Cancelable Biometric Transformations for E-Passport Security

P. Punithavathi, S. Geetha

Abstract*: *E-Passport or Electronic Passport is comprised of a microprocessor chip which contains biometric data used to authenticate the identity of passport holder. Facial image, fingerprint image and palm-print image are some of the currently standardized biometric modalities, embedded in the E-Passports. The privacy of the biometric data becomes a problem during storage and transmission. The biometric data cannot be revoked or re-issued unlike tokens or passwords, if compromised. The possibility of producing cancelable templates from the biometric features of user has been studied, thus eliminating threats to privacy and security of the biometric features. Cancelable template is obtained from original biometric image after intentional/repeated distortions (based on user-specific key), and thereby providing security to the templates. The distortions can be implemented either at signal or at feature level. The cancelable templates can be revoked or re-issued whenever required just by changing the user-specific key. The probability of applying cancelable transformations to secure the privacy of the biometric features in E-passport has been explored in the article.

Keywords*: *Biometrics, Cancelable biometrics, E-passport, Template Security, Transformed Template

I. INTRODUCTION

The ICAO – International Civil Aviation Organization [1] has imposed a set of rules for Machine Readable Travel Documents (MRTD), in 2004. Majority of the countries across the globe are following this specification is used as standard for the first generation of E-Passports. The specifications were comprised of several cryptographic algorithms to certify authenticity, security and privacy of personal data. Similarly a new mechanism called Extended Access Control "EAC" [2] was proposed by European Union in 2006. This EAC is comprised of Public Key Infrastructure and cryptographic protocols for improving security features of the personal data contained in the E-passport. This EAC suite has marked the era of second generation of E-Passports. Electronic passports, *E-Passport*, is comprised of an integrated chip. This chip inserted in the document's cover page contains biometric information of the passport holder. Biometric information aids in reliable authentication of the passport owner when compared with

non-biometric passports. As per the first specification of ICAO, the biometric information can be chosen from the images of several modalities like face, fingerprint and iris. Moreover, fingerprint data are mandatory for European Union passports, since 2009. Azerbaijan passports contain even palm-print of the passport holder from 2013. The biometric feature, also called as biometric template, is stored in JPEG form into the chip.

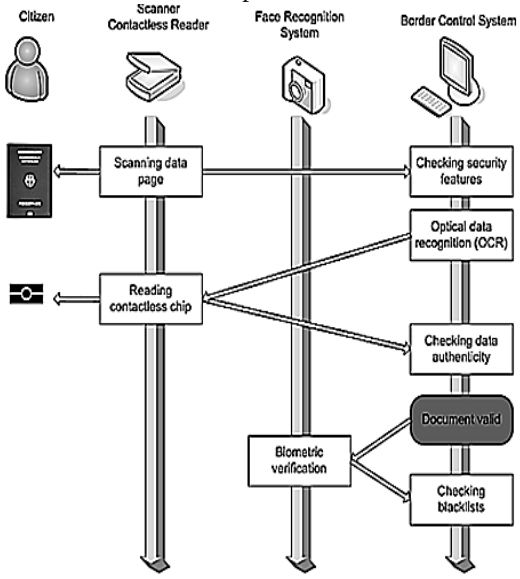

Fig.1. Flow diagram of E-gate **[3]**

The E-passport carried by the passport holder, is scanned by a contactless reader/scanner at the entrance of the Electronic gate or E-gate. At the same time, an image of the biometric feature of the passport holder is captured by the imaging device. This image is compared with the image stored in the contactless chip embedded in the passport to validate the passport holder. The entire flow diagram can be seen in Fig. 1.

