An E-Passport System with Multi-Stage Authentication: A Casestudy of the Security of Sri Lanka's E-Passport

Bhagya Wimalasiri[1] and Neera Jeyamohan[2]

[1] Asia Pacific Institute of Information Technology

Received: 16 December 2017 Accepted: 4 January 2018 Published: 15 January 2018

Abstract

E-passport or Electronic passport is one of the newly established research areas, especially since in the last few years there have been numerous reported attempts of illegal immigration across a number of country borders. Therefore, many countries are choosing to introduce electronic passports for their citizens and to automate the verification process at their border control security. The current e-passport systems are based on two technologies: RFID and Biometrics. New applications of RFID technology have been introduced in various aspects of people?s lives. Even though this technology has existed for more than a decade, it still holds considerable security and privacy risks. But together with RFID and biometric technologies an e-passport verification system can reduce fraud, identity theft and will help governments worldwide to improve security at their country borders. In 2017 Sri Lankan government proposed to introduce a new epassport scheme which will contain embedded RFID tags for person identification purpose. Therefore, this paper proposes a novel multi-stage e-passport verification scheme based on watermarking, biometrics and RFID.

Index terms— watermarking, e-passport, RFID, facial verification, signature verification, encryption, featurematching.

1 I. INTRODUCTION

-passports or electronic passports are a combination of traditional paper passports with an embedded Radio Frequency Identifier (RFID) tag. The RFID tag stores the information printed on the passport bio-data page along with additional biometric information (i.e., iris, fingerprint scans) of the holder. Being machine-readable, the concept of electronic passport improves the efficiency of the verification process at border control security. Concurrently the security of the entire passport authentication procedure is strengthened by e-passports with the duplication of bearer information printed on the bio-data page as well as the inclusion of biometric parameters. Many countries around the world have already adopted the use of electronic passports with the rest increasingly following in their footstep.

The security of an electronic passport system can be reinforced with the incorporation of a multitude of tactics that establish the owner's identity as well as remedy some of the inherent vulnerabilities of RFID

2 II. LITERATURE REVIEWS

Strengthening the security of e-passport systems has always been a sought-after research topic given its vitality to a fortified national defense system. With the adaptation of RFID as the principal technology in modern e-passport implementations, refining its security has become a leading research area given the hardware-based unsophisticated nature of the technology. Consequently, many security experts and academics have proposed various approaches to address known RFID vulnerabilities in the context of epassport systems as well methods to improve the security of passports systems overall.

Al-Hamami & Alhafez [1]have proposed the use of Diffie-Hellman key exchange Algorithm to share a private key between the RFID tag and the NFCimplemented Inspection System, while separately storing a unique watermark, inside the passport photo and the RFID tag. These stored watermarks will later be compared during the verification process to ensure that the Tag has not been cloned. Mehan et al. [2] suggested a method for authenticating electronic passports by using Elliptic Curve Cryptography (ECC) applied in the dual domain (i.e., spatial and frequency) where the passport holder's image is split into twin segments, and the holder's passport particulars are fragmented into two parts as well.

Wang et al. [3] proposed a two-stage verification method, where a person is enrolled, during which the image is watermarked, and authenticated established research areas, especially since in the last few years there have been numerous reported attempts of illegal immigration across a number of country borders. Therefore, many countries are choosing to introduce electronic passports for their citizens and to automate the verification process at their border control security. The current e-passport systems are based on two technologies: RFID and Biometrics. New applications of RFID technology have been introduced in various aspects of people's lives. Even though this technology has existed for more than a decade, it still holds considerable security and privacy risks. But together with RFID and biometric technologies an e-passport verification system can reduce fraud, identity theft and will help governments worldwide to improve security at their country borders. In 2017 Sri Lankan government proposed to introduce a new epassport scheme which will contain embedded RFID tags for person identification purpose. Therefore, this paper proposes a novel multi-stage e-passport verification scheme based on watermarking, biometrics and RFID.

technology itself. This paper proposes a system which utilizes a digital watermarking mechanism to establish owner's identity and to verify the integrity of the information stored in RFID tag. The system also comprised of encryption techniques to ensure the confidentiality of the information stored inside the RFID tag. The remainder of this paper will be structured as follows. Section 2 overviews the existing literature in the subject while section 3 addresses the security issues the proposed system attempts to solve. Section 4 discusses the proposed solution in detail. Experimental results obtained from the software simulation of the proposed system is analyzed in the 5 th section with the final section containing the concluding remarks.

when the watermark is extracted and verified. Their proposed system was based on multi-modal biometrics where both facial and palm samples of the user are extracted to produce the inputs.

