I. J. Computer Network and Information Security, 2012, 8, 55-64
Published Online August 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.08.07

Enhancement of Security and Privacy in Biometric Passport Inspection System Using Face, Fingerprint, and Iris Recognition

[1] V.K. NARENDIRA KUMAR & [2] B. SRINIVASAN
[1] Assistant Professor, Department of Information Technology,
[2]Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
[1]kumarmcagobi@yahoo.com, [2] 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. 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 deployment of biometric technologies, countries need to test and evaluate its systems since the International Civil Aviation Organization (ICAO) provides the guidelines, but the implementation is up to each issuing country. The paper also provides a cryptographic security analysis of the e-passport using face fingerprint, and iris biometric that are intended to provide improved security in protecting biometric information of the e-passport bearer.

Index Terms — Biometrics, e-Passport, Inspection System, Face, Iris, Fingerprint

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].

A passport is an internationally recognized travel document that verifies the identity and nationality of the bearer. 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. This improved security is also hoped to be accompanied with a faster processing time at border crossings.

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. 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. 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 [2].

A. 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 passport documents by more accurate identification of individuals. It is interesting to find out to what extent the integration of cryptographic security along with finger print and face biometric identification information into passports will improve their robustness against identity theft.

B. History of the passport

The concept of a passport has existed for several centuries, with the term 'passport' possibly originating from the medieval documents that were required to pass

through the gate (or 'Porte') of city walls. These documents were generally issued by local authorities to any traveler and contained a list of the locations through which the holder was permitted to pass. However, it was not until the 20th century that the modern concept of a multi-journey, multi-destination passport issued by the holder's country of nationality emerged. In 1920, the League of Nations, and later the United Nations and the ICAO, issued guidelines on standardizing passport features and layout. Less than 100 years after the first standards were devised, an estimated 600 million passports are believed to be in circulation worldwide. Although this represents only a fraction of the global population, the basic assumptions about a passport remain the same: this is an important document that is trusted internationally to establish the identity and nationality of the individual. Clearly the main – and legal – reason most citizens apply for a passport is to facilitate easy travel from country to country. But the modern passport offers a lot more than access to other countries, continents and cultures. Today, the average citizen in the developed world is just as likely to show his or her passport for administrative purposes as they are for boarding an airplane or entering a country.

C. Validity Period for a Biometric passport

The validity period of a biometric passport is at the discretion of the issuing State; however, in consideration of the limited durability of documents and the changing appearance of the passport holder over time, a validity period of not more than ten years is recommended. States may wish to consider a shorter period to enable the progressive upgrading of the biometric passport as the technology evolves.

D. Biometric

Biometric technologies are automated methods of recognizing an individual based on their physiological or behavioral characteristics such as face and fingerprints. Biometric systems are applications of biometric technologies and can be used to verify a person's claimed identity and to establish a person's identity.

Two interesting properties of biometric identification are:

1. The person to be identified is required to physically be present at the point of identification.
2. Identification is based on the biometric technique that does not depend on the user to remember a password or to carry a token.

There are two distinct functions for biometric devices:

1. To prove you are who say you are
2. To prove you are not who you say you are not.

The purpose of the first function is to prevent the use of a single identify by multiple people. The second function is used to prevent the use of multiple identities by a single person. It would have to be ensured that the biometric system either automatically cross checks the enrolled characteristics for duplicates, or otherwise does not allow a person to register their biometric under two different names. A common feature of any system that uses biometric is a trade-off between high security and a more usable system.

II. 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 and fingerprints [3].

A. Face Identification

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 [2]. 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 [6]. 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.

B. Fingerprint Identification

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 [3]. 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 [4]. 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. Iris Identification

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 [3].

III. Security Based On Assumptions

The biometric passport makes several simplifying assumptions which will eliminate many irrelevant details of our empirical analysis and thereby keeps the "big picture" of the analysis observable to the reader. For example, assume that the cryptographic schemes used in biometric passport systems are secure. It is assumed that the reader is familiar with the concepts and mechanisms offered by cryptography and public key infrastructures. Our analysis uses the following assumptions:

Assumption I: **Signature schemes are secure.** The probability that an adversary not having access to the private key creates a forged passport signature so that the verification of the signature is true-is negligible. Cryptographers have worked a lot with this subject. Therefore, in this work assume that the signature schemes are secure.

Assumption II: Whilst the use of **cryptography techniques** adds complications to the implementation of biometrics enabled passports, such techniques add value in that they will provide front-line border control points with an additional measure to determine the authenticity of the passport document. It is assumed that their use is the sole measure for determining authenticity and it should not be relied upon as a single determining factor.

