DETECTION OF FORGERY AND FABRICATION IN PASSPORTS AND VISAS USING CRYPTOGRAPHY AND QR CODES

Cheman Shaik

VISH Consulting Services Inc, 6242 N Hoyne Avenue, Chicago IL 60659, USA
cheman_shaik@rediffmail.com

ABSTRACT

In this paper, we present a novel solution to detect forgery and fabrication in passports and visas using cryptography and QR codes. The solution requires that the passport and visa issuing authorities obtain a cryptographic key pair and publish their public key on their website. Further they are required to encrypt the passport or visa information with their private key, encode the ciphertext in a QR code and print it on the passport or visa they issue to the applicant.

The issuing authorities are also required to create a mobile or desktop QR code scanning app and place it for download on their website or Google Play Store and iPhone App Store. Any individual or immigration authority that needs to check the passport or visa for forgery and fabrication can scan its QR code, which will decrypt the ciphertext encoded in the QR code using the public key stored in the app memory and displays the passport or visa information on the app screen. The details on the app screen can be compared with the actual details printed on the passport or visa. Any mismatch between the two is a clear indication of forgery or fabrication.

Discussed the need for a universal desktop and mobile app that can be used by immigration authorities and consulates all over the world to enable fast checking of passports and visas at ports of entry for forgery and fabrication.

KEYWORDS

Passport, Visa, Forgery, Fabrication, Cryptography, Encryption, Decryption, QR Code, Mobile App

1. INTRODUCTION

Passport is an important travel document issued by a Government to its citizens after a rigorous scrutiny and background check of the applicant. Similarly, visa is a permission to enter a foreign country issued by their consulate in the applicant's country of residence.

Passport and Visa forgery and fabrication is a serious concern for almost every country of the world as the holders of such forged documents might commit various types of crime and anti-social activities such as financial scams, bank fraud, drug trafficking, alien smuggling, illegal entry to advanced countries and terrorist activities [1].

Criminals and anti-social elements forge passports and visas by modifying the particulars on the original documents or fabricate entirely new documents. Usually, a passport or visa consists of two different zones, visual inspection zone and machinereadable zone. The Visual inspection zone contains all the details of passport or visa such as the type of passport, country code, name of the passport holder, nationality, sex, date of birth, place of issue, date of issue, date of expiry

etc. The machine readable Zone is printed at the bottom in OCR-B form which is readable with the OCR-B reader used by immigration/border authorities [2].

The issuing authorities also incorporate multiple security features in passports and visas, such as invisible images, watermarks, tiny fluorescent paper fibers, micro printing, invisible page numbers, heat activated ultra violet film etc. The assumption behind these security features is that fraudsters can't reproduce them. However, fraudsters are more updated and ahead of investigators and forensic specialists [2].

Passports and visas consist of some hidden features that are not visible to the naked eye but can be viewed in different light. These features include intaglio printing that creates a raised rough texture on the background page, optical variable ink that changes color based on the angle it is viewed, and UV light that makes the false documents glow under light [3].

2. LITERATURE SURVEY

In 2004, Kwang-Baek et al proposed a novel passport recognition method that supports code extraction using smearing method and contour tracking algorithm and code recognition using the enhanced Radial Basis Function (RBF) network [4]. However, sophisticated passport and visa forgers and fabricators can accordingly modify the code at the bottom of the passport or visa to exactly match the details printed on the passport or visa.

In 2007, Young-Bin et al proposed a method of extracting the characters from the passport main page and inserting them in the MRZ (Machine Readable Zone). If the data in the passport is not identical with the data decoded from the MRZ, it implies the passport is fabricated [5]. However, the passport and visa forgers and fabricators can accordingly modify the MRZ code also to match the data printed on passport and visa.

In 2008, Kwang-Baek et al further proposed passport recognition and face verification methods which can automatically recognize passport codes and discriminate forgery passports based on passport code and fonts [6]. However, this method is not foolproof as the forgers and fabricators can maintain the same codes and fonts using advance printing technology.

In 2014, Suman et al proposed a system to detect fraud in documents based on the height, orientation and intensity value of the pixels in the forged content [7]. However, this detection can be escaped by coping characters of the forged words from the same document.

In 2015, Romain Bertrand et al presented a method to detect forgery in documents based on the fonts, styles and sizes of characters. The method detects forgery based on the difference of character spacing in the forged content with that in the remaining document. However, for sophisticated forgers it is not difficult to identify the font, style and size of the original document and use the same in the forged content [8].

