I. J. Computer Network and Information Security, **2013, 12, 80-90**
Published Online October 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.12.10

Design and Development of Biometrics Secure Person Detection System for E-Passport using Cryptographic Security Protocols

V.K. Narendira Kumar [1]
[1] Assistant Professor, Department of Information Technology,
Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
kumarmcagobi@yahoo.com

Dr. B. Srinivasan [2]
[2]Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
srinivasan_gasc@yahoo.com

Abstract — The biometric passports are to prevent the illegal entry of traveler into a specific country and limit the use of counterfeit documents by more accurate identification of an individual. This IC chip is integrated into the cover of a passport, called a biometric passport. Biometric Passports have been introduced in many countries to improve the security in Inspection Systems and enhance procedures and systems that prevent identity and passport fraud. The electronic passport is the privacy and security risks that arise by embedding with biometric technology. The goal of the adoption of the biometric passport is not only to expedite processing at border crossings, but also to increase security. Policymakers have put their faith in the technological promise of biometric identification because absolute identification could eliminate mismatched computer records and stolen identities.

Index Terms —Biometrics, Cryptographic, E-Passport, Face, Fingerprint, Palm print, Iris

I. INTRODUCTION

E-Passports herald a global revolution in the issuance of travel documents and identity management. Passport and identity inspection systems used by airlines and border control authorities at airports, harbors, and roadside country borders will be able to more precisely match documents to people, authenticate data in the documents, and more efficiently process travelers at checkpoints. The biometric passport also offers substantial benefits to the rightful holder by providing a more sophisticated means of confirming that the passport belongs to that person and that it is authentic, without jeopardizing privacy [1].

The states are currently issuing biometric passports, which corresponds to more than 50% of all passports being issued worldwide. This represents a great enhancement in national and international security as (1) it improves the integrity of passports by the need to match the information contained in the chip to the one printed in the document and to the physical characteristics of the holders; and (2) enables machine-assisted verification of biometric and biographic information to confirm the identity of travelers.

The biometric passport standard provides details about establishing a secure communication between a biometric passport and an Inspection System (IS), the authentication of a biometric passport, details on storage mechanisms and biometric identifiers that should be used [3]. The chip also includes an electronic copy of the bearer's photo. The digital photograph of the individual provides a facial biometric that can be used for automated identification processes by employing facial recognition technology. Most implementations of the biometric passports by various countries have a single identifier only, the facial biometric. But the chip has sufficient capacity to include extensions, such as face, fingerprints and iris biometrics.

The International Civil Aviation Organization has adopted a global, harmonized blueprint for the integration of biometric identification information into machine readable passports [2]. This study aims to find out to what extent the integration of biometric identification information into passports will improve their robustness against identity theft. The integration of biometrics can provide better verification performance than the individual biometrics. Biometrics will also increase robustness of the biometric systems against the spoofing attacks and solve the problem of non-universality. Since the facial image is the mandatory biometric identifier to be included in the future passports, the study focus on the use of the facial image and finger prints for the identity verification of passport holders. In order of least secure and least convenient to most secure and most convenient, they are:

- Something you **have** - card, token, key.

- Something you **know**- PIN, password.
- Something you **are** - biometric.

The remaining sections are organized as follows: Brief outline of biometric passport systems is presented in section 2. System methodology steps are mentioned in Section 3. The other phases of the biometric passport security, logical data structure and implementation of the system are briefly explained in section 4, 5 and 6. Experimental results are given in Section 7. Finally, Section 8 describes the concluding remarks.

II. Literature Survey

Juels *et al* (2005) discussed security and privacy issues that apply to e-passports. They expressed concerns that, the contact-less chip embedded in an e-passport allows the e-passport contents to be read without direct contact with an IS and, more importantly, with the e-passport booklet closed. They argued that data stored in the RIFD chip could be covertly collected by means of “skimming” or “eavesdropping”. Because of low entropy, secret keys stored would be vulnerable to brute force attacks as demonstrated by Laurie (2007). Kc and Karger (2005) suggested that an e-passport may be susceptible to “splicing attack”, “fake finger attack” and other related attacks that can be carried out when an e-passport bearer presents the e-passport to hotel clerks. There has been considerable press coverage (Johnson, 2006; Knight, 2006; Reid, 2006) on security weaknesses in e-passports. These reports indicated that it might be possible to “clone” an e-passport [3].

A. Purpose of the Study

The primary objective of the study is to produce new knowledge with respect to security of biometric techniques and RFID in an e-passport setting. The results of the work should be useful for those making e-passport design decisions with respect to RIFD security and biometric technologies in an e-passport setting.

B. Statement of the Problem

The purpose of biometric passports is to prevent the illegal entry of travelers into a specific country and to limit the use of fraudulent documents by more accurate identification of individuals. It is interesting to find out to what extent the integration of RFID and biometric identification information into passports will improve their robustness against identity theft.

III. Biometrics in E-Passports

Biometrics in e-passports complying with the ICAO standard consists of a mandatory facial image and fingerprints. While the former are used by a significant number of countries and thus information on them is widely available, the latter is currently used seldom. Therefore, this section only covers the vulnerabilities of facial images, fingerprints, palmprint and iris images.

A. Face Image

Facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a nonintrusive method and is suitable for covert recognition applications. The applications of facial recognition range from static ("mug shots") to dynamic, uncontrolled face identification in a cluttered background (subway, airport). Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. It is questionable if a face itself is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. Facial recognition system should be able to automatically detect a face in an image, extract its features and then recognize it from a general viewpoint (i.e., from any pose) which is a rather difficult task. Another problem is the fact that the face is a changeable social organ displaying a variety of expressions [4].