The purpose of the approach suggested by Saeed et al. [4]was to increase the security of existing epassport protocols to eliminate the data leakage and tag-cloning threats associated with embedded RFID technology. They proposed the use of increased keysizes to avoid data leakage, storing the private key of the chip in an inaccessible location to prevent tagcloning. In the system suggested by Peeters et al. [5], they propose to ensure passport-bearer privacy by replacing the use of bootstrap from the low entropy value in the e-passport MRZ with a mutual authentication pattern. This method involves two authentication stages; a terminal authentication followed by an e-passport authentication. Viswanathan et al. [6]suggested a method that embeds an invisible watermark inside the passenger photograph, created using passenger's full name and passport number during the initial issuance of the passport. This method attempted at establishing a correspondence between passport's photo and its owner which could later be verified at border control.

3 III. SECURITY OF AN E-PASSPORT a) Establishing a link between facial image and biodata

One of the main prevalent issues in the e-passport authentication process is establishing a correspondence between the holder's facial photograph and the provided information. It is a common practice among illegal immigrants, blacklisted passengers, and other criminals to forge passport documents with their images and someone else's bio-data. Accordingly, it's evident that there is a requirement for a mechanism to bind the facial photograph of a passport holder with their information and be able to verify the authenticity of it.

4 b) Facial Image & Signature Verification

Forgery of passports using facial images resembling the valid owner of a passport and forging their signatures aren't entirely unheard of and is a practice that is continued to be carried out even to this day. According to an official authority at Department of Emigrations and Immigrations of Si Lanka, individuals have managed to manipulate the issuance office into issuing passports that necessarily did not contain their personal information. This type of counterfeit is done by trying to impersonate the legitimate owner of the information where the impersonator either accurately resembled the appearance of the authentic owner (i.e., twin sibling, relative) or managed to manipulate the appearance (i.e., change hair, wear make-up) to resemble the original owner. Similar kinds of attempts are carried out to falsify the hand-signatures of passport holders which necessitates the requirement of a system that allows for the detection of such forgeries.

5 c) Data Skimming

An inherent vulnerability related to the security of RFID technology is the ability to read the material stored inside an RFID tag, by any individual in possession of an RFID reader, since there isn't any default mechanism in place to encrypt the information stored within the tag. The danger of this threat lies in the fact that even a short distance, such as 3-foot, could allow an attacker to perform a skimming attack against an e-passport. Skimming poses one of the greatest threats related to e-passports since as per the mandate of the ICAO (International Civil Aviation Organization), epassports contain sensitive passenger information such as passenger name, date of birth and passport identification number [7]. Actual deployments will include biometric information, nationality, profession, and place of birth [7]. Hence, it's imperative to deploy a mechanism that ensures the confidentiality of the stored information within the RFID tag.

6 d) Tag Cloning

Cloning means that an adversary produces emulators of a genuine RFID transponder that behave identically and hence cannot be distinguished from the original transponder [8]. Although Baseline ICAO regulations mandate digitally signing e-passport data, which theoretically allows the RFID reader to validate that the data originated from the legitimate passportissuing authority, it still fails in binding the data to anepassport or RFID tag. Thus it provides no defense against potential cloning of e-passport tags [7]. This vulnerability requires being readily addressed to protect the integrity of any e-passport system.

7 e) The Validity of Information Stored Inside the RFID Tag

It's extremely vital that the border security can verify that an e-passport contains the exact data that was written in the tag during the issuance process. They should be able to authenticate that the information stored by the legitimate passport issuing authority has not been tampered with and that they can undeniably verify the authenticity of information stored inside the embedded RFID tag ensuring guaranteed national security.

8 IV. PROPOSED SOLUTION

The proposed solution addresses all the security concerns discussed under section 3, details of which are explained in this section. This phase takes place at Department of Emigration & Immigration of Sri Lanka where the passports are issued for individuals for the first time. The stages involved in the passport issuance process are individually discussed as follows.

