacyjnego. Stali mieszkańcy oraz służby policyjne i wojskowe otrzymują specjalne dowody tożsamości, przykładowo kartę *MyPR,* przeznaczoną dla mieszkańców. Wszystkie takie karty mają jednak podobne cechy. Malezja była pierwszym krajem na świecie, który wprowadził dowód tożsamości z wbudowanym mikroprocesorem zawierającym niezbędne dane biometryczne [12].

MyKad jest wydawana National Registration Department (NRD), a wnioski o wydanie składa się przez Internet. Karta zawiera niepowtarzalny numer składający się z 12 cyfr ułożonych w trzy grupy oddzielone od siebie myślnikami, zgodnie z wzorem: RRMMD-D-PB-###G. Pierwsza grupa odpowiada dacie urodzenia posiadacza dowodu, druga to kod miejsca urodzenia, a trzecia jest generowana komputerowo przez NRD [13].

Filipiny: PhilSysID

PhilSysID, dowód tożsamości stosowany w Filipinach, został wprowadzony w 2018 r. Wnioskodawcy są zobowiązani do przedstawienia akceptowanego przez rząd dokumentu z imieniem i nazwiskiem, fotografią i podpisem. Osobom poniżej 18 roku życia musi towarzyszyć opiekun prawny. Karta *PhilSysID* zawiera trwały dwunastocyfrowy numer identyfikacyjny, nazywany Numerem *PhilSys* (*PhilSys Number*, PSN) i nadawany każdemu obywatelowi. Wnioski o wydanie składa się przez Internet. Załączone do wniosku domunenty są natępnie sprawdzane przez urzędników w centrach rejestracyjnych, a po określonym czasie następuje wydanie karty. Ponieważ PSN jest poufny, do celów transakcji publicznych zabezpiecza się go innym kodem – Numerem Karty *PhilSys* (*PhilSys Card Number*, PCN). Karta *PhilSysID* zawiera pełne dane demograficzne i biograficzne jej posiadacza oraz podpisany cyfrowo kod QR [14].

Metody

W niniejszym badaniu zastosowano podejście jakościowe. Dane pozyskane ze źródeł drugiego i trzeciego stopnia (na podstawie obserwacji poczynionych na temat dokumentów bezpieczeństwa popartych już istniejącymi raportami, tekstami i artykułami przeglądowymi) pozwoliły na porównanie dokumentów tożsamości wydawanych w różnych krajach. Do zebranych danych zastosowano podejście indukcyjne w celu identyfikacji zagadnień, zjawisk oraz wzorców, a natępnie stworzenia ram koncepcyjnych. Powstałe w ten sposób obserwacje szczegółowe dały podstawę do uogólnienia wyników.

Wyniki i dyskusja

W tabeli 1 porównano zabezpieczenia w dowodach tożsamości stosowanych w pięciu badanych krajach.

Na liście znajdują się 22 typy zabezpieczeń. Z zamieszczonej tabeli wynika, że najmniej zabezpieczeń

zawiera brazylijski dowód tożsamości (8). Kolejne pozycje zajmują Indie (10), Malezja (12), Filipiny (12) i Południowa Afryka (14). Najpowszechniej występujące zabezpieczenia (stosowane w czterech albo pięciu krajach) to numer seryjny, fotografia, podpis, wzór tła i obraz widmo. Ten ostatni jest nieużywany tylko w Brazylii. Niektóre zabezpieczenia, takie jak kod kreskowy, obraz wielowarstwowy czy alfabet Braille'a, występują tylko w inteligentnym dowodzie tożsamości z Południowej Afryki. Wytłaczane logo stosują tylko Indie, ukryty obraz – tylko Filipiny, a zabezpieczenia przed kserokopiowaniem – tylko Malezja. Pozostałe zabezpieczenia wykazują umiarkowaną spójność, tj. są używane przez 2–3 kraje. Można je więc uznać za kluczowe elementy dokumentów osobistych. Obejmują one grawerowanie dotykowe lub laserowe, hologram, wzór giloszowy, kod QR, mikrotekst, optycznie zmienny atrament lub urządzenia zmienne optycznie, odcisk palca, elementy czułe na światło UV, pieczęć lub emblemat czy mikroprocesor. Karty identyfikacyjne używane w Południowej Afryce, Malezji i Brazylii zawierają mikroprocesor pozwalający z łatwością przekształcić je w karty cyfrowe i wirtualne, co zmniejsza ryzyko oszustwa lub kradzieży. W tabeli 2 przedstawiono rozkład liczbowy zabezpieczeń w dokumentach pochodzących z pięciu badanych krajów.

Wnioski

Jak powiedziano we wstępie, większość zabezpieczeń można przypisać do jednego z trzech poziomów: zabezpieczenia łatwo widzialne, zabezpieczenia wymagające specjalnych metod, np. wizualizacji w świetle UV, oraz zabezpieczenia kryminalistyczne. Co interesujące, najwięcej z nich oraz najbardziej zaawansowanych zawierają dowody tożsamości w Południowej Afryce [14]. Po pierwsze tamtejsza karta ma poliwęglanowy rdzeń zawierający elementy chroniące przed fałszerstwem. Po drugie – dane biometryczne przechowywane w mikroprocesorze oraz klucz szyfrujący do identyfikacji pozwalają ustalić tożsamość właściciela bezdotykowo. Mimo że karta brazylijska zawiera najmniej zabezpieczeń, sama obecność mikroprocesora zarówno w jej starej, jak i nowej (cyfrowej) wersji to ważny element znacznie poprawiający bezpieczeństwo.