B. Fingerprint

A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.

C. Palmprint

The palmprint recognition module is designed to carry out the person identification process for the unknown person. The palmprint image is the only input data for the recognition process. The person identification details are the expected output value. The input image feature is compared with the database image features. The relevancy is estimated with reference to the threshold value. The most relevant image is selected for the person’s identification. If the comparison result does not match with the input image then the recognition process is declared as unknown person. The recognition module is divided into four sub modules. They are palmprint

selection, result details, ordinal list and ordinal measurement. The palmprint image selection sub module is designed to select the palmprint input image. The file open dialog is used to select the input image file. The result details produce the list of relevant palmprint with their similarity ratio details. The ordinal list shows the ordinal feature based comparisons. The ordinal measurement sub module shows the ordinal values for each region.

D. Iris Recognition

Iris recognition technology is based on the distinctly colored ring surrounding the pupil of the eye. Made from elastic connective tissue, the iris is a very rich source of biometric data, having approximately 266 distinctive characteristics. These include the trabecular meshwork, a tissue that gives the appearance of dividing the iris radically, with striations, rings, furrows, a corona, and freckles. Iris recognition technology uses about 173 of these distinctive characteristics. Iris recognition can be used in both verification and identification systems. Iris recognition systems use a small, high-quality camera to capture a black and white, high-resolution image of the iris. The systems then define the boundaries of the iris, establish a coordinate system over the iris, and define the zones for analysis within the coordinate system.

E. Biometric System Modules

Enrollment Unit: The enrollment module registers individuals into the biometric system database. During the phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

Feature Extraction Unit: The module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

Matching Unit: The module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one too many matching).

Decision Maker: The module accepts or rejects the user based on a security threshold and matching score.

IV. System Methodology

An e-passport bearer presents his/her document to a border security officer who scans the MRZ information in the e-passport through a MRZ reader and then places the e-passport near an e-passport reader to fetch data from the microchip [5]. The current implementation consists of three protocols:

- *Basic Access Control (BAC) protocol (optional):* It provides encrypted communication between the RIFD chip and the Inspection System (IS).
- *Passive Authentication (PA) protocol (mandatory):* A border security officer reads and verifies the authenticity of e-passport content stored in the RIFD chip [6].
- *Active Authentication (AA) protocol (optional):* It provides integrity verification of e-passport's data.

The two new protocols that intend to replace active authentication and thus now consists of the following four protocols:

- *Basic Access Control (BAC) protocol (mandatory):* It facilitates the e-passport and the IS to establish an encrypted communication channel.
- *Chip Authentication (CA) protocol (mandatory):* A mechanism to detect cloned e-Passports
- *Passive Authentication (PA) protocol (mandatory):* As in first generation passport standard.
- *Terminal authentication (TA):* Only if all protocols are completed successfully, the e-passport releases sensitive information like secondary biometric identifiers. The e-passport performs the collection of protocols as specified in the first generation e-passports, therefore providing backward compatibility [7].

A. Logical Data Structure

The ICAO issued a standardized data structure called Logical Data Structure (LDS) for the storage of data elements. This was to ensure that global interoperability for e-Passport Tags and Readers could be maintained. The specifications state that all the 16 data groups are write protected and can be written only at the time of issue of the e-Passport by the issuing state shown in table 1. A hash of data groups 1-15 are stored in the security data element, each of these hashes should be signed by the issuing state.

Table 1: Passport Logical Data Structure

Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Face biometrics
DG 4	Encoded Fingerprint biometrics
DG 5	Encoded Palm print biometrics
DG 6	Encoded Iris biometrics
DG 7	Displayed Portrait
DG 8	Reserved for Future Use
DG 9	Signature
DG 10	Data features
DG 11-13	Additional Details
DG 14	CA Public Key
DG 15	AA Public Key
DG 16	Persons to Notify
SDE	Security Data Element

V. Biometric Passport Security Goals

Researcher analyzes e-passport protocols by first identifying their security goals. Researcher assumes that a country implements the highest level of Cryptographic security and multiple biometrics for e-passports.

A. Data Confidentiality

Data confidentiality ensures the privacy of e-passport details and encryption is the common technique that provides confidentiality [11]. In the case of e-passport, encryption is used to create a secure channel between the e-passport reader and the microchip. Note that the cryptographic keys used for encryption have to be guarded against unauthorized access (data elements within the LDS or keys stored in the DF).

B. Data Integrity

Data integrity prevents against illegal modifications of information exchanged between the e-passport reader and the microchip. Also the DF, SOD and LDS should be secure against any unauthorized modifications, i.e., any data tampering should be easily detectable by the border security centre.

C. Data Authentication

Data origin authentication ensure that the source of the transmission in a protocol is authentic, i.e., the data on the RIFD chip should be bound to information on MRZ and to the data that appears in the e-passport bio-data page currently being examined by a border security officer.

D. Certificate Manipulation

Certificates acts as an off-line assurance from a trusted authority that the certified public key really does belong to the principal who is in possession of corresponding secret key. However, it is the responsibility of the protocol to validate that the corresponding secret key is actually held by the principal claiming ownership of the public key. The e-passport reader should have a guarantee that certificates presented by the e-passport are valid and match the data on the e-passport. ICAO has implemented a PKI which would store signature certificates from issuing state and organizations.