II. NEED FOR E-PASSPORT

The E-Passport is comprised of all the personal information of the passport-holder, printed both in a digital and machine-readable format. Thereby the security of the personal information and identity of the passport holder is enhanced. The chances of passport forgery and fake passports can be minimized. The E-Passports play a vital role in the following applications:

Revised Manuscript Received on December 16, 2019.
***** Correspondence Author
P. Punithavathi, School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, Tamil Nadu, India. Email: p.punitavathi2015@vit.ac.in
S. Geetha*, School of Computing Science and Engineering, Vellore Institute of Technology Chennai Campus, Chennai, Tamil Nadu, India. Email: geetha.s @vit.ac.in

- Reducing illegal immigrations
- Cross-border security
- Provide smooth travel experience with online facilities
- Provide quick and protected border crossings
- Genuine trade practice
- Provide national security
- Minimize identity theft

III. LITERATURE SURVEY

Biometric enabled passports are described as E-passports [4]. Worldwide, such applications are handled by the government agencies. Recently several researchers have shown interest towards Basic Access Control (BAC) mechanism involving E-passports in accordance with ICAO standards. Juels et al. in [5] identified several flaws in traditional passports as Belgian, Dutch or German passports [6]. The Machine Readable Zone (MRZ) precisely holds the passport number, the date of birth of the holder and the expiry date of the passport. The critical information is stored on low entropy MRZ. Hence BAC is highly susceptible to brute force attack.

Some of the flaws in BAC have been corrected by Password Authentication Connection Establishment (PACE) in order to resist active attacks [7]. But the PACE technology was found to have several flaws by Chaabouni and Vaudenay [7].

The electronic chip can be invaded through prevailing threats. The crucial biometric information stored in the chip is thus under risk because biometrics once lost is lost forever and can never be compromised again. The perils of applying cryptographic algorithms [8], in securing the biometric information, has proved to be unsuccessful.

IV. SECURITY THREATS TO BIOMETRIC FEATURES STORED IN E-PASSPORT

Several Security threats to the biometric features in E-passport have been listed in this section as follows:

- Denial of Service – The genuine passport holders are denied of services due to overwhelming of resources. Hence the genuine passport holders are deprived of the services which have to be offered to them.
- Coercion – An imposter may force genuine passport holder to get the access to the E-gate system.
- Circumvention – An imposter may intrude or spoof to gain access to the data or resources of the genuine passport holder.
- Collusion – Due to the absence of well-defined user-privileges, a lot of confusion may occur.
- Repudiation – One of the genuine passport holders, may gain access to the E-gate and then make prerogative statements that imposter has breached the E-gate.
- Replay Threat – An imposter may use previous recordings of biometric features of genuine passport holder to possess access rights to the E-gate.
- Covert acquisition – An imposter may abuse the means of identity of the genuine passport holder, without his/her knowledge.
- Hill-climbing Threat – An imposter may flood the matching unit with synthetically generated templates. The imposter tries to generate an approximate replica of the biometric features of passport holder, by randomly modifying the biometric templates based on the match score output by the matching unit.
- Linkage Threat– An imposter may guess the biometric features of genuine passport holder by the output of template generation unit.
- Brute-force Threat – An imposter may send possessed biometric templates of genuine passport holder to the matcher until the matcher accepts one, erroneously thinking that it has been input by the genuine passport holder.

V. SECURING PRIVACY OF BIOMETRIC FEATURES IN E-PASSPORT USING CANCELABLE TRANSFORMATIONS

Cancelable biometrics system applies feature/signal level transformations on original biometric features based on user specific password or key. The matching is performed in transformed domain. The first attempt towards the direction of transformed biometrics was recorded by Soutar et al. [9], but the concrete notion of cancelable biometrics was yet formulated by Ratha et al. [10].

The cancelable biometric system has the following properties as per the guidelines of ISO/IEC FCD 24745 [11]. These properties make cancelable biometrics to become popular over traditional biometric systems.

- Non-invertibility: The cancelable transformation is strictly one-way. The original biometric features can never be reconstructed from the transformed template
- Diversity: Several transformed templates can be generated from a biometric feature. These templates never correlate with each other
- Revocability: If a template stored in database has been compromised, the generation of a new template is easy
- Performance: The cancelable transformation never deteriorates the recognition performance

The cancelable biometrics is a best technique to preserve the privacy of the biometric identities as mentioned in [12].

