Mathematical Machine Readable Authentication Protocols for Network Security

R.M.L.S. Chandrarathna
Lecturer, Department of Computer Mathematics, Sri Lanka Institute of Information Technology, (SLIIT), Sri Lanka

Corresponding Author: chandrarmlssri@yahoo.com

Received: 05-02-2023 Revised: 21-02-2023 Accepted: 17-03-2023

ABSTRACT
Since the International Civil Aviation Organization created standards that allow passports to store biometric identification, electronic passports have been widely and quickly embraced throughout the world. The use of biometrics for identification has the potential to improve people's quality of life and make the world a safer place to live in. By more precisely identifying a person, biometric passports are meant to stop travelers from entering a nation illegally and to reduce the use of fake documents. This article examines the biometric e-passport design for the face, fingerprint, palmprint, and iris. This article focuses on the personal security and privacy of e-passport holders, as well as the actual security benefits that governments have gained from the use of face, fingerprint, palmprint, and iris recognition technology in e-passports. Researchers looked at the facial fingerprint, palmprint, and iris biometrics now utilized with e-passports as well as the key cryptographic elements and supporting procedures. The report also offers a security evaluation of the e-passport's use of face fingerprint, palmprint, and iris biometrics, which are meant to increase security by safeguarding the ePassport holder's biometric data.

Keywords: mathematics, network security, machine

I. INTRODUCTION

A biometric passport is another name for an ePassport. An electronic passport is a kind of identification that includes pertinent biographic and biometric data about the holder. A Radio Frequency Identification (RFID) Tag with cryptographic capability is also integrated inside the object. By eliminating counterfeiting and proving beyond a reasonable doubt the identification of the document's holder, the successful integration of biometric technologies into papers like e-Passports promises to boost border security. Biometrics are quantifiable traits of a person used to identify them. Depending on their intended use, biometric systems can operate in verification or identification modes. A person delivers an identification claim to the system during a verification task, and the system just needs to validate the claim. An unknown person presents themselves to the system during an identification task, and it must identify them. There are generally three methods of authentication. They are: Something you hold - card, token, key, in order from least secure and convenient to most secure and convenient. PIN or password that you are familiar with. Biometric refers to something you are. The three technologies that make up E-Passports—biometric, RFID, and public key infrastructure—are introduced. The researcher also does a good job of summarizing three technical studies' descriptions of the protocols and operation of the e-Passport standards. This is the first piece of work to analyze the e-Passport's protocols. Additionally, the researcher outlines several real dangers to the e-Passport system.

II. BACKGROUND OF THE STUDY

In their 2005 article, Juels et al. examined the security and privacy concerns related to e-passports. They voiced worry that an e-passport's contact-less chip may be used to read its contents without making physical contact with an IS and, more significantly, with the booklet closed. They claimed that information kept on the chip may be secretly gathered by "skimming" or "eavesdropping." As Laurie has shown, due to poor entropy, stored secret keys are susceptible to brute force attacks. (2007). An e-passport may be vulnerable to "splicing attack," "fake finger attack," and other attacks that can be carried out when an e-passport bearer presents the e-passport to hotel clerks, according to Kc and Karger (2005). The security flaws of e-passports have received extensive journalistic coverage (Johnson, Knight, and Reid 2006). According to these reports, it might be easy to "clone" an electronic passport. The ICAO begins work on MRTD in 1968. 1980: OCR-B Machine Readable Zone (MRZ) first standard. In 1997, the ICAO-NTWG (New Technology WG) begins to develop biometrics. The US wants to hasten the process after 9/11. Version 1.1 of the standard was released in 2004 and includes ICC and biometrics. EU develops expanded access control and more personal data in 2006.