9 a) Acquisition of Information

During this initial stage of the system, relevant information about the passport applicant will be acquired (i.e., applicant image, signature, full name, gender, assigned passport number, date and place of birth, profession, NIC number, nationality, type of passport, date of issue and date of expiration). The acquired data will be validated for the correct data input format (i.e., dates in DD/MM/YYYY format etc.) and the existence of mandatory fields (such as first and last names, passport number etc.). Failure of the input validation process will prompt the data entry operator to enter the data in the correct format or to complete all mandatory fields.

10 b) Watermarking the Facial Image

Watermark creation requires applicant first, second, third and family names and passport number as input parameters. A random four-digit numeric key will be generated using which each input parameter will be encoded to produce a numeric value. However, since not all applicants possess second and third names, in such cases a custom value will be assigned for those parameters. Using these encoded parameters, a numeric watermark and the location to store the generated watermark within the image will be calculated and the watermark will be embedded in the calculated location. The watermark will be embedded replacing the highest intensity of RGB channels at any calculated location. As illustrated in figure 1 The RFID tag contain all initially acquired information of the applicant. To prevent data skimming attacks the information stored in the RFID tag will be encrypted using AES. The key for the AES encryption will be randomly generated to contain 14 alphanumeric and special characters. All information initially acquired will be saved in a centralized passport holder information database. Additionally, all required watermark calculation values will be stored in the centralized watermarking information database, which will be used during the validation process to verify the recalculated watermark.

11 d) Save Information in Corresponding Databases

The key that was used for the AES encryption will also be centrally stored.

12 2) Passport Verification b) Verification of RFID-stored Information c) Facial Image Verification

During the second stage of the verification process, the facial image section of the scanned biodata page is compared against a centrally stored facial image template. The images are matched using the feature key-points based algorithm SIFT, which would display the number of best-matched key-points between the two images. If the number of similar key-points is equal or greater than a predetermined threshold, set based on experimental results, the two images will be verified as similar. Otherwise, the proposed solution will flag the bearer-image as a mismatch.

13 d) Hand-Signature Verification

This stage follows a verification procedure akin to the facial image verifications procedure. The section of scanned bio-data page where the bearer's signature is contained is extracted as an image and compared against the centrally stored template of the bearer signature that has been obtained during the issuance stage. The SIFT algorithm is again utilized here to detect identical key-points between the two images. Based on experimental results, a different threshold is set for signature verification, where the similarity of the two signatures is authenticated if the number of matched key-points is similar or greater than the determined threshold.

14 e) Recalculate and Verify Watermark

This is the final stage of the verification mechanism. The central database is accessed, and the bearer's full name and the key used for the initial watermark calculation is extracted. The watermark is recalculated using the retrieved information along with the bearer passport number in real-time. The recalculated watermark values (watermark plus storage location) are compared against the centrally stored values to ensure the legitimacy of the watermark thus establishing a correspondence between bearer information and their facial image. Furthermore, the watermark embedded inside the facial image (which is stored inside the RFID tag) is compared against the centrally stored watermark. This is done to ensure that the RFID tag is bound to the holder of the passport which confirms that the tag has not been cloned.

15 V. EXPERIMENTAL RESULTS

The prototype was developed using Python programming language version 2.7. As the inputs for the developed verification prototype, passport holder's passport number and the scanned bio-data page of the passport are acquired which proceeds the following multi-stage verification procedure.