A. Enrolling Cancelable Fingerprint Template into Chip in E-Passport

The enrolment process involves generation of cancelable fingerprint template from binary fingerprint template using the random projection based cancelable transformation technique [13]. The benefits of using random projection based cancelable transformation are highlighted in [13]. To summarize the process, binary fingerprint features are generated from fingerprint image using the technique in [14]. A random matrix generation unit generates a Gaussian distributed random

matrix which will act as user-specific key. The random matrix projection unit projects the random matrix on the fingerprint features to achieve a cancelable fingerprint template which is stored into the chip. A copy of the random matrix is given to the user. This process is illustrated by Fig. 2.

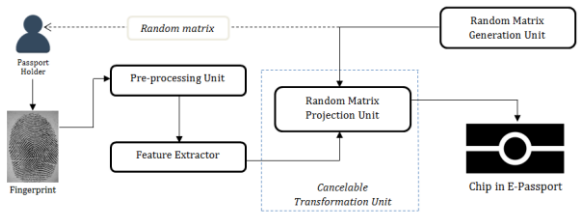

Fig. 1. Enrolling cancelable fingerprint template into chip in E-Passport

B. Authenticating Cancelable Fingerprint Template Stored in Chip of E-Passport:

During authentication procedure, the random projection matrix is provided by passport holder to the cancelable transformation unit to compute a transformed template corresponding to the biometric features of the passport holder. A one-to-one matching is performed to verify the identity of the passport holder. The individual's identity is verified by comparing the stored cancelable template and the query template. The process is illustrated by Fig. 3.

C. Re-Issuing Cancelable Fingerprint Template:

The biometric templates are stored in JPEG format in the chip. If it is compromised, it cannot be re-issued like tokens or passwords. The cancelable transformations on the other hand, offer the advantage of re-issuing a new transformed template even when the template stored in the chip is compromised. The process involved in re-issuing cancelable fingerprint template is as follows:

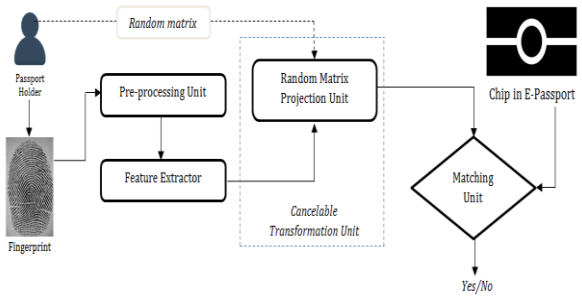

Fig. 2. Authenticating cancelable fingerprint template

Step 1: The cancelable fingerprint template (transformed template) and the transformation history (time during which the template was written onto the chip) is transmitted to a template genuineness verification module.

Step 2: The genuineness of the cancelable fingerprint template is checked by the verification module.

Step 3: If the cancelable fingerprint template has been found to be compromised, then a new cancelable fingerprint template generation process is triggered. A new cancelable fingerprint template is generated just by changing the random matrix.

Step 4: The chip is updated with the new cancelable fingerprint template.

Step 5: If the cancelable fingerprint template has not been compromised, then the same cancelable fingerprint template is retained on the chip.

The process has been described in Fig. 4.