2.1. Technical Challenges An interoperable system for international travel is necessary, and ICAO guidelines have helped to set up some of the necessary infrastructure. However, individual governments always exercise caution when signing any international agreement because they worry that they may give up some of their unique rights. The NTWG avoided discussing a number of implementation difficulties, particularly in the security sphere, in an effort to uphold national sovereignty over passports. Now that modern electronics are being used, these questions are crucial for maintaining interoperability between national systems. However, other suppliers will need to achieve comparable performance levels with elevated accuracy and detection rates in order for widespread deployment to take place.

2.2. Domestic Challenges It will be significantly more difficult to safeguard the electronic passport than it will be to secure the biometric technologies in passports. However, it is evident that contactless chips have many benefits, such as higher capacities and lower prices. Although substantial adoption of the technology is anticipated in the private sector over the next few years, it has not yet occurred in either the public or private sectors. Simply said, contact-based chips are not as reliable as contactless technology. Major retailers like Walmart are looking into integrating RFID into their supply chain since there aren't enough barcodes accessible and because it is a superior tracking technology to almost all others. As this rollout progresses, RFID may also become an essential component of a variety of other routine activities, such entering a place of employment or processing a credit card purchase.

2.3. International Challenges The distribution of electronic passports is still under progress, although many nations are still lagging behind. Undoubtedly, some countries may be unable to advance due to the continuous discussion over the best way to preserve the data stored on the RFID tags. The international community would do well to take the time necessary to accomplish the project correctly given its complexity and the requirement that it stay static for a sizable number of years. Many nations started distributing e-passports too soon, which caused a one-year delay. However, Congressional action will be necessary to prevent this delay.

2.4. After an image has been captured, the first activity that must be done is an initial alignment. The eyes, nose, and mouth are the most frequently used features to determine the direction and positioning of the face. The vast majority of facial biometric algorithms follow this methodology as the norm. Depending on whether the application is for identity or verification, processing changes after this point. Finding out a person's identity is the process of identification. The only thing that must be verified is that a subject is who they say they are [9]. The system matches the probe's captured image to the gallery during identification. The kind of comparisons done depends on the matching algorithm in question as well as the biometric that was employed. The system returns a rank ordering of identities after the comparison.

2.5. Each finger's tip bears a unique set of ridges and furrows called a fingerprint. For many years, fingerprints were used to identify people, and the matching rate was very high. By leaving an inked impression of the fingertip on paper, patterns have been extracted. Digital photographs of these patterns are now available thanks to small sensors. The first image for fingerprint identification is obtained through a live finger scan performed when the finger is in close proximity to a reader device that can also check for validating characteristics like temperature and pulse. The feature extraction module in real-time verification systems uses images captured by sensors to calculate the feature values. The position and orientation of a few crucial places known as minutiae points often correlate to the feature values. The two-dimensional minute patterns that were retrieved from the user's print and those in the template are compared during the matching procedure. The fact that existing fingerprint identification methods use a lot of processing resources is one issue.

2.6. The palmprint recognition module is made to carry out the procedure of identifying a person for the unidentified person. The only input data for the recognition procedure is a picture of a palmprint. The expected output value is the information used to identify the person. The picture feature from the input is compared to the image feature from the database. With reference to the threshold value, the relevancy is estimated. For the purpose of identifying the person, the most pertinent image is chosen. The recognition process is flagged as "unknown person" if the comparison result does not match the input image. Four smaller modules make up the recognition module. These include the selection of palmprints, outcome information, an ordinal list, and an ordinal measurement. The palmprint input image is selected by the submodule for palmprint image selection. The input image file is chosen using the file open dialog. The list of pertinent palmprints with their similarity ratio information is produced by the result details. The comparisons based on ordinal features are displayed in the ordinal list. The ordinal values for each region are displayed in the submodule for ordinal measurement.

