# DESIGN AND IMPLEMENTATION OF E-PASSPORT SCHEME USING CRYPTOGRAPHIC ALGORITHM ALONG WITH MULTIMODAL BIOMETRICS TECHNOLOGY

V.K. Narendira Kumar [1] and B. Srinivasan [2]

[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*

*Advancements in technology have created the possibility of greater assurance of proper travel document ownership, but some concerns regarding security and effectiveness remain unaddressed. Electronic passports have known a wide and fast deployment all around the world since the International Civil Aviation Organization the world has adopted standards whereby passports can store biometric identifiers. The use of biometrics for identification has the potential to make the lives easier, and the world people live in a safer place. The purpose of biometric passports is 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 paper analyses the face, fingerprint, palmprint and iris biometric e-passport design. This papers focus on privacy and personal security of bearers of e-passports, the actual security benefit countries obtained by the introduction of e-passports using face, fingerprint, palmprint and iris recognition systems. Researcher analyzed its main cryptographic features; the face fingerprint, palmprint and iris biometrics currently used with e-passports and considered the surrounding procedures. Researcher focused on vulnerabilities since anyone willing to bypass the system would choose the same approach. On the contrary, solely relying on them may pose a risk that did not exist with previous passports and border controls. The paper also provides a security analysis of the e-passport using face fingerprint, palmprint and iris biometric that are intended to provide improved security in protecting biometric information of the e-passport bearer.*

### *KEYWORDS*

*E-Passport, Biometrics, Cryptographic, Face, Fingerprint, Palmprint and Iris.*

## 1. INTRODUCTION

An electronic passport (e-Passport) is an identification document which possesses relevant biographic and biometric information of its bearer. It also has embedded in it a Radio Frequency Identification (RFID) Tag which is capable of cryptographic functionality. The successful implementation of biometric technologies in documents such as e-Passports aims to strengthen border security by reducing forgery and establishing without doubt the identity of the documents' bearer. Biometrics is measurable characteristics of an individual used to identify him or her. Biometric systems can function in verification or identification modes depending on their

DOI : 10.5121/ijait.2011.1603 

intended use. In a verification task, a person presents an identity claim to the system and the system only needs to verify the claim. In an identification task, an unknown individual presents himself or herself to the system, and it must identify them. In general, there are three approaches to authentication. 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 [1].

Introduction to the three constituent technologies in E-Passports: Biometric, RFID, and Public Key Infrastructure. Researcher also effectively summarizes the contents of three technical reports which describe the protocols and the functioning of the e-Passport specifications. This is the first work that analyses the protocols behind the e-Passport. Researcher also presents some feasible threats to the e-Passport protocol.

## 2. 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 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.

### 2.1. Technical Challenges

A system of international travel requires some degree of interoperability, and ICAO guidelines have provided some of the framework for that interoperability. Individual states always remain cautious in entering into any international agreement, however, fearing that they will lose some of their individual rights. In its efforts to maintain national sovereignty over passports, the NTWG avoided touching on several implementation issues, particularly in the security arena. These questions are essential to ensuring interoperability between national systems now that advanced electronics are being deployed. In order for widespread deployment to occur, though, more vendors will need to reach similar performance levels with increased accuracy and detection rates [8].

### 2.2. Domestic Challenges

The electronic passport is secure will prove substantially more difficult than actually securing it biometric technology in passports. It is quite clear, however, that contactless chips offer significant advantages, including larger capacities and lower costs. The technology also has yet to experience widespread deployment in either the private or public sector, though such deployment can be expected in the private sector in the next few years. Contact-based chips simply lack the robustness of contactless technology. A lack of available barcodes, in addition to the fact that RFID is a superior tracking technology compared to virtually any available, has led major retailers like Walmart to investigate inclusion of RFID in its supply chain. As this deployment occurs, RFID may also become an integral part of numerous other everyday tasks, such as entering a place of work or making a credit card transaction.

## 2.3. International Challenges

Electronic passport rollout plans continue to move forward, but some many countries, continue to lag behind. Certainly, the ongoing debate over how best to protect data stored on the RFID tags may be preventing some nations from moving forward. Given the complex nature of the project and the need for it to remain static for a substantial number of years, the international community would be well served to take the time necessary to implement it correctly. Many countries to begin issuing e-passports were too soon, and delayed it by one year. However, such a delay will require Congressional action [8].

## 2.4. Face Recognition

The first task needed after the capture of an image is an initial alignment. The features commonly used to identify the orientation and location of the face is the eyes, nose, and mouth. This approach is the standard used on most facial biometric algorithms. After this stage, processing varies based on whether the application is identification or verification. Identification is the process of determining who someone is. Verification only needs to confirm that a subject is the person they claim to be [9]. In identification, the system compares the captured image (probe) to the gallery. The type of comparisons made depends both on the biometric used and on the matching algorithm in question. After the comparison, the system returns a rank ordering of identities.

## 2.5. 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 [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.

## 2.6. Palm print

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.

### 2.7. 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 [3].

### 4.8. Cryptographic

The data stored in the passport is highly confidential, the Contactless IC chip must have mechanisms for protection and integrity of the data. The ICAO recommended that the passport should have the following properties [6]:

- A cryptographic checksum is used to protect data integrity. The system can detect if data has been altered by comparing the checksum in the passport against the real-time computation of the stored data. Symmetric or asymmetric secret keys can be used to ensure data privacy. Passport-issuing countries have the option not to encrypt the data.
- A digital watermark is used to protect the integrity of facial and iris image. Some digital bits may be buried into an image for further verification purposes without degrading the quality of the image.
- Unique IC chip serial numbers are used to prevent cloning of chips.
- A Public Key Infrastructure (PKI) for generation and management is required.