E. Security and Privacy Solutions

Cryptography can be applied to RFID to provide security and privacy. The problem of applying cryptography to RFID tags is that computation is required for encryption and decryption. This is a problem of low-cost RFID tags because it cannot run standard functions of cryptography [8]. Even symmetric key encryption cannot be executed in low-cost RFID. The research of Juels suggests minimalist cryptography so that cryptography can be applied to low-cost RFID tags [9]. Public key-based Basic Access Control for electronic passport is one of the first examples, which is deployed using RFID authentication [10]. Figure 1 shows biometric passport with RFID chip embedded.

Skimming: By using an embedded metallic element in the passports, it provides RF signal blocking. The RF blocking material covers the passport so that it only can be physically opened when it should be read.

Eavesdropping: Basic Access Control (BAC) minimizes the chance of skimming and eavesdropping. Initial interaction should be necessary between the RFID chip in the passport and the control reader which contain protocols that are for the secure communication channel. Once authentication is done successfully, the data from passport will be issued. If not, the passport declines the access of data content.

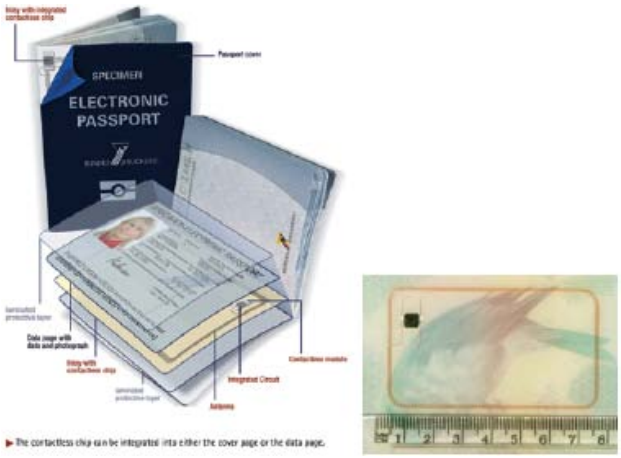

Figure. 1: The Biometric Passport Using RFID Chip.

Tracking: Unique Identifier (UID) is still possible to be tracked even though BAC is used. The solution of tracking is using a random UID (RUID). Embedded random number generator (RNG) generates a RUID.

Cloning: RFID chip can be copied, so it can be used for another electronic passport. By comparing the RIFD chip data and the data on electronic passports data page, it is possible to diminish of cloning. Using Public Key Infrastructure (PKI) is one of the ways to prevent cloning. PKI can be applied to the travel document, so that comparing the data between the RIFD chip and travel document. If the data is stored by authority, the data is not changed.

Temporary Deactivation: There is another way to protect personal privacy. By making RFID tags deactivate, privacy can be protected. One of the ways to deactivate is using Faraday cage which can block out external electrical fields. EPC global tags make enables to deactivate tags forever by using password-protected deactivate function. The tags which have temporary deactivation functions can be found in more expensive RFID tags [11].

VI. Radio Frequency Identification

A RFID chip is activated by a magnetic field from a reader and subsequently broadcasts the data that is stored in its memory. The fact that this personal information is being broadcast raises many questions about the use of this technology in such sensitive areas such as passports. It seems that contact chip technology would be preferable. However, the International Civil Aviation Organization (ICAO), the organization that developed the standards for electronic passports, analyzed these options and excluded contact chips from use in electronic passports. It was argued that contact chip technology, which is primarily used in card formats, would be difficult to put in a

passport style document. Also, because contact chip technology requires exposed areas that require precise contact points with a reader, it was postulated that a contact chip document would not be able to function for the entire ten-year lifespan of a passport. Therefore, a contactless chip technology, such as RFID is used in the electronic passports [12].

The two security concerns with the use of a RFID chip in an electronic passport are skimming and eavesdropping. Skimming is the act of reading the data on a chip without the holder's permission. Eavesdropping is when a party monitors the information in the communication between a chip and an authorized reader.

Due to the standardization of the RFID chips, the chip in an electronic passport can be read by commercially available readers. While this standardization is essential for international customs agents to be able to read any passport, it also makes it possible for anyone to potentially obtain a reader and "skim" the information from an electronic passport. The State Department proposes to address this problem by placing an "anti-skimming" material in the cover and spine of the passport. This material will shield the RFID chip when the passport is closed, mitigating the threat of skimming. Therefore, a person must physically open the passport booklet for it to be read.

Although the ICAO technical specifications for the use of contactless chips in passports claims that it is not possible to read an RFID chip from a distance greater than ten centimeters, critics argue that eavesdropping is possible from as much as 60 feet away. To protect against eavesdropping, the Department of State proposes to shield the reader area in customs checkpoints, so no transmissions will be detected by anyone nearby. Also, the proposed system involves a unique identifier to implement Basic Access Control (BAC) in order to keep passport information from being revealed to an unauthorized party.

VII. Implementation of the System

In order to implement this electronic passport system using cryptographic security and multiple biometrics technology efficiently, ASP.NET program is used. This program could speed up the development of this system because it has facilities to draw forms and to add library easily. There are three ways of doing authentication and authorization in ASP.NET:

Windows Authentication: In this methodology ASP.NET web pages will use local windows users and groups to authenticate and authorize resources.

Forms Authentication: This is a cookie based authentication where username and password are stored on client machines as cookie files or they are sent through URL for every request. Form-based authentication presents the user with an HTML-based Web page that prompts the user for credentials.

Passport Authentication: Passport authentication is based on the passport website provided by the asp.net. So when user logins with credentials it will be reached to the passport website where authentication will happen. If Authentication is successful it will return a token to your website.