Assumption III: The **digitally stored image of the face** is assumed not to be privacy-sensitive information. The face of the MRTD holder is also printed in the MRTD and can be readily perceived.

Assumption IV: The **digitally stored images of the fingerprints, and/or iris** are additional biometric features which States may choose to apply for national use. They are generally considered to be privacy sensitive and therefore need to be protected under the issuing State's national legislative framework.

Assumption V: The use of **Certificate Revocation Lists** (CRLs) is limited to country signing CA certificates and document signer certificates. CRLs are not applicable for individual Document Security Objects and document specific Active Authentication key pairs.

Assumption VI: **Certificate Verification:** The Inspection System, such as the BIS (BAC Inspection System) and the EIS (EAC Inspection System), verifies the SOD after verifying validity of the certificate chain for the PA (CSCA certificate → DS certificate) in order to verify for forgery and corruption of the biometric passport identity data recorded in the TOE. For this, the DS certificate and CRL shall be verified periodically. The EIS shall securely hold the digital signature generation key that corresponds to the IS certificate and shall provide the TOE with the CVCA link certificate, the DV certificate and the IS certificate in the EAC-TA.

Assumption VII: **Inspection System:** The Inspection System shall implement security mechanisms of the PA, the BAC and the EAC according to the ICAO document and EAC specifications on the basis of the verifying policy of the e-Passport for the biometric passport holder. Also, after session ends, the BIS and the EIS shall securely destroy all information used in communication and the TOE, such as the BAC session key, the EAC session key and session information, etc.

Assumption VIII: **IC Chip:** The IC chip, the underlying platform of the biometric passport, provides the random number generation and cryptographic operation to support security functions of the TOE. It also detects the TOE's malfunction outside the normal operating conditions and provides functions of the physical protection to protect the TOE from physical attacks using the probing and reverse engineering analysis.

Assumption IX: **MRZ Entropy:** The BAC authentication key seed takes the MRZ entropy to ensure the secure BAC authentication key.

The paper consider only those passport scenarios whose passport protocols base on public-key cryptography, certificates, and a public key infrastructure without addressing the protocols itself detailed, but this is no strong constraint. Furthermore assume the potential passport applier to use ordinary PCs with Windows or Linux software and an arbitrary connection to the Internet [11].

Technological securities issues are to be found in several dimension, but below thesis focus on hardware, software, and infrastructure as some of the most critical issues.

The following subsections address security issues of the client, the (passports) servers, and the connections between clients and servers. In particular thesis looks at the passport process itself as opposed to online passport registration, which is a separate, but important and difficult problem.

IV. 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 biometric 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 biometric passport by the issuing state shown in table I. 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 I: Logical Data Structure

Data Group	Data Element
DG 1	Document Details
DG 2	Encoded Headshot
DG 3	Encoded Face biometrics
DG 4	Encoded Fingerprint
DG 5	Encoded Iris
DG 6	Displayed Portrait
DG 7	Reserved for Future Use
DG 8	Signature
DG 9-10	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. Inspection System Security Issues

The use of electronic passports requires inspection systems to verify the passport and the passport holder. These inspection systems are primarily intended for immigration authorities at border control. Obviously the inspection systems need to support the security mechanisms implemented in a biometric passport. This appears to be a major challenge due to the diversity of options that may be supported by individual passports. In terms of security protocols and information retrieval the following basic options are allowed:

- Passive Authentication
- Active Authentication
- Basic Access Control (including OCR scanning of MRZ data)
- Extended Access Control (enhanced privacy protection mechanism).
- Chip Authentication
- Terminal Authentication
- Amount of personal data included
- Number of certificates (additional PKI certificates in the validation chain)
- Choice of biometrics (e.g. Face, Fingerprints, & Iris)
- Biometric verification methods

The problem with all these options is that a passport can select a set of preferred options, but an inspection system should support all of them. An associated problem in the introduction of the passport technology is that testing inspection systems becomes very cumbersome. To be sure that false passports are rejected the full range of options should be verified for invalid (combinations of) values. Finally, a secure implementation of the various cryptographic schemes is explanation. Passport forgery becomes a risk for inspection systems that have this vulnerability. Immigration authorities can defend themselves against this attack, and other hidden weaknesses, by proper evaluation of the inspection terminals to make sure that these weaknesses cannot be exploited.