2.7. Iris Recognition The distinctively colored ring that surrounds the eye's pupil serves as the foundation for iris recognition technology. The iris, which is made of elastic connective tissue, contains about 266 unique properties, making it an extremely rich source of biometric information. These include the trabecular meshwork, a tissue with striations, rings, furrows, a corona, and freckles that provides the appearance of drastically separating the iris. Approximately 173 of these distinguishing traits are used in iris recognition technologies. Systems for identification and verification can both use iris recognition. Iris identification systems take a high-resolution, black-and-white image of the iris using a compact, high-quality camera. The systems then build a coordinate system over the iris, identify the zones for analysis inside that coordinate system, and define the iris' boundaries.

e-ISSN: 2583-553X
Peer Reviewed Journal
https://doi.org/10.31033/abjar.2.2.2

III. ENROLLMENT UNIT OF THE BIOMETRIC SYSTEM

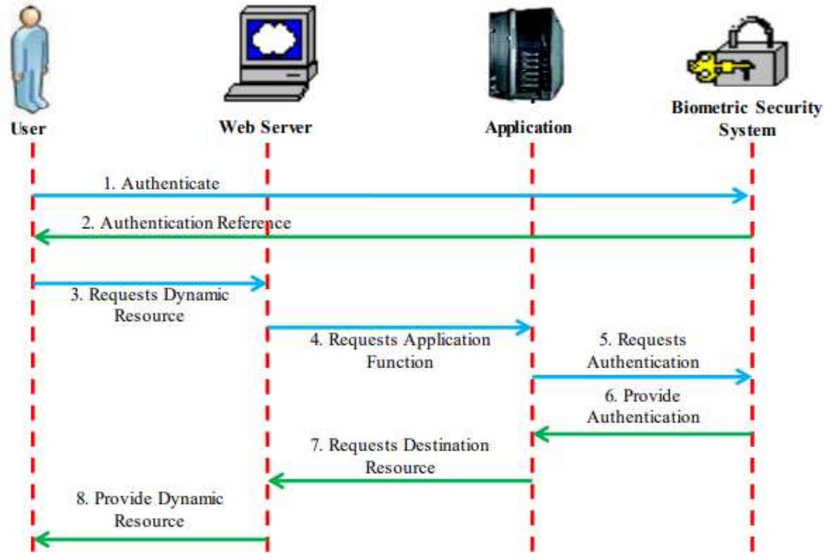
This module registers people in the biometric system's database. Feature Extraction Unit: This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard given to the person. During this phase, a biometric reader scans the person's biometric characteristic to produce its digital representation. Comparing Unit: This module evaluates the input against the template. When the system verifies the user's identification, it compares the user's master template to the new attributes and generates a score or match value. (one to one matching). Multiple match values are produced when a system doing identification compares the new features against the master templates of numerous users. (one too many matching). Decision Maker: Based on a security threshold and matching score, this module approves or rejects the user.

IV. E-PASSPORT SYSTEM DESIGN

System design is the process of changing a user-oriented document into a document targeted at database administrators or programmers. Before implementation, it undergoes a logical and physical design walkthrough.

4.1. Logical Data Structure (LDS)

For the storage of data items, the ICAO published a standardized data structure under this name. This was done to ensure that e-Passport Tags and Readers could remain interoperable on a worldwide scale. The specifications say that all 16 data groups are write protected and that only the issuing state listed in table 1 can write to them when the e-Passport is issued. The security data element (SOD) stores a hash of the data groups 1 through 15, and each of these hashes must be signed by the state publishing the document.


User
Web Server
Application
Biometric Security System
1. Authenticate
2. Authentication Reference
3. Requests Dynamic Resource
4. Requests Application Function
5. Requests Authentication
6. Provide Authentication
7. Requests Destination Resource
8. Provide Dynamic Resource

4.2. E-Passport Certification

The registration and verification processes are both part of the biometric authentication process for electronic passports. The e-Passport applicant registers their biometric at a secure site under human supervision during the registration phase. This biometric information is encoded using a feature extraction tool and then saved on the user's e-Passport Tag. The user is required to provide a sample of their biometric in order to be authenticated and have their identity verified at an inspection terminal. The recently submitted biometric is encoded using the same feature extraction approach. To determine the degree of similarity between the registered and given biometrics, a matching algorithm is executed at the terminal. The user's identification is successfully validated if the degree of similarity is judged to be greater than a predetermined threshold value. At the biometric registration or Verification stages, it is unfortunately not always possible to identify the usage of prosthetics without human supervision. It is clear that as automation grows and human oversight of the biometric process reduces, biometric spoofing attacks will get simpler to carry out.

