BIOMETRIC PASSPORT

Monika Chaudhary[1], Sonali Rai[2]

[1,2]*Department of Electronics and Communication Engineering,*
RKGITW, Ghaziabad-201003, (India)

ABSTRACT

A biometric passport, also known as an e-passport, ePassport or a digital passport is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travellers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or centre page, of the passport. This type of passport is believed to prevent forgery and make it faster and more secure for travellers to move between countries, but some argue that the use of RFID chips infringes on civil liberties. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

Keywords: Radio waves, RFID chip, Public Key Infrastructure (PKI), Contactless Chip, Microprocessor

I INTRODUCTION

A Biometric passport or an e-Passport contains an electronic chip. The chip holds the same information that is printed on the passport's data page: the holder's name, date of birth, and other biographic information. An e-Passport also contains a biometric identifier. All biometric passports have security features to prevent the unauthorized reading or "skimming" of data stored on the e-Passport chip. A biometric passport has intricately designed passport pages, complex watermarks and a data chip. This chip contains all crucial information related to the passport holder such as digital signature data, which helps in authenticating the passport. The biometrics are considered more personal and reliable than a passport photo or a PIN, as it uses personal traits such as facial or eye maps and fingerprints as primary identification features. These biometric features were accepted by The International Civil Aviation Organization (ICAO) after analyzing multiple other biometrics including retinal scan[1]. The currently standardized biometrics used for this type of identification system are facial recognition, fingerprint recognition, and iris recognition. These were adopted after assessment of several different kinds of biometrics including retinal scan also. Can this document solve all our past problems, fraud, illegal immigration, should we file each of us and exclude the ones who aren't? Would it help us fighting against terrorism?[2]

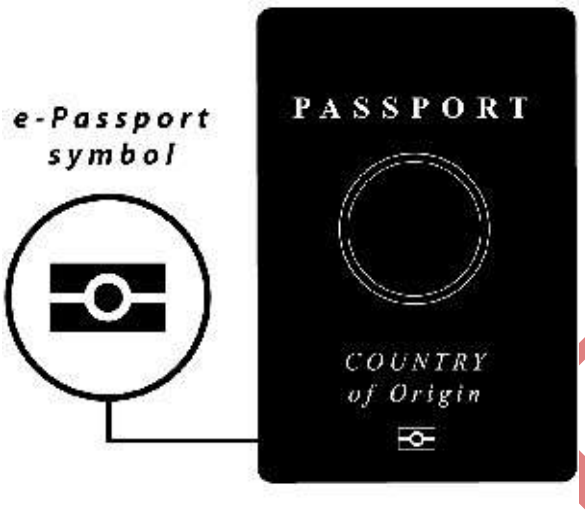

Fig 1: Symbol of Biometric Passport

II DESCRIPTION

Airport security has been one of the major issues of concern for most of the countries, especially considering the rising rate of militancy. Biometric technology has emerged as a powerful security support system to ensure access control at various public places[3]. Biometric passport is one of the most significant breakthroughs in the field, used to ensure a number of security aspects:

- Automated and secure immigration checks
- Detection of manipulated documents and information
- Identification and verification of the passport holder
- Avoidance of militancy attacks at the air terminals

2.1 Working of Biometric Passport

Biometric passports are based upon contact less smart card technology, making use of biometric identification. Biometric systems used for identification in biometric passports include fingerprint recognition, iris recognition and facial recognition. With biometric technology, the samples of an individual are stored on a microprocessor chip and used for electronic authentication in the future. Digital images of biometric features, including finger patterns and retina are stored in the identity register. To make it more secure, a number of access control features are integrated with a biometric passport:

- Random chip identifiers that too provide random chip identification number every time.
- Basic Access Control and Extended Access Control to encrypt the communication data between the passport chip and the chip reader.

- Active authentication to avoid duplication of chip and passive authentication to avoid alteration of chip data.

Standardization for biometric passports is provided by various organizations, including the International Civil Aviation Organization, ISO and IEC. As a result, the use of biometric passports has evolved as a great security alternative to prevent big threats in the aviation industry.[4,5,6]