## 3. BIOMETRIC SYSTEM MODULES

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

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 issued to the individual.

Matching Unit: This 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: This module accepts or rejects the user based on a security threshold and matching score [1].

## 4. E-PASSPORT SYSTEM DESIGN

System design is a transition from a user-oriented document to a document oriented to programmers or database personnel. It goes through logical and physical design walkthrough before implementation.

## 4.1. 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 (SOD), each of these hashes should be signed by the issuing state.

**Table 1** E-Passport Logical Data Structure

| Data Group | Data Element |
|---|---|
| DG 1 | Document Details |
| DG 2 | Encoded Headshot |
| DG 3 | Encoded Face |
| DG 4 | Encoded Fingerprint |
| DG 5 | Encoded Palmprint |
| 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 |
| SOD | Security Data Element |

## 4.2. E-Passport Certification

The Biometric authentication procedure for electronic passports involves two processes - Registration and Verification. During the registration phase, the e-Passport applicant registers their biometric at a secure location under human supervision. A feature extraction program is used to encode this biometric data after which it is stored on the user's e-Passport Tag. For user authentication and identity Verification at an inspection terminal, the user is made to supply a

sample of their biometric. The same feature extraction algorithm is used to encode the freshly supplied biometric. A matching algorithm is run at the terminal to obtain the degree of similarity between the registered and supplied biometric. If the degree of similarity is deemed to be greater than a certain threshold value, the biometric is accepted and the user's identity is verified successfully. Unfortunately, without human supervision, it is not always possible to detect the use of prosthetics at the biometric registration or Verification stages. It is easy to see that biometric spoofing attacks will become easier to perform as automation increases and human supervision of the biometric process decreases [4].

## 5. IMPLEMENTATION OF E-PASSPORT SYSTEM

In order to implement this biometric electronic passport system for person identification using face, fingerprint, palmprint and iris recognition 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.

### 5.1. Public Key Infrastructure

In normal situations, certificate-issuing organizations known as Certificates Authorities (CA's) are grouped in a trusted hierarchy, where the children CA's trust the parent CA's. All CA's directly or indirectly trust the top-level Root CA. Revoking one certificate means all its children CA's are no longer trusted. 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.

### 5.2. 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, fingerprint, palmprint and iris data in the e-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 i.e. researcher can only establish that the face, fingerprint, palmprint and iris data on the Tag is correct, not the authenticity of the Tag itself. 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, fingerprint, palmprint and iris 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].

### 5.3. 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 e-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.

- 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 $KP_{uAA}$.

### 5.4. Basic Access Control

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 e-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].

### 5.5. Chip Authentication

The Chip Authentication protocol is aims to replace Active Authentication as a mechanism to detect cloned e-Passports. If CA 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 key agreement protocol. Note that the e-Passport Tag already has a Chip Authentication public key and private key (in secure memory).

### 5.6. Terminal Authentication

The Terminal Authentication protocol is a protocol that is executed only if access biometrics data is required. It is a challenge-response mechanism that allows the Tag to validate the Reader used in Chip Authentication. The Reader proves to the Tag using digital certificates that it has been authorized by the home and visiting nation to read e-Passport Tags.

## 6. E-PASSPORT PROTOCOLS

The ICAO e-passport is a complex protocol suite that consists of three sub protocols namely, BAC, PA and AA. Such a protocol suite is not only difficult to formalize, but also verification of such systems more often leads to an exponential state-space explosions. 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 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 BAC, the e-passport reader performs PA.
- The chip and the e-passport reader execute the AA protocol.

The e-passport authentication heavily relies on PKI. Researcher model only one level of certification hierarchy, up to the document signer and researcher assume that document signer public key is certified by its root (country signing authority) and, is valid and secure. This does not weaken the verification process of the e-passport protocol suite, but only indicates that the model assumes the “ideal” PKI implementation. Researcher also supposes that cryptographic primitives and face, fingerprint, palmprint and iris biometric used in the system like hash functions, MAC, and generation of keys are secure [8].

### 6.1. 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 ($PK_i$,$SK_i$) 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 an e-Passport are also certified by its root certification authority.

## 6.2. Phase One – Inspection System (IS) 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 chip.

Step 2 (P) The e-Passport 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 → 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 $K_{eP}$.

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

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.

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

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 $K_{IS}$.

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

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 $K_{ePIS.}$

### 5.2.3 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 $S_{eP} = SIGN_{SKeP} (MRZ \| K_{ePIS})$ 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, an 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. 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.

## 6. CONCLUSIONS

The work represents an attempt to acknowledge and account for the presence on e-passport scheme using face, fingerprint, palmprint and iris recognition, towards their improved identification. The application of biometric 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.

## REFERENCES

[1] A.K.Jian, "Biometrics personal identification in networked society" Technical report 1999.

[2] C.Hesher, "A novel technique for face recognition using range images" in the Proceedings of 7th International Symposium on Signal Processing and Its Application, 2003.

[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", Technical report, ICAO.

[5] KLUGLER, D. (2005), "Advance security mechanisms for machine readable travel documents, Technical report", Federal Office for Information Security (BSI), Germany.

[6] ICAO, "Machine Readable Travel Documents", Part 1 Machine Readable Passports, 5th Edition, 2003

[7] Riscure Security Lab, "E-passport privacy attack", Cards Asia Singapore, April 2006.

[8] D. Wagner, "Security and privacy issues in e-passports", Cryptology ePrint, Report 2005.

[9] ICAO, "Biometrics Deployment of Machine Readable Travel Documents", Version 2.0, May 2004.

## 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 30 technical papers and conference presentations. He is a reviewer for several scientific journals. His research interests are focused on advanced network, image processing, video processing, visual human-computer interaction, and multimodal 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.