V. AUTHENTICATION IN E-PASSPORT SYSTEMS

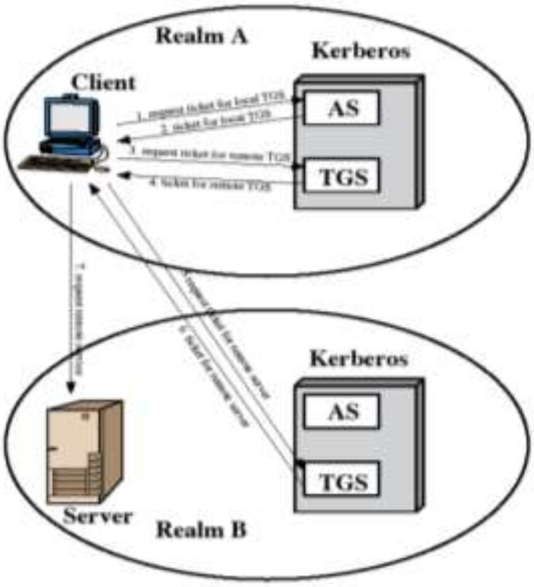
The International Civil Aviation Organization (ICAO) has established two distinct mechanisms: active and passive authentication, to validate secure chips that are contained in ePassports. In active authentication, the secure controller processes the chip's cryptographic data; in passive authentication, no calculation is done and only a verification device can read the contents of a tamper-proof chip. Consequently, secure memory devices are used for passive authentication whereas processors are needed for active authentication. A novel form of EAC authentication known as Chip Authentication has recently been introduced. Some of the Far Eastern nations also suggested similar authentication. The ASP.NET application is utilized to effectively create this biometric electronic passport system for individual identification using face, fingerprint, palmprint, and iris recognition. This program has the ability to simply add libraries and draw forms, which could speed up the development of the system.

5.1. Public Key Infrastructure Under normal circumstances, a hierarchy of trusted organizations known as Certificate Authorities (CAs) is formed, with the offspring CAs trusting the parent CAs. When a certificate is revoked, all of its progeny CAs are no longer trusted because they all directly or indirectly depend on the top-level Root CA. In ICAO, the nation cannot immediately cancel all the passports issued with a compromised private key, though. Any private key signature is supposed to remain valid for the duration of the passport's issuance. Every time a key is revoked, it is not practical to ask hundreds or even thousands of passport holders to renew their documents. Instead, these passports ought to be utilized as usual and a mechanism ought to alert the customs officers to examine the passport more carefully. A Country Signing CA is in charge of generating the public and private key pairs needed to sign Document Signer Certificates for each nation, including the US. The issuing nation should construct this key pair and keep it in an extremely secure, offline CA infrastructure. The longer of: The period of time the key will be used to issue passports should be the lifetime of a country signing CA key.

5.2. Only one cryptographic protocol is required by the ICAO, and that is passive authentication. Its main objective is to enable a Reader to confirm the validity of the e-Passport's biometric face, fingerprint, palmprint, and iris data. As the Tag participates in the protocol passively and doesn't do any processing, this system is known as passive authentication. It is important to keep in mind that passive authentication does not link the Tag to a passport; rather, researchers can only confirm that the face, fingerprint, palmprint, and iris information on the Tag is accurate, not the Tag's legitimacy. The Inspection System gets the certificate of the document verifier that issued the document, and using the certificate's public key, it verifies the digital signature and the biometrics that were used to sign the biometric face, fingerprint, palmprint, and iris data. The Reader computes the hash of each of these data components and compares them to the hashed values saved after determining the validity of the signature. If a match is found, it can be determined that the information on the Tag was not altered.