A. Security Methods Comparison

Besides Passive Authentication by Digital Signatures, additional security methods must be used in order to protect the chip and its data. Table II show the advantages and disadvantages of each security method described in this section.

TABLE II. Security Methods Comparison

METHOD	ADVANTAGE	DISADVANTAGE
Passive Authentication	Proves that the content of SOD and LDS are authentic	Does not prevent exact copy or chip substitution. Does nor prevent unauthorized access.
Active Authentication	Prevents copying of SOD and proves that is has been read from authentic chip Proves that chip has not been substituted	Requires processor chips.
Basic Access Control	Prevents skimming. Prevents eavesdropping	Does not prevent exact copy or chip substitution (requires also copying of conventional document).
Extended Access Control	Prevents unauthorized access to additional biometrics. Prevents skimming of additional biometrics.	Requires additional Key management. Does not prevent exact copy or chip substitution (requires also copying of conventional document).

B. Security Properties

By placing a secure sketch of a biometrics on the biometric passport, the proposed system has implemented a strong mapping between a passport and its owner. The act of using someone else's passport as your own has now become quite a bit more difficult.

Also, the system increases the reliability of a passport without putting any personal data at risk. The passport owner's biometric data is not stored anywhere on the passport. Through the use of cryptography, a secure sketch of a biometric data is all that is needed to regenerate the key that is associated with a person's face, fingerprint, and iris.

Very little overhead is placed upon the passport holder. Anyone who is having their passport examined must already present the passport to the person who is performing the check. After implementing the proposed system, the only additional burden will be that the passport holder will need to place his biometric data on biometric scanners for identity verification.

An advantage that using a face, fingerprint, and iris or other form of biometric has over another scheme is that the user is only presenting himself. This is something that the user always has with him and cannot forget at home. There is no need to remember an extra passphrase or physical key. In any case, using biometrics is preferred over either of those two methods because a key or passphrase only prove that you know something that the owner of the passport should know. It does not prove that the passport actually belongs to you.

Since the key is merely the passport holder's face, finger, and iris there is no need to create a large infrastructure for the scheme that is proposed by this biometric passport system. An example of a large infrastructure would be setting up a secure, replicated database that holds the public and private key pairs of all of the citizens. Another example would involve creating an entirely new form of identification such as "passport" Implementing an entirely new system results in the need for new departments within the government, distribution and adjustment to the new card, and installation costs.

The biometric passport system already involves installing RFID readers at every passport check station. Implementing the notion of a secure sketch and associated public key requires only that biometric scanners be installed along with the new tag reading units. In addition to the cost of purchasing biometric scanners, there is also the cost of implementing software that will perform the scanning of face, fingers, iris and the transformations that are necessary for comparing two biometric data scans reliably.

VI. Inspection System

Country A's inspection system is presented with a biometric passport issued by country B. A's inspection system wishes to access biometric data in the biometric passport. The figure 1 shows the workings in a biometric passport inspection system highly simplified form. The groundwork for this has been prepared ahead of time. Country B was asked for permission for this type of access and as a result, country A was able to issue an appropriate inspection system certificate. The inspection system first authenticates the biometric passport ('Chip Authentication'). A specially-adapted key-agreement protocol is used to enable each end to independently generate the same secret key to secure the subsequent steps. This gives a much greater level of protection than that afforded by Basic Access Control, including resistance to man-in-the-middle attacks. The biometric passport then challenges the inspection system to prove its entitlement to read the sensitive data ('Terminal Authentication'). The inspection system provides a certificate chain back to the aforementioned inspection certificate that represents that entitlement. This is signed using the key from the Chip Authentication stage. When this is all verified the biometric passport can release the requested face, fingerprint, and iris images.