In 2019, VeriDoc Global developed a software solution that suggests embedding a Secured QR code on a passport with a unique digital hash inside the QR code. The same hash is placed on the blockchain network for security, verification, and most important end-user validation [9]. However, blockchain is a complicated, heavy weight solution to detecting forgery and fabrication in passports and visas.

3. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography, also called asymmetric key cryptography, uses two different keys for encryption and decryption. It is used for secure communication between two unknown parties

over an insecure communication channel. The public key and private key are generated using a key generation equation and hence the two keys are mathematically related. One can not be derived from the other with today's existing computing power even with a cluster of super computers.

The public key is shared publicly whereas the private key needs to be kept highly confidential. Any compromise of the private key will directly lead to compromise of the communication made between the two parties involved. RSA, ECC, ElGamal and NTRU are the trusted, tested and proven public key cryptosystems in the industry. The security of these encryptions comes form the hardness of solving their underlaying mathematical problem [10].

4. QR CODES

QR code is a two-dimensional matrix of black data modules over a white background. It is mostly square shaped though sometimes it could be rectangular when the surface it needs to be printed on is cylindrical. A QR code can contain a website address, web page link, a plain text of binary, numeric, alphanumeric, Japanese, Chinese or Korean characters. The number of characters stored in a QR code depends on the type of characters as different characters require different size of bits to represent.

A QR code may be used to encode contact details, business card, product information, YouTube video link, Social Media link, location on Google Maps and so on. QR code is tolerant to partial damage and works properly even if it is partially damaged due to its format information section storing data about error correction rate. A QR code is surrounded by a thick white order which differentiates itself from the background images [11] [12] [13].

5. APPLYING CRYPTOGRAPHY AND QR CODES ON PASSPORT AND VISA

In this section we present a solution to detect forgery in passports and visas. The solution requires that the foreign affairs department of every country obtain a cryptographic key pair and publish their public key on their website in the form of QR code. It facilitates easy integration of the public keys in any QR code scanner apps installed on smart phones and desktops. Passport and visa holders and immigration authorities of all countries around the world can integrate the public keys of various countries into their scanning applications.

Further, the foreign affairs departments are required to create a QR code scanning mobile app and provide it for download on their website, Google Play Store and iPhone App Store. Their public keys should be stored in their app memory.

When the foreign affairs department of any country issues a passport to their citizen or visa to a foreign national, they should encrypt the passport or visa particulars with their private key and generate a ciphertext. The ciphertext should be encoded in a QR code which must be printed on the passport or visa.

Any individual who received a passport or visa from an agent wants to check it for forgery or fabrication can download the QR code scanner app on his/her smart phone from the foreign affairs department's website, Google Play Store or Appstore and scan the QR code. The scanner app reads the ciphertext encoded in the QR code, decrypts it with the public key already stored in its memory and displays the details of the passport such as the name, gender, date of birth, type of passport, place of issue, issue date, expiry date etc. The passport holder can verify the details by comparing them with the details printed on the passport. Any mismatch of the details is a clear indication of forgery.

Similarly, to check the validity of a visa, the visa holder needs to down the QR code scanner app from the visa issuing authority's website and scan the QR code on the visa.

When the QR code on a visa is scanned, the scanner app reads the ciphertext encoded in the QR code and decrypts it with the issuing authority's public key already stored in its memory and displays the details of the visa such as the visa holder's name, date of birth, visa type, validity etc. The visa holder can check the details for correctness and compare them with the details on the visa. Any mismatch of the details is a clear indication of forgery in the visa.

Figure 1 below shows a specimen passport for illustration purpose. Such a passport can be verified for forgery or fabrication by immigration authorities only by checking the features such as hologram, invisible images, watermarks, microprinting etc. However, incorporating the same features in forged and fabricated passports is only difficult but not nearly impossible. Forgers and fabricators are getting more and more sophisticated day by day with technology.

Figure 1 A specimen passport without any QR code

In QR coded passport or visa, before printing it all its details are captured and encrypted with the issuing authority's private key. The ciphertext generated by the encryption is encoded in a QR code which is printed on the passport or visa. Table 1 below shows the passport details and the QR code encoding the ciphertext generated on encryption.

Passport Details Captured	QR Encoding the Details
Visa Type: P Issuing Country: BEL Passport No: EM000000 Surname: PEETERS Given Name: EMMA Date of Birth: 12 12 1994 SEX: F Place of Birth: BRUXELLES Date of Issue: 18 04 2014 Date of Expiry: 17 04 2021 AUTHORITY: SPF AFFAIRES ESTRANGERES	

Figure 2 below shows a specimen passport with the same QR code printed on it.