5.3. The ICAO specifications include an optional mechanism called active authentication. It seeks to determine whether a Tag has been replaced or copied using a straightforward challenge-response system. The Tag on the e-Passport stores a public key (KPuAA) and its hash representation if Active Authentication is supported. The safe region of Tag memory houses the matching private key (KPrAA). The Tag must demonstrate to the Reader that it is in possession of this private key in order to verify its legitimacy. The Reader transmits to the Tag a 64-bit string (R) that was produced at random. The Tag encrypts this string with the key KPrAA and then signs it before sending it to the Reader. The public key KPuAA kept in the biometric data is obtained by the Reader. The Reader uses its understanding of R and KPuAA to confirm the signed string's accuracy.

5.4. Basic Access Control (BAC) is an optional protocol that aims to limit the ability of Readers to read Tag data to those who have physical access to the passport. The reader must demonstrate knowledge of a pair of secret keys, known as "access keys," that are obtained from biometric data on the Machine Readable Zone (MRZ) of the passport while attempting to scan an e-Passport with BAC functionality. A session key for secure messaging is created from these keys.


Realm A
Kerberos
Client
AS
TGS
1. request ticket for local TGS
2. ticket for local TGS
3. request ticket for remote TGS
4. ticket for remote TGS
7. request remote service
5. request ticket for remote server
6. ticket for remote server
Kerberos
AS
TGS
Server
Realm B

5.5. Chip Authentication As a method to identify counterfeit e-Passports, the Chip Authentication protocol aspires to take the position of Active Authentication. In order to replace the BAC-derived session keys and enable secure messaging, a new set of encryption and MAC keys are established once CA is successfully completed. The protocol for static key agreement is used to accomplish this. Keep in mind that the Chip Authentication public key and private key are already included on the e-Passport Tag. (in secure memory).

5.6. Terminal Authentication Only if access to biometric data is necessary, the Terminal Authentication protocol is carried out. The Tag can verify the Reader used in Chip Authentication thanks to a challenge-response system. Digital certificates are used by the Reader to demonstrate to the Tag that it has received permission from both the home and visiting country to read e-Passport Tags.

VI. E-PASSPORT AUTHENTICATION PROTOCOLS

The ICAO e-passport is a complicated protocol suite made up of the BAC, PA, and AA subprotocols. Not only is it challenging to codify such a protocol suite, but verification of such systems frequently results in exponential state-space explosions. The following stages represent how researchers depict the flow of the e-passport protocol: When an e-passport is presented at a border security checkpoint, the chip and the e-passport reader execute the BAC protocol to create a secure (encrypted) communication channel between them. The chip and the e-passport reader carry out the AA procedure when the BAC has been successfully completed. The authentication of e-passports mainly relies on PKI. Only the document signer's public key is considered authentic and secure by the researcher, who models a single level of certification hierarchy up to that point (the country signing authority). This just shows that the model assumes the "ideal" PKI implementation, not that the e-passport protocol suite's verification process is compromised. Theoretically, the system's face, fingerprint, palmprint, and iris biometrics, as well as cryptographic primitives including hash functions, MACs, and key generation processes, are secure.

6.1. Initial Configuration of an E-Passport All participants in the protocol exchange the public numbers p, q, and g, where p is the modulus, a prime number of at least order 1024 bits. Q is a prime number that falls between 159 and 160 bits. Each entity has a unique public key and private key pair (PKi, SKi), where PKi = g(SK i) mod p. Entity i's public key (PKi), which is certified by its root certification authority (j), is represented as CERTj.(PKi , i). The root certification authority of an e-Passport also verifies the public parameters p, q, and g that it uses. 6.2. When an e-Passport is given to an inspection system (IS), the IS examines the MRZ information on the e-Passport using an MRZ reader before sending the command GET CHALLENGE to the e-Passport chip. Step 2 (P) The e-Passport chip now performs its part in the key agreement procedure to establish a session key by generating a random eP £ R 1 eP q - 1 and computing KeP = geP mod p.