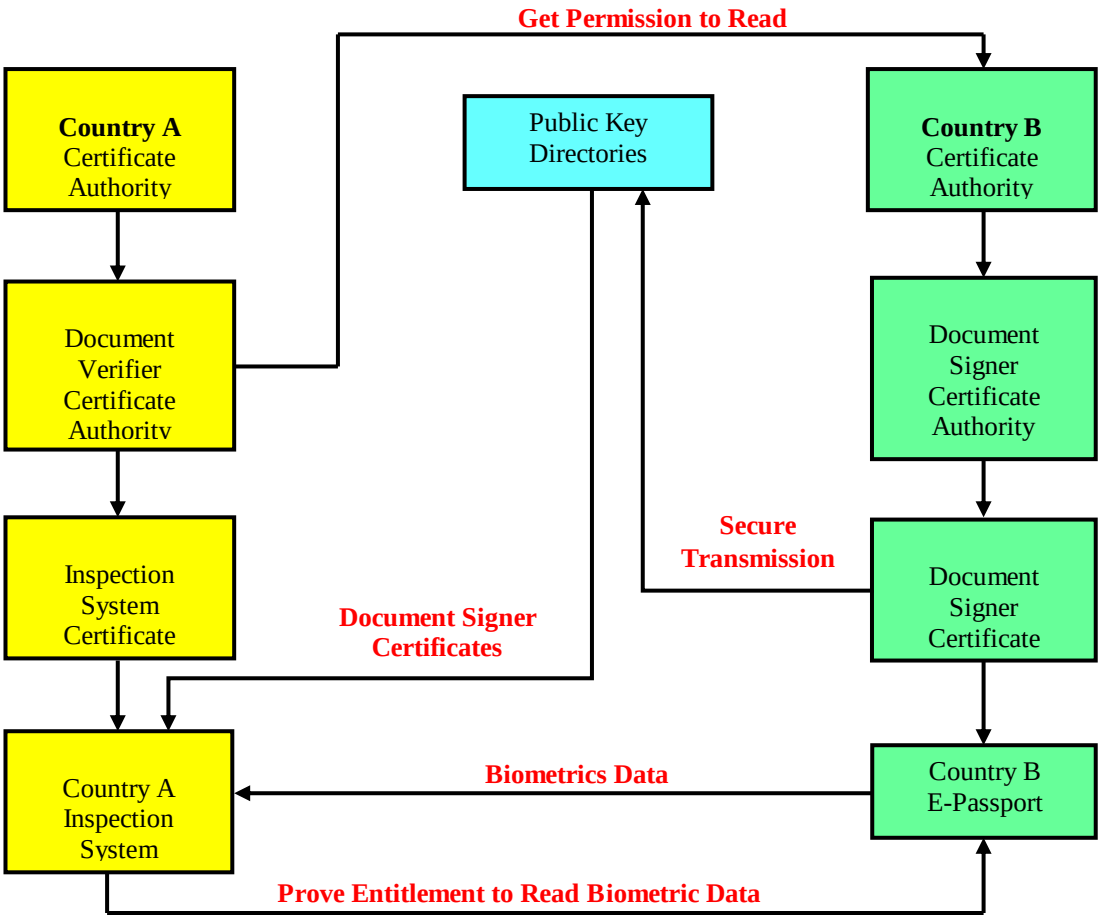

Figure 1: Biometric Passport Inspection System

A. Public Key Infrastructure

In normal situations, certificate-issuing organizations known as Certificates Authorities (CA's) are grouped in a trusted hierarchy. All CA's directly or indirectly trust the top-level Root CA. However, in ICAO, when a private key is compromised, the country cannot automatically invalidate all the passports issued with this key. The passport signed by any private key is expected to last for the issuing period. It is not feasible to ask hundreds or even thousands of passport holders to renew their passports every time a key is revoked. Instead, these passports should be used as normal, and a mechanism should notify the custom officials inspect the passport in greater detail. For each country such as the US, there is a Country Signing CA responsible for creating a public/private key pair, which is used to sign the Document Signer Certificates. This key pair should be generated and stored in a highly protected, offline CA infrastructure by the issuing country [5]. The lifetime of a Country Signing CA Key should be the longer of:

- The length of time the key will be used to issue passports
- The lifetime of the passport issued by the key.

To ensure security, the ICAO recommended the countries to replace the CA key every 3-5 years [5]. Under each country, there are numerous passport-issuing offices. Each of them is a Document Signer with a public/private key pair and has a Document Signer Certificate. Each passport is signed by the Document Signer Certificate to ensure data integrity. In order to avoid large amount of passports with invalid keys when a Document Signer Certificate Key is revoked, the suggested lifetime of the key should be about three months, less if the office issue a lot of passports per period of time. If a key or a certificate needs to be revoked, the Country CA must communicate bilaterally to all other countries and to the ICAO Public Key Directory within 48 hours [7]. In addition, a full revocation list should be exchanged every 90 days. All the private keys of Document Signer is stored in the passport-issuing office, where as the public key is stored in the ICAO Public Key Directory. The directory is a central source used to distribute the public key to the participating countries. Each participant country is responsible for downloading the latest version of the keys and making sure passports are indeed signed by the Document Signer.