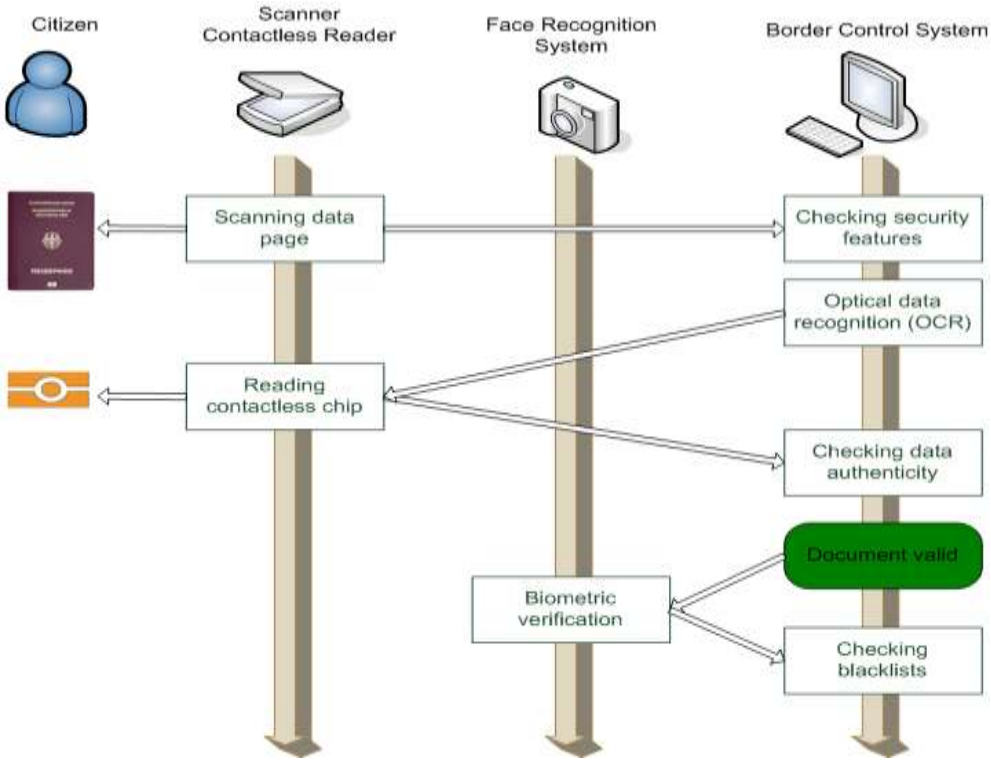

Fig 2: Inspection Process

2.2 Data Protection

Biometric passports are equipped with protection mechanisms to avoid and/or detect attacks:

- **Non-traceable chip characteristics**. Random chip identifiers reply to each request with a different chip number. This prevents tracing of passport chips. Using random identification numbers is optional.
- **Basic Access Control (BAC).** BAC protects the communication channel between the chip and the reader by encrypting transmitted information. Before data can be read from a chip, the reader needs to provide a key which is derived from the Machine Readable Zone: the date of birth, the date of expiry and the document number. If BAC is used, an attacker cannot (easily) eaves drop transferred information without knowing the correct key. Using BAC is optional.
- **Passive Authentication (PA).** PA prevents modification of passport chip data. The chip contains a file (SOD) that stores hash values of all files stored in the chip (picture, fingerprint, etc.) and a digital

signature of these hashes. The digital signature is made using a document signing key which itself is signed by a country signing key. If a file in the chip (e.g. the picture) is changed, this can be detected since the hash value is incorrect. Readers need access to all used public country keys to check whether the digital signature is generated by a trusted country. Using PA is mandatory.

- **Active Authentication (AA).** AA prevents cloning of passport chips. The chip contains a private key that cannot be read or copied, but its existence can easily be proven. Using AA is optional.
- **Extended Access Control (EAC).** EAC adds functionality to check the authenticity of both the chip (chip authentication) and the reader (terminal authentication). Furthermore it uses stronger encryption than BAC. EAC is typically used to protect fingerprints and iris scans. Using EAC is optional. In the EU, using EAC is mandatory for all documents issued starting 28 June 2009.
- **Shielding the chip.** This prevents unauthorized reading. Some countries – including at least the US – have integrated a very thin metal mesh into the passport's cover to act as a shield when the passport cover is closed.[7,8] The use of shielding is optional.

2.3 Comparison Between normal passport and biometric passport

Normal passport	Biometric passport
It does not have a microchip.	It contains a RFID chip.
Content of the passport can be changed.	Content of the chip cannot be changed.
No special identification is used.	It uses biometric identification.
There is no security of data when passport is lost.	Data is fully secured.

III CONCLUSION

It is expected that by 2015, ICAO would have a database of over a billion people worldwide. With a sudden rise in fraudulent methods, it has become mandatory for international security agencies to reinforce security features in passports. Therefore, a biometric passport helps in preventing the theft of identity and fraud. The ICAO suggests facial recognition as the principal biometric followed by iris and fingerprint recognition. The biometric information stored on passport helps in identifying fraud and automating immigration checks in future. E-Passports help to securely identify the traveller, provide protection against identity theft, protect privacy and make it difficult to alter a document. The biographic and biometric data contained in the electronic chip can be compared to both the traveller and the travel document being presented. There are multiple layers of security in the e-Passport process that prevent duplication. Thus it can be concluded that biometric passports are more secured, reliable, accurate, anti-theft then normal passports. These passports are accepted worldwide by most of the countries. India will become one of the biometric passport user very soon.

REFRENCES

[1] "ICAO Document 9303, Part 1, Volume 1 (OCR machine-readable passports)"(PDF). Retrieved 8 September 2010.

[2] "ICAO Document 9303, Part 1, Volume 2 (e-passports)" (PDF). Retrieved 8 September 2010.

[3] "Passport and visa". Swedavia. Retrieved 5 June 2010.

[4] Holger Funke: Automatic Border Control Systems (eGate) http://blog.protocolbench.org/2013/08/automatic-border-control-systems-egate

[5] "Fingerprinting Passports" (PDF). Retrieved 8 September 2010.

[6] Goodin, Dan (26 January 2010). "Defects in e-passports allow real-time tracking, The Register, Dan Goodin, 26th Jan 2010". Theregister.co.uk. Retrieved 8 September 2010.

[7] "Metal shields and encryption for US passports". Newscientist.com. Retrieved 8 September 2010.

[8] "Attacks on Digital Passports" (PDF). Retrieved 8 September 2010.