Figure 2 A specimen passport with QR code

When the passport holder or any immigration authorities want to check the passport for forgery or fabrication at the time of entry at a port, they can download the scanner app of the passport issuing authority and scan the QR code which will display the same details mentioned in the passport, if it is genuine.

Table 2 below shows QR code scan of the passport and the details captured in the scan. The captured details should be verified with the details printed on the passport. Any mismatch of the details is a clear indication of forgery or fabrication. As the passport is not forged or fabricated, the details captured in the QR code scan exactly match the details on the passport

QR code scan of the passport	Passport Details Captured from QR Code Scan
	Visa Type: P Issuing Country: BEL Passport No: EM000000 Surname: PEETERS Given Name: EMMA Date of Birth: 12 12 1994 SEX: F Place of Birth: BRUXELLES Date of Issue: 18 04 2014 Date of Expiry: 17 04 2021 AUTHORITY: SPF AFFAIRES ESTRANGERES

Table 2 QR code scan of passport and the details captured in the scan

6. QR CODE SCAN OUTPUT OF FORGED PASSPORTS AND VISAS

When a forger or fabricator modifies or completely changes the content in a genuine passport or visa bearing a QR code, he or she has two options, either leaving the QR code as is or replacing the actual QR code with his own QR code encoding the new content encrypted with his own private key. Fig.3 below shows a forged specimen passport leaving the QR code as is.

Figure 3 A forged specimen passport with QR code

In the above passport the forger has changed the surname and given name of the passport holder. When the passport holder or immigration authorities verify the passport with the QR scanning app of the issuing authorities, it will display the original details of the passport whereas the passport shows different details.

Table. 3 below shows the content on the forged passport and the content captured in the QR code scan.

Content Displayed from the QR code scan	Content Printed on the Passport
Visa Type: P Issuing Country: BEL Passport No: EM000000 Surname: **PEETERS** Given Name: **EMMA** Date of Birth: 12 12 1994 SEX: F Place of Birth: BRUXELLES Date of Issue: 18 04 2014 Date of Expiry: 17 04 2021 AUTHORITY: SPF AFFAIRES ESTRANGERES	Visa Type: P Issuing Country: BEL Passport No: EM000000 Surname: **JACOBS** Given Name: **ANNA** Date of Birth: 12 12 1994 SEX: F Place of Birth: BRUXELLES Date of Issue: 18 04 2014 Date of Expiry: 17 04 2021 AUTHORITY: SPF AFFAIRES ESTRANGERES

As the passport holder's name from the QR code scan result mismatches with the one printed on the passport, it is a clear indication of forgery.

On the other hand, if the forger prints a different QR code that he generated using his own private key, it will produce a totally junk text on the QR code scan by the verifier, which will again prove forgery of the passport.

Similarly, when the QR code on a visa is scanned, it will produce content that mismatched the information on the visa, thereby proving forgery or fabrication.

7. PASSPORT INFORMATION ENCODING IN QR CODE

First, before printing a passport the passport, the issuing authority's software application should collect all the passport details such as the passport holder's surname, given name, date of birth, sex, place of issue, issue date and expiry date etc., and form a plain string by concatenating them all. The formed plain text string should be encrypted by the software application with the issuing authority's private key and the generated ciphertext should be encoded in a QR code which should be printed on the passport main page.

Encryption may be performed using a tested, proven public key cryptography algorithm such as RSA and ECC. The current industry standard bit length for RSA key is 2048. The plain text string of the passport details M may be encrypted to a ciphertext C as follows:

C = Me mod n where e is the private key exponent and should be kept secret.

Encode the ciphertext C in a QR code and print it on the passport ready for issue.

When a passport holder, the issuing authority or any foreign immigration authorities want to check the passport for forgery or fabrication at a port of entry, they can download the scanner app of the issuing authority and scan the QR code, which will capture the ciphertext encoded in it and decrypt it using the public key already stored in the app memory to obtain the original information M as follows:

M = Cd mod n where d is the public key exponent.
n is the key modulus which is common on both sides.
The plain text M regenerated in the QR code scan should be compared with the actual details printed on the passport. Any mismatch between the two is a clear indication of forgery or fabrication.

Similarly, for visa verification at a port of entry, the immigration authorities can scan the QR code on the visa with their own QR code scanning app and compare the scan result with the details printed on the visa.