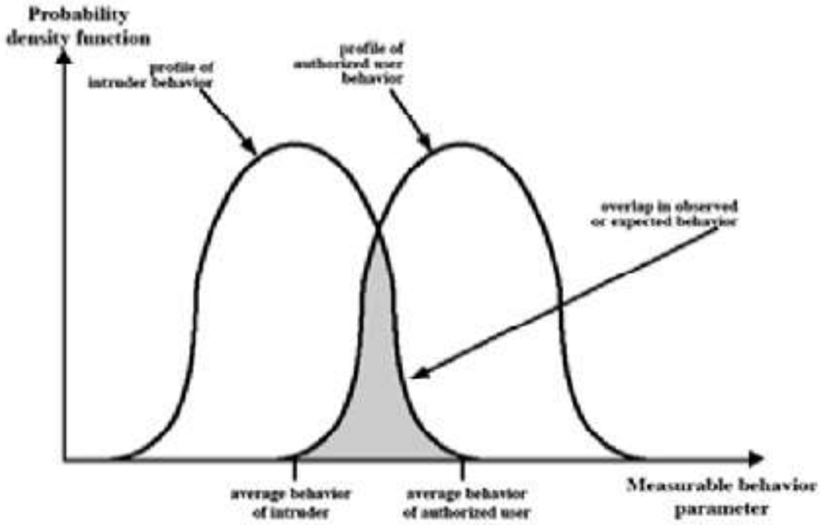
In response to the GET CHALLENGE command, the e-Passport sends KeP together with its domain parameters p, q, and g. Following receipt of the e-Passport response, the IS generates a random IS £R 1 IS q - 1 and calculates its portion of the session key as KIS = gIS mod p. The communication containing the MRZ value of the e-Passport and KeP is digitally signed by the IS. It then makes contact with the closest DV of the nation issuing the e-Passports and receives its public key. SIS = SIGNSKIS (MRZ || KeP). Using the DV's public key PKDV, the IS encrypts and transmits its signature, SIS, the MRZ data, and KeP. IS DV: ENCPK DV (SIS, MRZ, KeP), CERTCVCA (PKIS, IS) Step 4 (DV) The DV decrypts the message received from the IS and authenticates the SIS signature and CERTCVCA (PKIS, IS). If the verification is successful, the DV is certain that the IS is valid and generates a digitally signed message SDV to show this to the e-Passport. The public key PKIS of IS is used by the DV to encrypt and convey the signature SDV. SDV = SIGNSKDV (MRZ || KeP || PKIS), CERTCVCA (PKDV, DV). DV IS: ENCPKIS (SDV, [PKeP]) The DV may decide to deliver the e-Passport's public key if necessary.

The IS system now trusts the DV to be authentic, which is obviously advantageous. To verify during e-Passport authentication, it can receive a copy of the PK. Step 5 (IS) The IS computes the session key KePIS = (KIS) eP after decrypting the message received, and then uses KePIS to encrypt the signature received from the DV, the e-Passport MRZ data, and KeP. As part of the session key KIS, it also digitally signs its portion. Step 6 C: The e-Passport computes the session key KePIS = (KIS) eP after receiving the message from the IS: KIS, SIGNSKIS (KIS, p, q, and g), and ENCKePIS (SDV, MRZ,KeP). The message is decrypted using the session key, and the signatures SDV and VERIFYPKIS (SIGNSKIS (KIS, p, q, g)) are also verified. When the verification is completed, the ePassport is satisfied that the IS system is real and can continue to release its information. Using the session key KePIS, all further communications between an e-Passport and IS are encrypted. The IS sends an INTERNAL AUTHENTICATE command to the e-Passport in Step 1 C of Phase Two of the process for e-Passport authentication. The ePassport generates a signature SeP = SIGNSKeP (MRZ || KePIS) and delivers its domain parameter certificate to the IS upon receiving the instruction. Using the session key KePIS, the entire message is encrypted. ENCKePIS (SeP, CERTDV (PKeP), and CERTDV (p, q, and g)) is what eP IS.