B. Passive Authentication

Passive Authentication is the only mandatory cryptographic protocol in the ICAO. Its primary goal is

to allow a Reader to verify that the biometric face data in the biometric passport is authentic. This scheme is known as passive authentication since the Tag performs no processing and is only passively involved in the protocol. One must note that Passive Authentication does not tie the Tag to a passport. The Inspection System retrieves the certificate of the issuing document verifier; using the public key from the certificate it verifies the digital signature and biometric used to sign the biometric face data. Once the validity of the signature is established, the Reader computes the hash of each of these data elements and compares them with the hashed values stored. If there is a match, it can be established that the data on the Tag was not manipulated [7].

C. Active Authentication

Active Authentication is an optional protocol in the ICAO specifications. Using a simple challenge-response mechanism, it aims to detect if a Tag has been substituted or cloned. If Active Authentication is supported, the Tag on the biometric passport stores a public key (KP_{uAA}) in Data and its hash representation. The corresponding private key (KP_{rAA}) is stored in the secure section of Tag memory. In order for the Tag to establish its authenticity, it must prove to the Reader that it possess this private key [13].

- The Reader sends a randomly generated 64 bit string (R) to the Tag.
- The Tag signs this string using the key KP_{rAA} and sends this signature to the Reader.
- The Reader obtains the public key KP_{uAA} stored in biometric Data.
- The Reader verifies the correctness of the signed string using its knowledge of R and KP_{uAA}.

D. Basic Access Control

The Basic Access Control (BAC) is an optional protocol that tries to ensure that only Readers with physical access to the passport can read Tag data. When a reader attempts to scan the BAC enabled biometric passport, it engages in a protocol which requires the Reader to prove knowledge of a pair of secret keys (called `access keys') that are derived from biometric data on the Machine Readable Zone (MRZ) of the passport. From these keys, a session key which is used for secure messaging is obtained [8].

E. Chip Authentication

The Chip Authentication protocol is aims to replace Active Authentication as a mechanism to detect cloned biometric passports. If Chip Authentication is performed successfully it establishes a new pair of encryption and MAC keys to replace BAC derived session keys and enable secure messaging. It does this using the static Diffie-Hellman key agreement protocol. Note that the biometric passport Tag already has a Chip Authentication public key and private key (in secure memory).

The biometric passport and an IS instantiate a non-concurrent protocol run (session) between them, whereas the session connections between an IS and a DV may run concurrently. An IS is always the initiator of a protocol run and a biometric passport is always the responder. The underlying security for Diffie-Hellman (DH) key exchange; the Decisional Diffie-Hellman (DDH) assumption holds. Cryptographic primitives such as symmetric and public key encryption, digital signatures, message authentication codes and hash functions are secure under the standard security notions in the cryptographic literature.

VII. Biometric Passport Protocol

To resolve the security issues identified in both the first- and second-generation of biometric passports, in this section, we present an on-line secure biometric passport protocol (OSEP protocol). The proposed protocol leverages the infrastructure available for the standard non-electronic passports to provide mutual authentication between a biometric 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 OSEP protocol changes this to an active monitoring system. The border security check-point or the DV can now crosscheck against the database of known offenders themselves, thus simplifying the process of the identification of criminals [10].

The on-line secure biometric passport protocol provides the following security features: A biometric passport discloses its information stored on the biometric passport chip only after a successful authentication of the IS (Inspection System). This prevents revealing the biometric passports identity to a third party that is not authorized or cannot be authenticated. This prevents the covert collection of biometric passport data from 'skimming' or 'eavesdropping' attacks that were very effective against both the first- and the second-generation biometric passports [9].

- The OSEP protocol provides proof-of-freshness and the authenticity for messages between the participating entities.
- The OSEP protocol uses the existing ICAO PKI implementation (as in first generation biometric passports) and eliminates the need for cross-certification among the participating countries, as required by the EAC (second-generation biometric passports).
- The OSEP protocol eliminates the need for certificate chain verification by a biometric passport. Only the top level certificate ($CERT_{CVCA}$ ( )) is required to be stored in a biometric passport, thus reducing the memory requirements and preventing a

malicious reader from performing a DOS attack on a biometric passport.

- The OSEP protocol also requires an IS to provide proof-of-correctness for public key parameters to a biometric passport. This allows a biometric passport to verify that an IS is using the correct domain parameters and to prevent related attacks [12].

A. Biometric Passport Initial Setup

All entities involved in the protocol share the public quantities p, q, and 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, SK_i) 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 a biometric passport are also certified by its root certification authority.