Anonymous Access: If you do not want any kind of authentication then you will go for Anonymous access.

Researcher model the flow of e-passport protocol according to the following stages: When an e-passport is presented at a border security checkpoint, the RIFD chip and the e-passport reader execute the BAC protocol, in order to establish a secure (encrypted) communication channel between them. On successful completion of PA the RIFD chip and the e-passport reader execute the AA protocol.

A. On-line Secure E-Passport Protocol

To resolve the security issues identified in both the first- and second-generation of e-Passports, in this section, we present an on-line secure e-Passport protocol (OSEP protocol). The proposed protocol leverages the infrastructure available for the standard non-electronic passports to provide mutual authentication between an e-Passport and an IS. Currently, most security organizations are involved in passive monitoring of the border security checkpoints. When a passport bearer is validated at a border security checkpoint, the bearer's details are collected and entered into a database. The security organization compares this database against the database of known offenders (for instance, terrorists and wanted criminals).

The on-line secure e-Passport protocol provides the following security features: An e-Passport discloses its information stored on the e-Passport RIFD chip only after a successful authentication of the IS (Inspection System). This prevents revealing the e-Passports identity to a third party that is not authorized or cannot be authenticated. This prevents the covert collection of e-Passport data from 'skimming' or 'eavesdropping' attacks that were very effective against both the first- and the second-generation e-Passports.

- The OSEP protocol uses the existing ICAO PKI implementation (as in first generation e-Passports) and eliminates the need for cross-certification among the participating countries, as required by the EAC (second-generation e-Passports).
- The OSEP protocol eliminates the need for certificate chain verification by an e-Passport. Only the top level certificate ($CERT_{CVCA}( )$) is required to be stored in an e-Passport, thus reducing the memory requirements and preventing a malicious reader from performing a DOS attack on an e-Passport.
- The OSEP protocol also requires an IS to provide proof-of-correctness for public key parameters to an e-Passport. This allows an e-Passport to verify that an IS is using the correct domain parameters and to prevent related attacks.

B. Biometric Passport Initial Setup

All entities involved in the protocol share the public quantities p, q, g where:

- *p* is the modulus, a prime number of the order 1024 bits or more.

- q is a prime number in the range of 159 -160 bits.
- g is a generator of order q, where $Ai < q$, $g^i \neq 1 \bmod p$.
- Each entity has its own public key and private key pair (PK_i, SKi) where $PK_i = g^{(SK)}_i \bmod p$.
- Entity i's public key (PK_i) is certified by its root certification authority (j), and is represented as $CERT_j$ (PK_i, i).
- The public parameters p, q, g used by an e-Passport are also certified by its root certification authority.

C. Phase One – Inspection System Authentication

Step 1 (IS) When an e-Passport is presented to an IS, the IS reads the MRZ information on the e-Passport using an MRZ reader and issues the command GET CHALLENGE to the e-Passport RIFD chip.

Step 2 (P) The e-Passport RIFD chip then generates a random eP £ $_R$ $1 \leq eP \leq q - 1$ and computes $K_{eP} = g^{eP} \bmod p$, playing its part in the key agreement process to establish a session key. The e-Passport replies to the GET CHALLENGE command by sending K_{eP} and its domain parameters p, q, g.

$$eP \rightarrow IS: K_{eP}, p, q, g$$

Step 3 (IS) On receiving the response from the e-Passport, the IS generates a random IS £$_R$ $1 \leq IS \leq q - 1$ and computes its part of the session key as $K_{IS} = g^{IS} \bmod p$. The IS digitally signs the message containing MRZ value of the e-Passport and K_{eP}.

$$S_{IS} = SIGN_{SKIS} (MRZ \parallel K_{eP})$$

It then contacts the nearest DV of the e-Passports issuing country and obtains its public key. The IS encrypts and sends its signature S_{IS} along with the e-Passport's MRZ information and K_{eP} using the DV's public key PK_{DV}.

$$IS \rightarrow DV: ENC_{PK\,DV} (S_{IS}, MRZ, K_{eP}), CERT_{CVCA} (PK_{IS}, IS)$$

Step 4 (DV) The DV decrypts the message received from the IS and verifies the $CERT_{CVCA}$ (PK_{IS}, IS) and the signature S_{IS}. If the verification holds, the DV knows that the IS is genuine, and creates a digitally-signed message S_{DV} to prove the IS's authenticity to the e-Passport.

$$SDV = SIGN_{SKDV} (MRZ \parallel K_{eP} \parallel PK_{IS}), CERT_{CVCA} (PK_{DV}, DV)$$

The DV encrypts and sends the signature S_{DV} using the public key PK_{IS} of IS.

$$DV \rightarrow IS: ENC_{PKIS} (S_{DV}, [PK_{eP}])$$

The DV may choose to send the public key of the e-Passport if required. This has an obvious advantage, because the IS system now trusts the DV to be genuine. It can obtain a copy of e-Passport's PK to verify during e-Passport authentication.

Step 5 (IS) After decrypting the message received, the IS computes the session key $K_{ePIS} = (K_{IS})^{eP}$ and encrypts the signature received from the DV, the e-Passport MRZ information and K_{eP} using K_{ePIS}. It also digitally signs its part of the session key K_{IS}.

$$IS \rightarrow eP: K_{IS}, SIGN_{SKIS} (K_{IS}, p, q, g), ENCK_{ePIS} (S_{DV}, MRZ, KeP)$$

Step 6 C On receiving the message from the IS, the e-Passport computes the session key $K_{ePIS} = (K_{IS})^{eP}$. It decrypts the message received using the session key and verifies the signature SDV and $VERIFY_{PKIS}$ ($SIGN_{SKIS}$ (K_{IS}, p, q, g)). On successful verification, the e-Passport is convinced that the IS system is genuine and can proceed further in releasing its details. All further communications between an e-Passport and IS are encrypted using the session key K_{ePIS}.