Potrzeba wykorzystania jak największej liczby odpowiednio zaawansowanych zabezpieczeń w celu uzyskania zamierzonego efektu staje się oczywista w obliczu możliwej kradzieży dokumentów osobowych czy fałszerstwa. Częstość fałszerstw jest bezpośrednio związana z liczbą prób nielegalnego użycia i procentowym udziałem kradzieży tożsamości w danym kraju. Na przykład w Południowej Afryce kradzież tożsamości za pomocą dokumentu naraża ofiarę na wysokie pożyczki zaciągnięte na jej nazwisko [15]. Malezyjski National Registration Department potwierdził 1047 przypadków użycia fałszywej karty tożsamości w okresie od 1990 do 2013 roku [16]. W Brazylii udział nielegalnego użycia dokumentów tożsamości sięga 37,5%, a 55 milionów Filipińczyków jest narażonych na utratę swoich danych. Z kolei w Indiach 6% prób uwierzytelnienia za pomocą linii papilarnych przechowywanych na karcie *Aadhaar* kończy się niepowodzeniem. Co więcej, do 2020 r. rząd unieważnił 40 955 sfałszowanych numerów kart *Aadhaar*.

Zaradzić wyżej wymienionym problemom można na dwa sposoby:

a. Stosując więcej dobrej jakości zabezpieczeń o bardziej zaawansowanych technologicznie strukturze i metodzie użytkowania;
b. Wprowadzając odpowiednie kary za fałszowanie dokumentów tożsamości.

W odniesieniu do samych zabezpieczeń dokument tożsamości stosowany w Estonii uchodzi za najbardziej zaawansowany i rozbudowany. Dokument zawiera czip przechowujący wbudowane pliki, kolorową fotografię, kod QR, drugi obraz widoczny tylko pod odpowiednim kątem oraz 2048-bitowy publiczny klucz szyfrujący, pozwalający bezproblemowo korzystać z dokumentu w środowisku elektronicznym. Kartę opracowano w gruniu 2018 r. dzięki współpracy pomiędzy światowymi ekspetami a estońskimi instytucjami rządowymi, w tym Estońskim Instytutem Nauk Sądowych i fundacją Enterprise Estonia. Karta ta może być wzorem dla innych krajów zmierzających do usprawnienia zabezpieczeń stosowanych w dokumentach tożsamości. We wszystkich z pięciu analizowanych krajach karą za fałszerstwo dokumentów jest grzywna i ograniczenie wolności na okres od 2 do 10 lat. O ile nielegalna imigracja do państw takich jak Estonia jest ograniczona, o tyle w krajach rozwijających się zjawisko to występuje na szeroką skalę – Indie i Brazylia pod tym względem znajdują się w pierwszej dziesiątce pośród krajów na całym świecie. Poprawa bezpieczeństwa narodowego w krajach rozwijających się wymaga zatem ulepszenia dowodów tożsamości – stanowi to ważny element bezpieczeństwa zarówno osobistego, jak i państwowego, ponieważ pozwoli zmniejszyć skalę nielegalnej imigracji, podszywania się i kradzieży tożsamości. Nieposiadanie niezbędnego dokumentu bezpieczeństwa wiąże się z tym, że dana osoba jest nielegalnym imigrantem lub oszustem. W przypadku gdy dokument bezpieczeństwa lub dowód tożsamości jest związany z obywatelstwem kraju, osoba nieposiadająca go nie będzie uważana za część prawdziwej populacji. Dokument tożsamości zatem to środek prawny, który potwierdza przynależność posiadacza do przestrzegającej prawa części ludności.

Perspektywy na przyszłość

O przyszłości dokumentów osobistych zadecyduje rozwój zaawansowanych zabezpieczeń i związanych z nimi usług. Biorąc pod uwagę analizowane kraje, od Malezji, która pierwsza wprowadziła dowód tożsamości z chipem komputerowym, biometrią odcisków palców i identyfikacją fotograficzną, po Filipiny, gdzie złożono ponad 75 milionów wniosków o krajowy dowód tożsamości, konieczność ustanowienia bezpieczniejszego i bardziej rozbudowanego krajowego systemu ustalania tożsamości staje się w perspektywie globalnej jeszcze bardziej złożona.

Wykorzystanie postępu technologicznego do opracowania systemu identyfikacji w Południowej Afryce zaowocowało stworzeniem uniwersalnej karty z mikroprocesorem do cyfrowego ustalania tożsamości i uwierzytelniania. Brazylia również znacznie ulepszyła swoje dowody tożsamości, udostępniając je w formacie cyfrowym za pośrednictwem rządowej aplikacji oraz wprowadzając kod QR, dzięki któremu autentyczność karty można sprawdzić w dowolnym momencie [17]. W Indiach przyszłość zabezpieczeń stosowanych w karcie *Aadhaar* zapowiada się optymistycznie. Wicedyrektor UIDAI przekonuje, że karta niedługo uzyska biometryczny system blokowania i odblokowywania, zapobiegający dostępowi osobom nieupoważnionym w razie jej zgubienia lub kradzieży. Wprowadzona zostanie też karta w formacie wirtualnym, co jeszcze bardziej zmniejszy ryzyko kradzieży. Co więcej, aby zwiększyć dostępność karty *Aadhaar*, tożsamość będzie też potwierdzana bez połączenia z siecią [18].

Przyszłość bezpiecznych dokumentów osobistych zależy obecnie od wprowadzenia takich zmian w krajach rozwiniętych czy szybko rozwijających się, ale także w krajach słabo rozwiniętych, które powinny opracować swoje systemy identyfikacji. Pozwoli to na poprawę ich własnej pozycji, jak i bezpieczeństwa na świecie.