B. Phase One – Biometric Inspection System

Step 1 (BIS) When a biometric passport is presented to a BIS, the IS reads the MRZ information on the biometric passport using an MRZ reader and issues the command GET CHALLENGE to the biometric passport chip.

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

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

Step 3 (IS) On receiving the response from the biometric passport, the IS generates a random *IS* $\pounds_R$ $1 \leq IS \leq q - 1$ 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 biometric passport and K_{eP}.

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

It then contacts the nearest DV of the biometric passports issuing country and obtains its public key. The IS encrypts and sends its signature S_{IS} along with the biometric 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 biometric 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 biometric 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 biometric passport's PK to verify during biometric 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 biometric 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 biometric 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 biometric passport is convinced that the IS system is genuine and can proceed further in releasing its details. All further communications between a biometric passport and IS are encrypted using the session key K_{ePIS}.

C. Phase Two – Biometric Passport Authentication

Step 1 C The IS issues an INTERNAL AUTHENTICATE command to the biometric passport. The biometric passport on receiving the command, the biometric 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 biometric passport is genuine and authentic.

During the IS authentication phase, and IS sends the biometric passport's MRZ information to the nearest biometric passport's DV, which could be a biometric passport country's embassy. Embassies are DV's because they are allowed to issue biometric passports to their citizens and because most embassies are located within an IS's home country, any network connection issues will be minimal. Sending the MRZ information is also advantageous, 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

States are encouraged to use biometrics to establish or validate identity at border control. The use of biometric data does not ensure that a person has provided their correct name, citizenship and other information, but when biometric identity has been confirmed, it does help to prevent the person from using another name in their dealings. Biometric identity should be identified at ports of entry and ideally points of exit.

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 system. 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.

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.

IX. Conclusions

The work represents an attempt to acknowledge and account for the presence on inspection system for biometric passport using face, fingerprint, and iris recognition towards their improved identification. The application of biometric recognition in passports requires high accuracy rates; secure data storage, secure transfer of data and reliable generation of biometric data. The passport data is not required to be encrypted, identity thief and terrorists can easily obtain the biometric information. 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. More research into the technology, additional access and auditing policies, and further security enhancements are required before biometric recognition is considered as a viable solution to biometric security in passports. The adversaries might exploit the passports with the lowest level of security. 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 a biometric passport bearer. The main cryptographic features and biometrics used with biometric passports and considered the surrounding procedures. Biometric passports may provide valuable experience in how to build more secure and biometric identification platforms in the years to come.

References

[1] A. K. Jain, R. Bolle, *"Biometric personal identification in networked society"* 1999, Norwell, MA: Kluwer.

[2] B. Jeng and L.Y. Chen. How to enhance the security of e-passport. In Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, pages 2922–2926, 2009.

[3] 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, 2003.
[4] D. Monar, A. Juels, and D. Wagner, "*Security and privacy issues in e-passports"*, Cryptology ePrint Archive, Report 2005/095, 2005.
[5] Friedrich. The Introduction of German Electronic Passports. Second Symposium on ICAO-Standard, MRTDs, Biometrics and Security, September 2006.
[6] HOME AFFAIRS JUSTICE, *"EU standard specifications for security features and biometrics in passports and travel documents"*, Technical report, European Union, 2006.
[7] Jaap-Henk Hoepman and Bart Jacobs. E-passports without the big picture. E-Government Monitor, February 20 2006.
[8] ICAO, "Machine readable travel documents", Technical report, ICAO 2006.
[9] KLUGLER, D., *"Advance security mechanisms for machine readable travel documents, Technical report"*, Federal Office for Information Security (BSI), Germany, 2005.
[10] ICAO, "*Machine Readable Travel Documents",* Part 1 Machine Readable Passports. ICAO, Fifth Edition, 2003
[11] Riscure Security Lab, *"Biometric passport privacy attack"*, at the Cards Asia Singapore, April 2006.
[12] ICAO, *"Biometrics Deployment of Machine Readable Travel Documents"*, Version 2.0, May 2004.
[13] M. Abid, "Secure e-passport protocol using elliptic curve diffie-hellman key agreement protocol", In: 4th International Conference on Information Assurance and Security. 2008, page no. 56-67

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 authored or co-authored more than 55 technical papers and conference presentations. He is an editorial board member for several scientific journals. His research interests are focused on Internet Security, Biometrics, Advanced Networking, Electronic Identification Systems, 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 authored or co-authored more than 70 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.