Step 2 (IS) The message is decrypted and the CERTDV (p, q, g), CERTDV (PKeP), and SeP are verified. If the results of all three checks are positive, the IS is persuaded that the e-Passport is real and valid. An IS sends the e-Passport's MRZ information to the closest e-Passport's DV, which could be an embassy of an e-Passport country, during the IS authentication phase. Embassies are DVs since they are permitted to issue e-Passports to their residents, and as the majority of them are situated inside an IS's country of residence, network connectivity problems are unlikely to be severe. The embassy now has a list of all its people who have passed through a border security checkpoint in a foreign country as a result of sending the MRZ information. We don't anticipate any privacy concerns because most nations require their citizens to register at embassies when they travel to another nation.

VII. EXPERIMENTAL RESULTS

The outcomes for current biometrical technologies and components play a significant role in the design, deployment, and operation of biometric passport systems. Performance of the passport system needs to be assessed for both new and old technology. The biometric (iris, finger, face, or palm print) is simply one component of a fully deployed program, albeit this is a fact that is sometimes neglected. System integrators must take into account the needs of the deployed application because biometric (sub) systems are frequently not created with security and/or privacy in mind.


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

To make sure that the right procedures are in place to reassure such consumers, it is important to address the anxieties and concerns of a sizeable portion of the user community as early as feasible in the design process. These worries might have to do with issues of safety or privacy, which could be partially resolved by laws and regulations. In this article, the introduction of a new biometric passport is covered specifically along with the needs, design, and application scenarios of biometrical systems in general. The ePassport's embedded chip is a proximity contactless chip that can only be read when it is held within 10 centimeters of a reader. Additionally, in order to access the data on the chip, the passport book must be open with the machine-readable zone set to read. The traveler's ePassport will be presented to border agents who are equipped with ePassport scanners, who will scan the machine-readable zone and open the chip to read it as well. The device also verifies additional security elements, such as the nation's signature. Passports will continue to be examined by border officials who do not have ePassport readers as they now do.

VIII. CONCLUSIONS

The study is an effort to recognize and account for the existence of users of the e-passport system utilizing face, fingerprint, palmprint, and iris recognition in order to improve their identification. High accuracy rates, secure data storage, secure data transfer, and dependable biometric data creation are all necessary for the application of biometrics in passports. Since the biometric information is not obliged to be encrypted, identity thieves and terrorists can simply access the passport data. Global use and acceptance of biometric passports are hampered by differences in privacy legislation between nations. Storing a special cryptographic key in printed form that is also retrieved during validation is one potential remedy for unencrypted wireless access to passport data. When the key is used to decrypt passport data, thieves are forced to physically take passports in order to steal personal data. Before biometric recognition is taken into consideration as a practical solution to biometric security in passports, further research into the technology, new access and auditing procedures, and additional security advancements are needed. The least secure passports could be used as a tool by the adversary. If extra security measures are put in place to make up for the shortcomings of the biometric technologies, including biometric identifying information in machine-readable passports will increase their resistance to identity theft.

REFERENCES

1. A.K. Jian. (1999). Biometrics personal identification in networked society. *Technical Report*.
2. C. Hesher. (2003). A novel method for face recognition using range images. in: *7th International Symposium on Signal Processing and Its Application*.
3. Home Affairs Justice. (2006). EU standard specifications for security features and biometrics in passports and travel documents. *Technical Report, European Union*.
4. ICAO. (2006). Machine readable travel documents. *ICAO*.
5. Klugler, D. (2005). Advance security mechanisms for machine readable travel documents. *Technical Report*.