16 a) Verify RFID Tag against the Central Server

As shown in figure 4, during this stage the information inside the RFID tag will be displayed against the centrally stored bio-data which is accessed using the passport number of the bearer. Under ideal circumstances, the information centrally stored must be identical to the information extracted from the RFID tag. As the first step of the verification process, using the passport number, the centralized passport holder information database is accessed, and the respective database record for passport holder is displayed. Simultaneously, the password for AES decryption of the RFID file is retrieved. The encrypted RFID file is then decrypted, and the information is displayed alongside the retrieved database information. Human intervention is required to verify the details and in this case the border-control official can decide whether or not the information presented in the passport and the information retrieved are similar. During this stage, the facial image contained in the scanned bio-data page is compared against the centrally stored image template of the passport bearer. As shown in figure 5 if the two images share a satisfactory number of identical key-points the porotype would declare them as authenticated. But as depicted in figure 6 if the two images do not contain a substantial number of similar key-points, i.e., the number of matching key-points are less than the desired threshold, the prototype will display an 'Image Mismatch' warning to the user. Correspondingly, during signature verification, the system will successfully authenticate if the two signatures, the scanned signature, and the centrallystored signature template, share the necessary number of similar key-points in between. But, if the system fails to detect the required number of similar key-points between the two images, then the system will warn the user that the signatures are a mismatch. The results are displayed in figures 7 and 8 respectively. During this final stage of verification, the watermark for the respective passport will be recalculated and compared against the centrally stored watermark and the watermark embedded inside the image stored in the RFID tag. If all three comparisons are identical, the system will conclude the process. ? ? ? ? 2 ? ? ? ? 3 ? ? ? ? 4 ? ? ? ? 5 ? ? ? ? 6 ? ? ? ? 7 ? ? ? ? 8 ? ? ? ?

17 VI. CONCLUSION

In this paper we propose a novel multi-stage authentication scheme that incorporates verification of data stored inside the RFID tag, watermarking, facial and signature authentication for e-passports. Information embedded within the RFID tag is first compared against the centrally stored bio-data to determine their similarity. The printed facial image and signature on the passport are compared against centrally stored items to validate their authenticity. As the final stage of the verification, the watermark embedded in the image stored inside the RFID tag will be recalculated and compared to establish owner identity as well prevent tag-cloning. All the

Figure 1:

1 

Figure 2: Figure 1 :

2


Figure 3: Figure 2 :

3


Figure 4: Figure 3 :

4

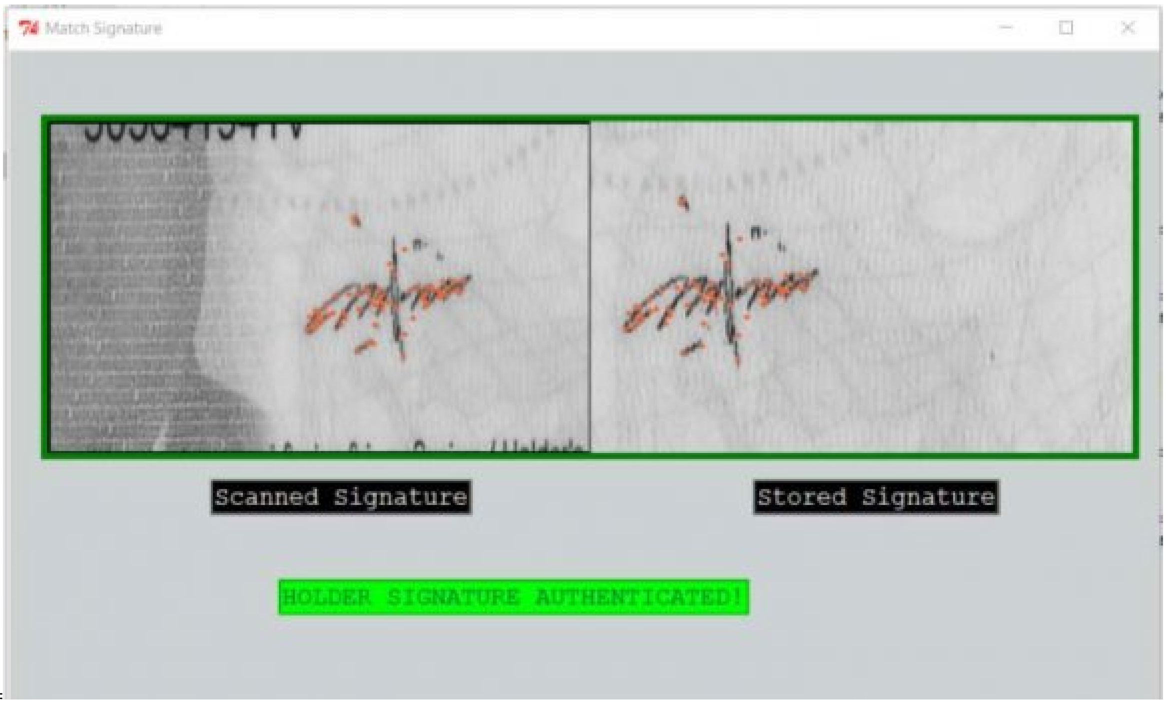

Figure 5: Figure 4 :