In a generic use case of any public key cryptography such as email communication and ecommerce transactions, encryption is performed with the public key, and decryption with the private key. However, in this case of forgery and fabrication checking, encryption should be performed with the private key, and decryption with the public key. This is because the public is on the verification side and the private entity is on the issuing side.

Another mandatory requirement that needs to be strictly met while creating the cryptographic key pair is that the encrypting key exponent e should not be taken as a small number like 3 or 65537 which is a usual practice in regular encryption use cases. The encrypting key exponent e must be the same order as the key modulus n. Otherwise, it would make it very easy for the attacker to find out the right e value that will generate the right QR code to be printed on the passport or visa to escape detection of forgery and fabrication.

8. IMAGE ENCODING IN QR CODE

The passport or visa holder's image also can be encoded on QR code. However, as the QR code has limitation on its storage size, it is not possible to encode the entire image. A checksum or hash of the binary string representing the image pixels can be computed and encoded as an

additional field in the QR code. This will detect forgery of the image also. When a verifier scans the QR code, the scanning application should run the same checksum or hash function and compare it with the value encoded in the QR code. Any mismatch indicates forgery or fabrication of the image.

9. A UNIVERSAL MOBILE AND DESKTOP APP FOR ALL COUNTRIES

Every day immigration authorities need to check thousands of passports at ports of entry, and therefore checking each passport with the corresponding country's scanning app would be cumbersome and time consuming due to country switching from passport to passport.

A universal desktop app may be developed for the use of immigration authorities, integrating the public keys of all countries of the world. Depending on the country the passport belongs to, the public key of the country may be fetched form the app memory and the ciphertext encoded in the QR code may be decrypted for comparison with the details printed on the passport. To enable automatic detection of the country from the QR code, passport issuing authorities may append the ciphertext in the QR code to their three-letter country code followed by a space, for example, "IND ciphertext" for Indian Passport. When the QR code scanner scans the QR code, it extracts the encoded text from the QR code and splits it into the country code and ciphertext, and based on the three-letter country code in the first token the country's private key is fetched from the app memory and the ciphertext is automatically decrypted for forgery and fabrication check.

A consortium of all world countries may be formed to direct the countries to create their cryptographic keys and share their public keys to be integrated in the universal scanning app. Advanced counties such as USA and UK may take the lead to develop such a universal scanning app and share it with the rest of the world countries.

10. SECURITY CONCERNS FOR GLOBAL IMPLEMENTATION

Security is not a concert for global implementation of passport and visa with encrypted QR codes through a universal scanning application because it does not require any private keys to be integrated in such a global application. The scanning application requires only public key of different countries' to be integrated in it. In public key cryptography public key is a public chunk of information that should be shared openly with the outside world, without which secure communication is not possible.

The private key of any public key cryptosystem should be saved with utmost security measures to prevent hacker and intruders from compromising it. However, the implementation of encrypted QR codes does not require any private key to be integrated in the distributed scanning application because the decryption by passport or visa holders or foreign immigration authorities require only the public key. Private key is required only by the passport or visa issuers at the time of encrypting their details.

11. ASSUMPTIONS AND LIMITATIONS

A strong assumption in implementation of the encrypted QR code passports and visas is that all issuing authorities of these documents securely store their private key with stringent security and access control measures. If the private key is compromised, the issuing authority should replace it with a new and also replace their public key in the scanning application. The details of the passports and visas issued there on should be encrypted with the new private key.

A limitation of QR code is it can store maximum 4296 alphanumeric characters. The size of the passport or visa information that will be encode in the QR code should be within this limit. For Chinese and Japanese characters, the limit is 1817 characters. However, the content of passport main page or visa is well within this limit.

12. BENEFICIARIES OF THE SOLUTION

The proposed solution will be useful to a multitude of beneficiaries including:

- individuals who want to check their own visas forgery and fabrication
- immigration authorities allowing entry to foreigners at their ports of entry
- consulates around the world who issue visas to foreigners.
- other government departments that issue identity documents such as driving license, state id, social security number etc
- banks who open accounts to new entrants in the country
- banks that open non-resident accounts to their customers working abroad
- hotels that rent rooms to foreigners in their country

Many people travel to the gulf countries for employment from India and other Asian countries. They all obtain visas in their passports through employment agents. There were several incidents where the job seekers were cheated with fake visas and eventually leading them to deportation. With this solution visa holders can check their visas for forgery and fabrication before travel using the issuing authority's scanning app.