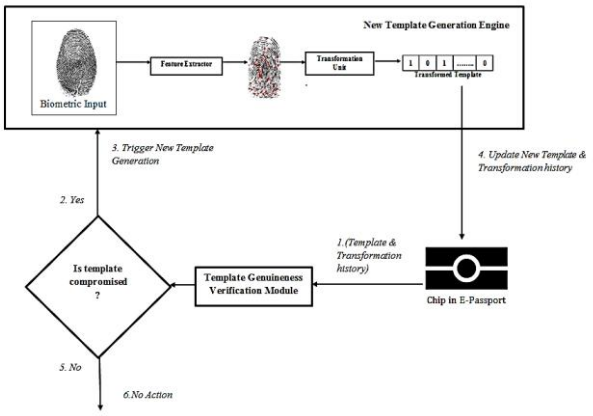

Fig. 3. Cancelable template revocation procedure

VI. BENEFITS OF CANCELABLE TEMPLATES OVER BIOMETRIC IMAGES IN E-PASSPORTS

The security (intrusion threats) of the biometric system and privacy (linkage threats) of the user is seriously challenged when a user's biometric template information is compromised by an imposter. Hence, the security and privacy of the biometric template is a critical problem that needs to be addressed to enhance the public acceptance of biometric technology. The cancelable transformation schemes have certain advantages like easy re-issuing and flexibility in the matcher design. If the cancelable fingerprint template has been compromised, the user-specific key (a random matrix in this case) is changed, i.e., the biometric template stored in the chip is updated. It is suggested to apply different transforms for different applications, to prevent impostors from tracking the genuine passport holders by cross-matching databases. In contrast to the biometric templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancelable biometric system.

VII. RECOGNITION ACCURACY OF PROPOSED SYSTEM

The performance of the cancelable templates generated using proposed transformation has been evaluated using recognition accuracy. The recognition accuracy represents the rate at which identity of owner of cancelable template can be verified. The more the accuracy rate, better is the performance. Table I summarizes the recognition accuracy of the proposed cancelable biometric system. The evaluation has been done using commonly used biometric modalities for immigration purposes like fingerprint and face with randomly selected images from FVC 2002 [15] and YALE [16] datasets, respectively. The randomly selected fingerprint

and face images were transformed using the proposed system as described with fingerprint modality in previous sections. The values indicate that the recognition accuracy is good.

Table I. Recognition Accuracy of the Cancelable Biometric System using Proposed System

Database	Modality	Recognition Accuracy (%) of Original Biometrics	Recognition Accuracy (%) of proposed System
FVC 2002 DB1	Fingerprint	96.78	**98.78**
YALE	Face	95.23	**97.23**

The Receiver Operation Characteristic (ROC) curve has been used to evaluate the recognition accuracy of the proposed system. Fig. 5 illustrates the ROC curves of the performance of the cancelable templates achieved for FVC2002DB1 and YALE datasets, respectively by applying proposed transformation.

The performance of the transformed templates has been compared with the performance of respective original biometric templates (without transformation). The transformed templates using proposed transformation have been found to perform better. The genuine and imposter have also been used to evaluate the recognition performance of the proposed system. The larger separation between impostor and genuine distributions indicates a better recognition performance. It is clear from Fig. 6 (a,b) that the recognition performance of the proposed system is good.