5

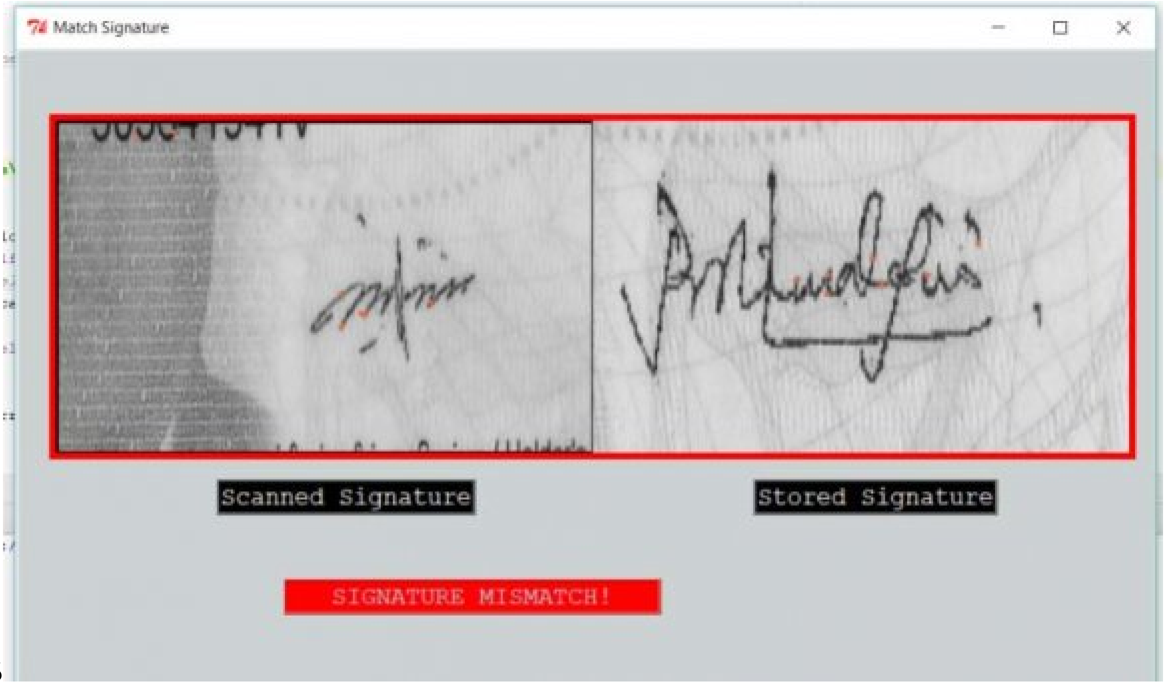

Figure 6: Figure 5 :