D. Phase Two - e-Passport Authentication

Step 1 C The IS issues an INTERNAL AUTHENTICATE command to the e-Passport. The e-Passport on receiving the command, the e-Passport creates a signature $S_{eP} = SIGN_{SKeP}$ ($MRZ \parallel K_{ePIS}$) and sends its domain parameter certificate to the IS. The entire message is encrypted using the session key K_{ePIS}.

$$eP \rightarrow IS: ENCK_{ePIS} (S_{eP}, CERT_{DV} (PK_{eP}), CERT_{DV} (p, q, g))$$

Step 2 (IS) The IS decrypts the message and verifies $CERT_{DV}$ (p, q, g), $CERT_{DV}$ (PK_{eP}) and S_{eP}. If all three verifications hold then the IS is convinced that the e-Passport is genuine and authentic.

During the IS authentication phase, and IS sends the e-Passport's MRZ information to the nearest e-Passport's DV, which could be an e-Passport country's embassy. Embassies are DV's because they are allowed to issue e-Passports to their citizens and because most embassies are located within an IS's home country, any network connection issues will be minimal, Because the embassy now has a list of all its citizens that have passed through a visiting country's border security checkpoint. We do not see any privacy implications, because, in most cases, countries require their citizens to register at embassies when they are visiting a foreign country.

VIII. Experimental Results

The successful design, deployment and operation of biometric passport systems depend highly on the results for existing biometrical technologies and components. These existing technologies as well as new solutions need to be evaluated on their passport system performance. An RFID chip will be embedded into the back cover of the passport. However it is often forgotten that the biometric face, finger, iris, and palm prints is only one part of a fully deployed application. As biometric (sub) systems are often not designed with security and or privacy in mind, system integrators will need to address the requirements of the deployed application in this light. The fears and concerns of a significant segment of the user population need to be addressed as early as possible in the design process, to ensure that appropriate mechanisms are in place to reassure such users. These concerns may relate to privacy or to safety issues, which may be addressed in part

through legal and regulatory measures. This article discusses the requirements, design and application scenarios of biometrical systems in general and the introduction of a new biometrical passport in particular.

The e-passport authentication system is divided into enrollment module and authentication module. The passport users who are included in the enrollment module are e-passport holder, Immigration administrator. Figure 2 shows the enrollment module in the e-passport authentication architecture design.

The applicant's biometric template(s) generated by the enrolment process can be searched against one or more biometric databases (identification) to determine whether the applicant is known to any of the corresponding systems (for example, holding a passport under a different identity, criminal record, holding a passport from another state).