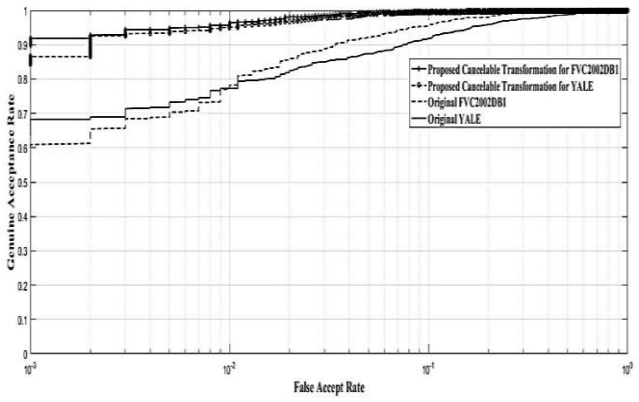

Fig. 5. ROC Curves for Proposed and Original Non-transformed Biometric Templates

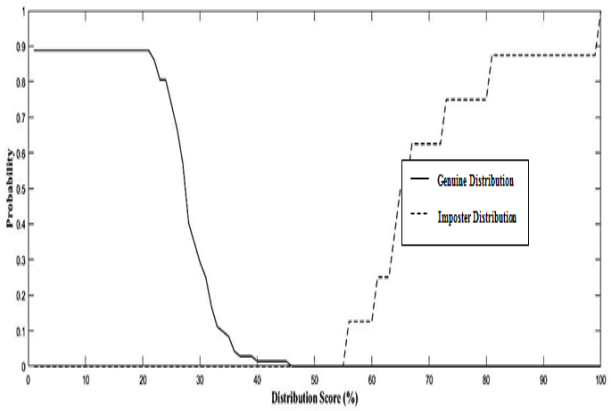

Fig. 6(a). Genuine and Imposter Distribution Curves of Proposed System for Samples from FVC2001DB1 Database

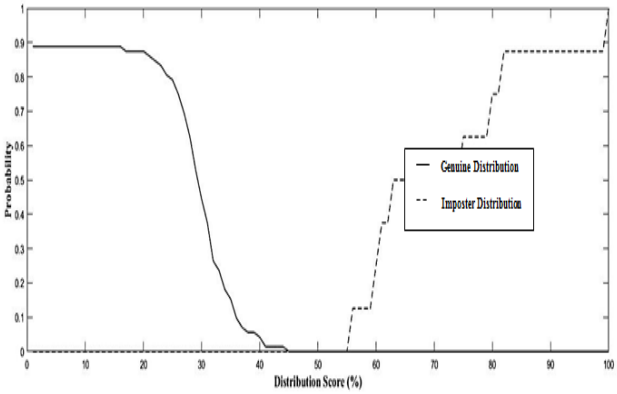

Fig. 6(b). Genuine and Imposter Distribution Curves of Proposed System for Samples from YALE Database

VIII. SECURITY ANALYSIS

A robust cancelable biometrics system must satisfy several requirements; namely, non-invertibility, diversity, and revocability. The security properties of the proposed system have been discussed in this section.

A. Non-invertibility Analysis

In the proposed work, cancelable templates have been generated from non-invertible and strong technique. These cancelable templates can never be inverted to original biometric features. This can be realized from [13]. Hence the proposed method is robust against template inversion attack.

B. Revocability and Diversity Analysis

The cancelable biometric system is revocable if it allows generation of a new key, in case the system storage is compromised, to construct a new template for biometric data belonging to same identity. In the proposed system, the random projection matrix is generated automatically during enrolment phase. In case of compromise, a new random projection matrix is generated during revocation phase. Therefore, the proposed system satisfies the revocability property.

Different cancelable templates generated out of a single biometric modality using corresponding random projection matrix in the proposed system never match with each other. On the other hand, each

individual can be enrolled in different biometric systems with different cancelable templates based on the random projection matrix. Thus, the proposed system satisfies diversity property.

IX. CONCLUSION

The privacy of biometrics stored in the chip of E-Passport, becomes essential because of the fact that the biometric features cannot be revoked. The biometric templates are currently being secured using well-known Triple Data Encryption Standard (3DES) cryptographic algorithm. Several methods have come up to break 3DES algorithm. Hence we presented the role of cancelable transformations in securing the biometric templates. Even though the solution is less interoperable but is more applicable when considering the privacy issues. We have highlighted the benefits of cancelable transformations through the experiments conducted on different biometric modalities – fingerprint and face. However the method is also extendable to transform other biometric modalities such as iris and palm-print which are used by several other countries for authentication.

ACKNOWLEDGMENT

The authors would like to thank the Management and Staff of Vellore Institute of Technology, Chennai Campus. The first author is supported by Visvesvaraya, Ph.D. Scheme, sponsored by Digital India Corporation, held by the Ministry of Electronics and Information Technology (MeitY), Government of India.