6

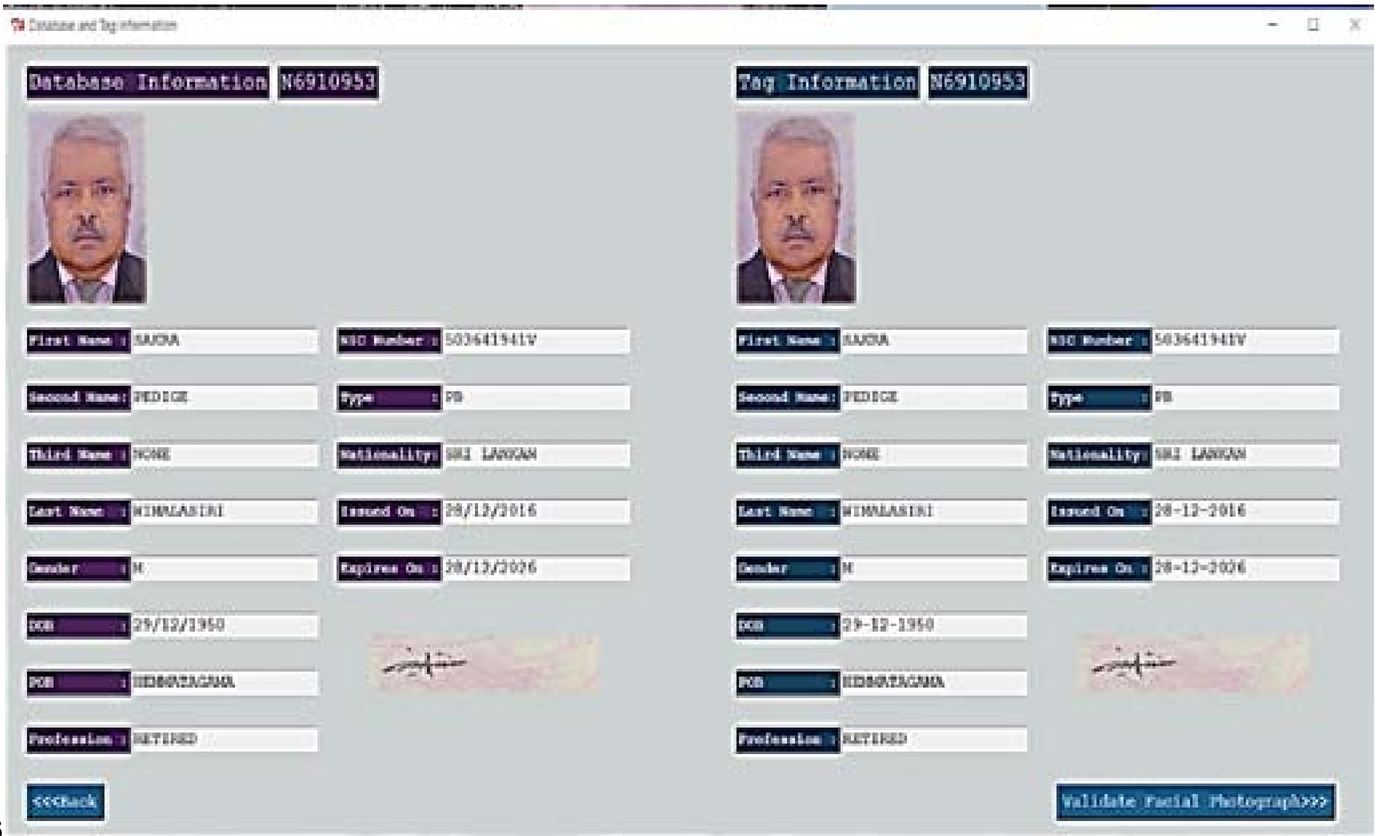

Figure 7: Figure 6 :

information stored inside the RFID tag is encrypted to eliminate skimming attacks. The experimental results reflect the functionality of the proposed solution at each stage. [1] [2] [3]

[1] An E-Passport System with Multi-Stage Authentication: A Case study of the Security of Sri Lanka's E-Passport