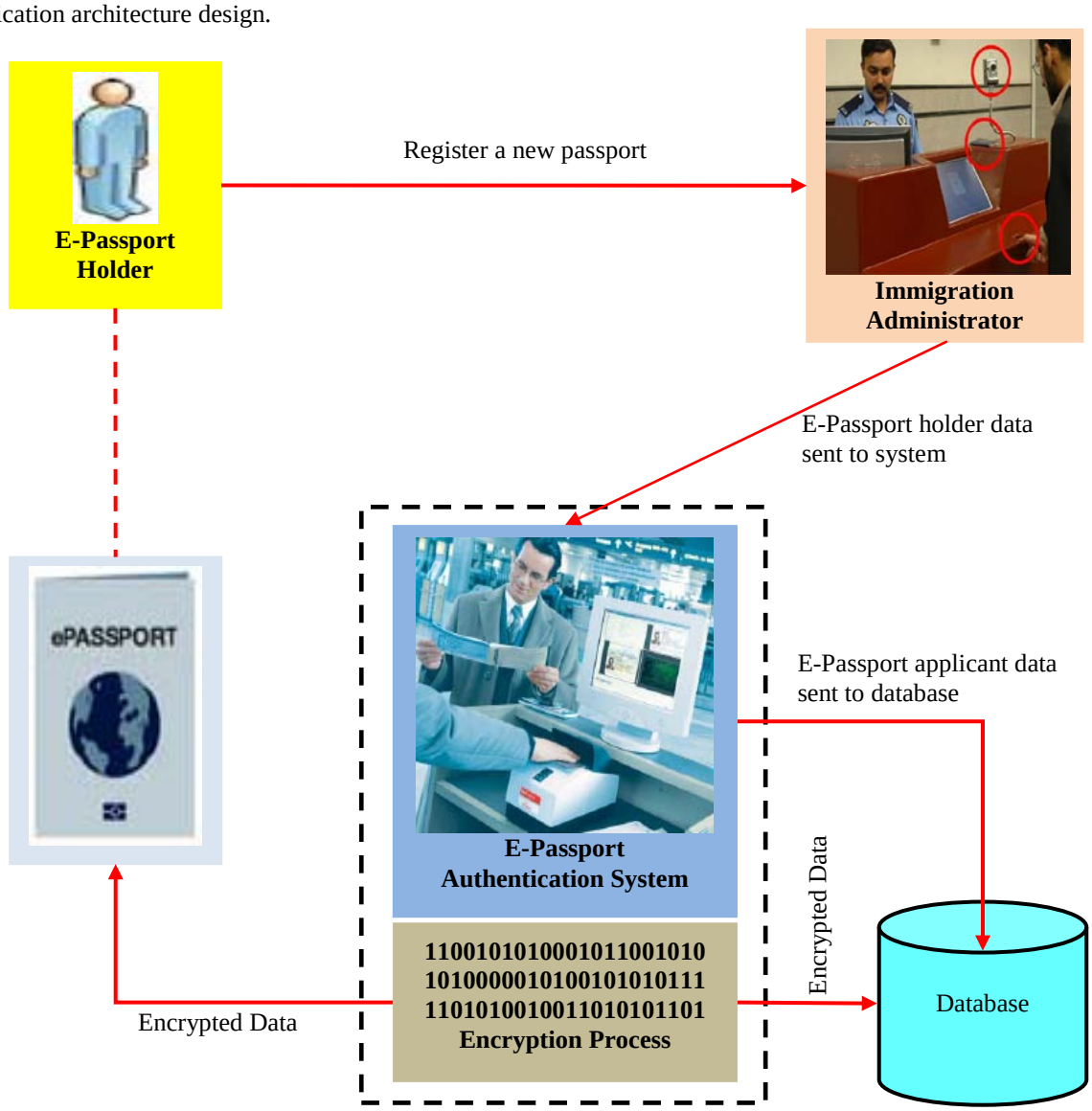

Figure. 2: Enrollment Module of E-Passport Authentication Architecture

When the applicant collects the passport (or presents them for any step in the issuance process after the initial application is made and the biometric data is captured) their biometric data can be taken again and verified against the initially captured template .

The identities of the staff undertaking the enrolment can be verified to confirm they have the authority to perform their assigned tasks. This may include biometric authentication to initiate digital signature of audit logs of various steps in the issuance process, allowing biometrics to link the staff members to those actions for which they are responsible.

Each time traveler (i.e. MRTD holders) enters or exit a State, their identities can be verified against the images or templates created at the time their travel documents were issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any Advance Passenger Information (API) system. Ideally, the biometric template or templates should be stored on the

travel document along with the image, so that travelers' identities can be verified in locations where access to the central database is unavailable or for jurisdictions where permanent centralized storage of biometric data is unacceptable.

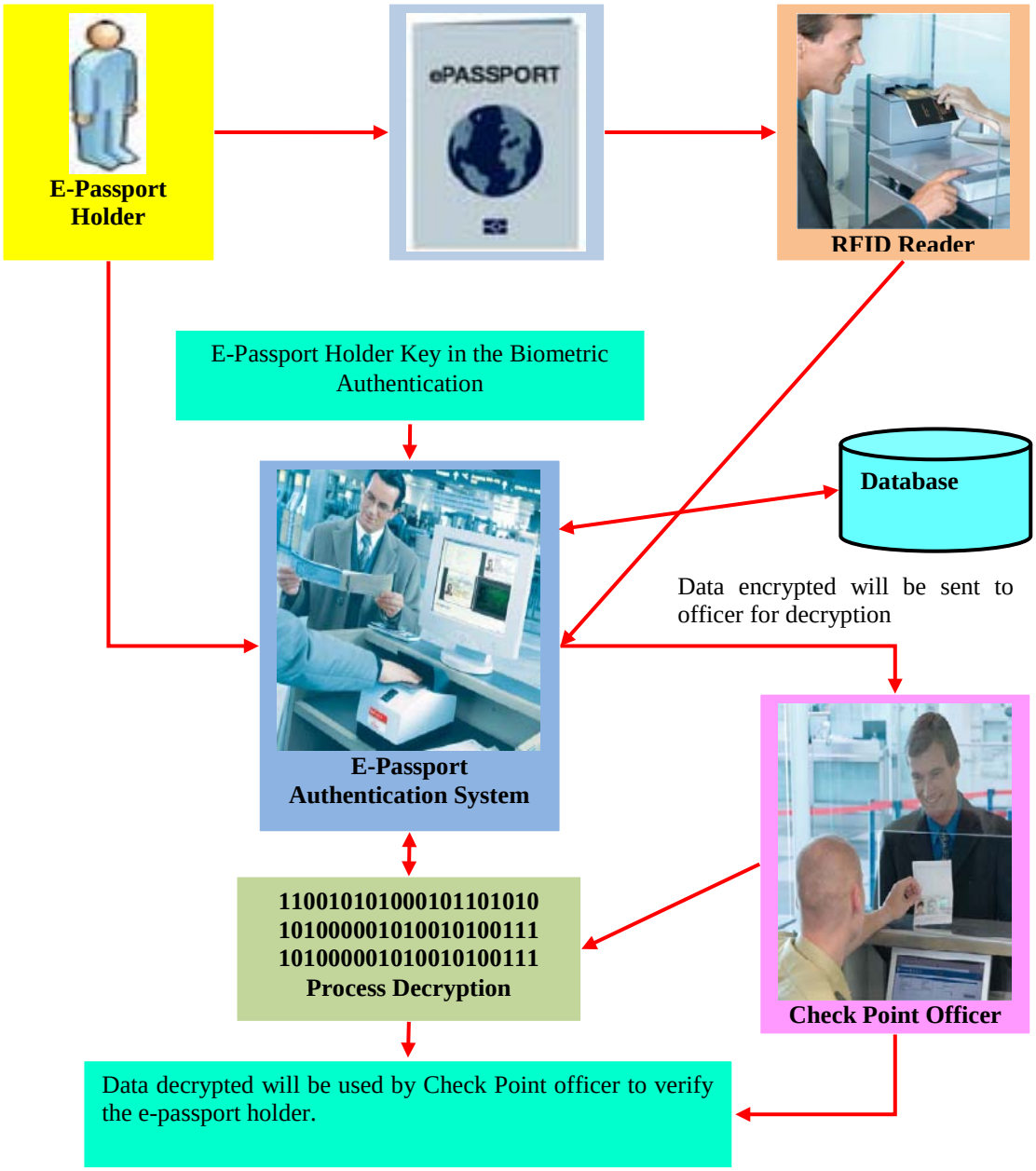

Figure. 3: Authentication Module of E-Passport Authentication Architecture

Two-way check - The traveler's current captured biometric image data, and the biometric template from their travel document (or from a central database), can be matched to confirm that the travel document has not been altered.