REFERENCES

1. "ICAO," [Online]. Available: https://www.icao.int/Pages/default.aspx.
2. "EAC," [Online]. Available: https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/SecurityMechanisms/securEAC/eac_node.html.
3. "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Biometric_passport.
4. V. Pasupathinathan, J. Pieprzyk and H. Wang, "An on-line secure e-passport protocol," Information Security Practice and Experience, vol. 4991, pp. 14-28, 2008.
5. A. Juels, D. Molnar and D. Wagner, "Security and privacy issues in e-passports," in First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.
6. G. Avoine, K. Kalach and J. J. Quisquater, "E-Passport: securing international contacts with contactless chips," in International Conference on Financial Cryptography and Data Security, 2008.
7. R. Chaabouni and S. Vaudenay, "The extended access control for machine readable travel documents," in Proceedings of the Special Interest Group on Biometrics and Electronic Signatures (No. LASEC-CONF-2009-016), 2009.
8. S. Geetha, P. Punithavathi, A. M. Infanteena and S. S. S. Sindhu, "A Literature Review on Image Encryption Techniques," International Journal of Information Security and Privacy, vol. 12, no. 3, pp. 42-83, 2018.
9. C. Soutar, A. Roberge and B. Vijaya Kumar, " Biometric Encryption using Image Processing," SPIE, pp. 17-188, 1998.
10. N. Ratha, S. Chikkerur, J. Connell and R. Bolle, "Generating cancelable fingerprint," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, pp. 561-572, 2007.
11. "ISO/IEC FCD 24745," [Online]. Available: https://www.iso.org/standard/52946.html.
12. P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan and K. K .R. Choo. "A lightweight machine learning-based authentication framework for smart IoT devices". *Information Sciences*, *484*, 255-268, 2019.
13. P. Punithavathi and S. Geetha, " (2017). Random Projection-based Cancelable Template Generation for Sparsely Distributed Biometric Patterns. I, 7(3).," Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 3, 2017.
14. S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," Pattern Recognition, vol. 47, no. 3, pp. 1321-1329, 2014.
15. F. V. Competition, 2002. [Online]. Available: http://bias.csr.unibo.it/fvc2002/.
16. "Yale face database," [Online]. Available: http://cvc.yale.

AUTHORS PROFILE

Punithavathi completed Bachelor of Engineering - Computer Science in 2007, and Master of Technology - Computer Science in 2014. She has achieved University Rank for M. Tech. She has four years of teaching experience. She is pursuing Ph. D. at VIT University, Chennai. She has been awarded with prestigious Visvesvaraya PHD Scheme supported by Media Lab Asia, Ministry of electronics and Information Technology, Government of India. Her areas of interest include biometric template security, image processing and multimedia security. She is a Life Member in HKCBEES and Student Member in IEEE.

Geetha is a Professor in School of Computing Science and Engineering, VIT University, Chennai Campus, India. She has received the B.E., and M.E., degrees in Computer Science and Engineering from Madurai Kamaraj University, India in 2000 and Anna University of Chennai, India in 2004, Ph.D. Degree from Anna University in 2011, respectively. She has 18+ years of rich teaching and research experience. She has published more than 80 papers in reputed International Conferences and refereed Journals. Her research interests include steganography, steganalysis, multimedia security, intrusion detection systems, machine learning paradigms and information forensics. She joins the review committee and editorial advisory board of journals like IEEE Transactions on Information Forensics and Security and IEEE Transactions on Image Processing, Springer Multimedia Tools and Security, Elsevier – Information Sciences. She has published 4 books. She has given many expert lectures, keynote addresses in international and national conferences. She has organised many workshops, conferences and FDPs. She is a recipient of University Rank and Academic Topper Award in B.E. and M.E. in 2000 and 2004 respectively. She is also the proud recipient of ASDF Best Academic Researcher Award 2013, ASDF Best Professor Award 2014, Research Award-2016, Performer Award – 2016, from VIT.