7

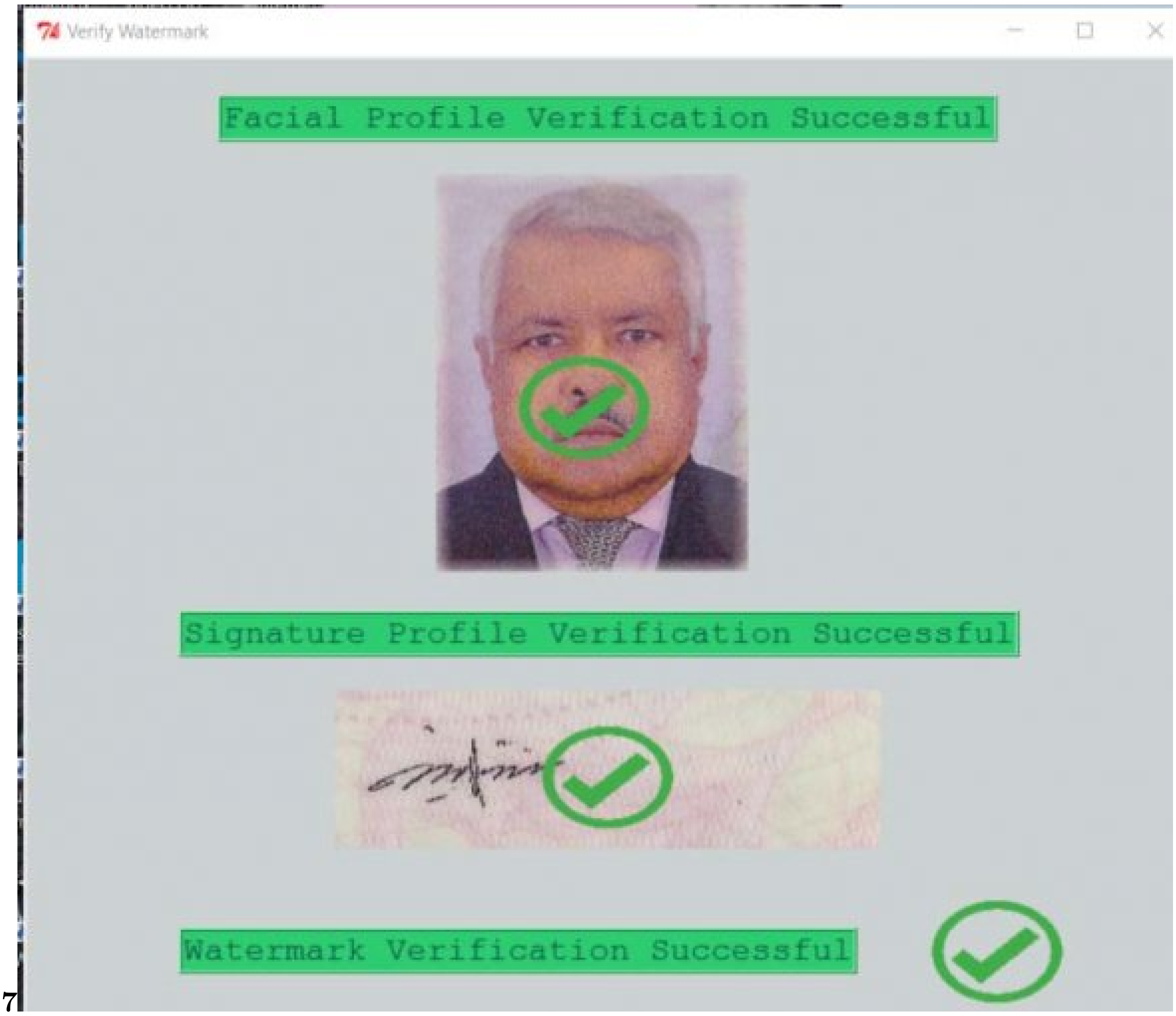

Figure 8: Figure 7 :

1

Passport	RFID Verification	Information	Facial Image Verification	Signature Verification	Watermark Verification
1					

Figure 9: Table 1 :

[Viswanatham et al. ()] *An Improved Authentication Scheme for Passport Verification Using Watermarking Technique*, V M Viswanatham , G S Reddy , P Jagadeesh , M D Reddy . 2012. 9 p. .

[Al-Hamami and Alhafez ()] 'Enhancing Security to Protect E-Passport against Photo Forgery'. A H Al-Hamami , M A A Alhafez . *Glob. J. Comput. Sci. Technol* 2016. 16 (6) .

[Miodrag et al. ()] B Miodrag , S David , S Ivan . *Rfid Systems Research Trends and Challenges*, 2013. 53.

[Mehan et al. ()] *Secure Electronic Passport Certification using Re-water Marking*, V Mehan , R Dhir , Y S Brar . 2013. 16 p. .

[Saeed et al. ()] *Securing ePassport System : A Proposed Anti-Cloning and Anti-Skimming Protocol*, M Q Saeed , A Masood , F Kausar . 2004. p. .

[Juels et al. ()] 'Security and Privacy Issues in ePassports'. A Juels , A Molnar , D Wagner . *Secur. Priv. Emerg. Areas Commun. Networks* 2005. 2005. p. .

[Peeters et al. (2014)] *Speedup for European ePassport Authentication / Shattering the Glass Maze*, R Peeters , J Hermans , B Mennink . September. 2014. 1 p. .

[Liu (2014)] 'The study of recent technologies used in E-passport system'. Y Liu . *IEEE Glob. Humanit. Technol. Conf. -South Asia Satell. GHTC-SAS* 2014. 2014. July. 2014. 3 p. .