Three-way check - The traveler's current biometric image data, the image from their travel document, and the image stored in a central database can be matched (via constructing biometric templates of each) to confirm that the travel document has not been altered. This technique matches the person, with their passport; with the database recording the data that was put in that passport at the time it was issued.

Four-way check - A fourth confirmatory check, albeit not an electronic one, is visually matching the results of the 3-way check with the digitized photograph on the Data Page of the traveler's passport.

Besides the enrolment and border security applications of biometrics as manifested in one-to-one and one-to-many matching, States should also have regard to, and set their own criteria, in regard to:

Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint, or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO-standardized biometric image and/or template, Receiving States must select their own

biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters.

The e-passport holder registers to the system by providing the personal data and some important documentation to the immigration officer. After that, Immigration Administrator will make the enrollment for the e-passport holder by filling the data into the enrollment system. After enrollment process, the data of the e-passport holder will be encrypted by proposed cryptography technique and stored into immigration database and RFID tag inside the e-passport. Besides that, Enrollment module also includes the modifying process and deleting process. Modifying process will be carried out if there was a special request from e-passport holder to change the information of the e-passport, the e-passport spoil, or finished pages. Deleting process will be carried out if the previous e-passport validation date was expired or the e-passport holder lost their passport. They have to register a new e-passport in order to get an e-passport again.

The passport user involve in the authentication module are e-passport holder and check point officer. When e-passport holder arrives to check point, e-passport holder will put the e-passport onto RFID reader, and a signature required key in by e-passport holder so that authentication process can be performed to verify an e-passport holder. After authentication process authenticated the e-passport holder, RFID reader will read the encrypted data which was stored inside the RFID tag in e-passport. The encrypted data will be sent to the system to match with the encrypted data in the database system. If the encrypted data in the e-passport match with the encrypted data which is stored inside the database during enrollment process, the encrypted data in the e-passport will be decrypted by a certain key [13]. Then the check point officer has to check and verify the identity of the e-passport holder. Figure 3 shows the authentication module in the e-passport authentication architecture design.

The attributes inherent in the e-Passport provide a here to fore unavailable means of improving the security of the international travel system. These are described below under three general categories: preventing the use of multiple identities; linking the bearer to the document in a traditional border operations environment; and serving as a strong token to drive a biometric identification process. After these uses have been explored in some detail, the paper will examine why the e-Passport may not be universally accepted by states as the sole device used to fully automate the border clearance process for registered participants as envisioned by the process flow.

Accuracy of the biometric matching functions of the system. Issuing States must encode one or more facial, fingerprint, palm print or iris biometrics on the MRTD as per LDS standards (or on a database accessible to the Receiving State). Given an ICAO standardized biometric image and/or template, receiving States must select their own biometric verification software, and determine their own biometric scoring thresholds for identity verification acceptance rates – and referral of imposters [14].

Every type of biometric measurement can be classified with a number of characteristics that should be considered in a selection process see table II. Being familiar with these characteristics will help you to better understand how to think objectively about each type. Sure, some of the available biometric technologies are cool, but it's no longer we have to make *rational* decisions about purchasing and using technology.

Table II: Comparison of Biometric Technologies

Technology	Face	Finger	Iris	Palm
How it works	Captures and compares facial patterns	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares dimensions of palm
Enrollment time	About 3 minutes	3 minutes, 30 Seconds	2 minutes, 15 seconds	About 1 minute
Transaction time	10 seconds	9 to 19 seconds	12 seconds	6 to 10 seconds
False non-match rate	3.3% – 70%	0.2% – 36%	1.9% – 6%	0% – 5%
False match rate	0.3% – 5%	0% – 8%	Less than 1%	0% – 2.1%
User acceptance issues	Potential for privacy misuse	Associated with law enforcement, hygiene concerns	User resistance, use difficulty	Hygiene concerns
Factors affecting Performance	Lighting, orientation of face, and sunglasses	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Hand injuries, arthritis, swelling
Variability with age	Affected by aging	Stable	Stable	Stable

Universality: This refers to whether each person has the characteristic being measured. For instance, nearly everyone in your organization will have at least one finger for fingerprint biometrics, but gait-based biometrics may be more difficult if you have any wheelchair-bound staff members.

Uniqueness: How well the particular biometric distinguishes people. Palm is the best, and fingerprints and iris scans are pretty good too.

Permanence: A good biometric system should measure something that changes slowly (if at all) over time. DNA and fingerprints are very good over the long term; handwriting and voice change somewhat from decade to decade.

Collectability: This refers to how easily the biometric can be measured. face scores very low (it isn't easy to collect); fingerprint and palm-scan biometrics rate quite high. Gait requires a person to walk over a distance, which would be hard to do while sitting at a workstation. Retina scan requires the subject get really close to a digital camera.

Performance: This refers to the overall technology burden: how much equipment, time, and calculation go

into performing a comparison. The fingerprint method fares very well; fingerprint readers are small, compact, and accurate. Biometrics tends to be costly, slow, and labor-intensive.

Accuracy: How well does a biometric system distinguish between subjects, and what are the false acceptance and false rejection rates?

Acceptability: Will users be willing to use the biometric technology? face will score low because of privacy reasons. Retina scans will score low because some people will be uncomfortable putting their eye really close to something that seems intrusive. Similarly, people won't mind swiping a finger across a surface-type fingerprint scanner or getting an iris photographed from a few feet away, but some are squeamish about sticking their fingers into a device (too many "B" movies).

Circumvention: This refers to how easily a forgery can be made that will fool the biometric system (early fingerprint devices, for example, could be fooled with "gummy fingers"). *Proof of life* testing — a feature that determines whether a sample comes from a *living* body part — is incorporated into many biometric systems so digital images of body parts are less likely to fool the system. But circumvention also refers to whether someone can attack a biometric system in other ways, such as replaying known good credentials through a network connection.

IX. Conclusions

The work represents an attempt to acknowledge and account for the presence on e-passport using biometrics recognition towards their improved identification. The application of facial, fingerprint, palm print and iris recognition in passports requires high accuracy rates; secure data storage, secure transfer of data and reliable generation of biometric data. An RFID chip will be embedded into the back cover of the passport. Border guards will be able to compare the face of the person standing in front of them with the image of the person stored onto the RFID chip. This image will also have to match the image printed into the passport page. Policymakers have put their faith in the technological promise of biometric identification because absolute identification could eliminate mismatched computer records and stolen identities. The discrepancy in privacy laws between different countries is a barrier for global implementation and acceptance of biometric passports. A possible solution to un-encrypted wireless access to passport data is to store a unique cryptographic key in printed form that is also obtained upon validation. The key is then used to decrypt passport data and forces thieves to physically obtain passports to steal personal information. The inclusion of biometric identification information into machine readable passports will improve their robustness against identity theft if additional security measures are implemented in order to compensate for the limitations of the biometric technologies. It enables countries to digitize their security at border control and provides faster and safer processing of an e-passport bearer. E-passports may provide valuable experience in how to build more secure and biometric identification platforms in the years to come.

References

[1] Ari Juels, Paul Syverson, and Dan Bailey, "High-power proxies for enhancing RFID privacy and utility", Workshop on Privacy Enhancing Technologies (PET 2005), May 2005.

[2] G. Avoine. "Cryptography in Radio Frequency Identification and Fair Exchange Protocols", PhD thesis, EPFL, Lausanne, Switzerland, December 2005.

[3] G. Tsudik, "YA-TRAP: Yet Another Trivial RFID Authentication Protocol", In International Conference on Pervasive Computing and Communications, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press. 2006.

[4] C.Hesher, A.Srivastava, G.Erlebacher, *"A novel technique for face recognition using range images"* in the Proceedings of Seventh International Symposium on Signal Processing and Its Application, 2007.

[5] G. Tsudik, "A family of dunces: Trivial RFID identification and authentication protocols", In Privacy Enhancing Technologies 7th International Symposium, PET 2007, Ottawa, Canada, June 20-22, 2007: Revised Selected Papers, volume 4776, page 45. Springer, 2007.

[6] D. Monar, A. Juels, and D. Wagner, *"Security and privacy issues in e-passports"*, Cryptology ePrint Archive, Report 2005/095, 2008.

[7] HOME AFFAIRS JUSTICE, *"EU standard specifications for security features and biometrics in passports and travel documents"*, Technical report, European Union, 2008.

[8] J. Wu and D. R. Stinson, "A Highly Scalable RFID Authentication Protocol", In Proceedings of the 14th Australia Conference on Information Security and Privacy, Brisbane, Australia, July 2009.

[9] Inoue, S. and Yasuura, H., " RFID Privacy using user-controllable uniqueness", In Proceedings of RFID Privacy Workshop, MIT, MA, USA. 2010.

[10] Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, Ltd, 2010.

[11] Riscure Security Lab, *"E-passport privacy attack"*, at the Cards Asia Singapore, April 2011.

[12] M. Lehtonen, F. Michahelles, T. Staake, and E. Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In *Int. Conf. on Ambient Intelligence Development – Amid'06*, 2011.

[13] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System

Administration conference (LISA 2006), Washington DC, December 2012.

[14] Stephen A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, May 2012.

First Author Profile:

Mr. V.K. NARENDIRA KUMAR M.C.A., M.Phil., Assistant Professor, Department of Information Technology, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India. He received his M.Phil Degree in Computer Science from Bharathiar University in 2007. He has author more than 40 international journal article publications. He has authored or co-authored more than 60 technical papers and conference presentations. He is an editorial board member for several scientific international journals. His research interests are focused on Internet Security, Biometrics, Advanced Networking, Visual Human-Computer Interaction, and Multiple Biometrics Technologies.

Second Author Profile:

Dr. B. SRINIVASAN M.C.A., M.Phil., M.B.A., Ph.D., Associate Professor, PG & Research Department of Computer Science, Gobi Arts & Science College (Autonomous), Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India. He received his Ph.D. Degree in Computer Science from Vinayaka Missions University in 11.11.2010. He has author or co-authored more than 45 international journal article publications. He has authored or co-authored more than 75 technical papers and conference presentations. He is a reviewer for several scientific e-journals. His research interests include automated biometrics, computer networking, Internet security, and performance evaluation.