13. ADOPTION AND IMPLEMENTATION

Once few countries adopt the practice of issuing QR coded passports to their citizens and QR coded visas to foreigners, all other countries realize its benefits and quickly join the initiative. The formation of a global consortium and the release of a universal app discussed in the previous section would be a great thrust to the adoption of this solution.

The solution can be quickly developed without requiring a huge team and resources. It requires only obtaining a cryptographic key pair by each country and include some enhancement in their passport and visa printing software for encryption and QR code encoding.

Even before the formation of the global consortium of the world countries, interested countries can individually implement this solution in their passport issuing centers, immigration ports and their consulates around the world.

14. ENCRYPTED QR CODES VS BLOCKCHAIN

Blockchain is a public, shared, distributed ledger of records stored on a network of nodes. Information stored on blockchain is nearly impossible to tamper. However, blockchain is very complicated technology that brings its advantages with lot of challenges.

In order to maintain the passport and visa information, each country needs to have its own blockchain. On the other hand, if the country joins a common global blockchain of all countries, it needs to meet lot of technical and management challenges, including maintenance of own nodes, resiliency, efficiency, data backup and recovery, governance, audit, privacy and confidentiality.

On the other hand, cryptography and QR codes offer a very light weight, low-cost solution to issue tamper proof passports and visas, without any dependencies on other countries.

15. CONCLUSION

Passport and visa forgery is a serious concern for almost all countries of the world, especially the advanced countries. The motive behind crossing borders with forged and passports and visas could be drug trafficking, smuggling and terrorist activities. Detecting forgery and fabrication in these travel documents is essential for the immigration authorities at their ports of entry.

In this paper we presented a technical solution to detect forgery and fabrication in passports and visas using cryptography and QR codes. The solution requires that passport and visa issuing authorities obtain a cryptographic key pair and publish the public key in the form of QR code on their website or trusted app stores and securely store the private key. Also, their passport and visa printing software should be enhanced to extract the passport and visa details and encrypt the information with the private key. The generated ciphertext should be encoded in a QR code which should be printed on the passport or visa.

Further, the issuing authorities should create a mobile or desktop app and place it on their website, or any trusted App Store for download. Any passport or visa holders or immigration authorities can download the app and verify the travel documents for forgery and fabrication by scanning the QR code. When a QR code is scanned, the scanning app will extract the ciphertext encoded therein and decrypts it with the public key of the issuing authorities stored in the app memory and displays the details of the passport or visa. The displayed details should be compared with the details printed on the document. Any mismatch between the two is a clear indication of forgery or fabrication.

A consortium of all world countries may be formed and a universal scanning app may be developed wherein the public keys of all countries can be integrated. Such an app will be very useful to all travelers and immigration authorities around the world.

A future work recommendation for passport and visa issuing authorities of any country conduct a proof-of-concept and run a pilot project implanting the idea and report their success and document any challenges faced during the implementation.

DISCLAIMER

The passport shown in the figures is only a specimen passport obtained from Google search and used in this paper only for the purpose of illustration of the proposed solution.

REFERENCES

1. U.S Department of State, "Passport and Visa Fraud: A Quick Course", https://2009-2017.state.gov/m/ds/investigat/c10714.htm
2. Reeta R Gupta and N Ravi, "Passport Forgery and Forensic Examination of Indian Passport", Journal of Forensic Sciences & Criminal Investigation - Volume - 5 Issue - 1 September 2017
3. Miss A.M Investigations, “How to spot a fraudulent document”, https://missaminvestigations.co.uk/2018/10/15/how-to-spot-a-fraudulent-document/
4. Kwang-Baek, KimYoung-Ju, KimAm-Suk Oh, "An Intelligent System for Passport Recognition Using Enhanced RBF Network", International Conference on Computational and Information Science CIS 2004: Computational and Information Science pp 762-767.

5. Young-Bin Kwon and J.-h. Kim, “Recognition based verification for the machine readable travel documents,” in International Workshop on Graphics Recognition (GREC 2007), Curitiba, Brazil. Citeseer, 2007
6. Kwang-Baek Kim, Sungshin Kim, "A passport recognition and face verification using enhanced fuzzy ART based RBF network and PCA algorithm", Neurocomputing, Volume 71, Issues 16–18, 2008, Pages 3202-3210
7. S. V. Patgar, K. Rani, and T. Vasudev, “An unsupervised intelligent system to detect fabrication in photocopy document using variations in bounding box features,” in Contemporary Computing and Informatics (IC3I), 2014 International Conference on. IEEE, 2014, pp. 670–675
8. R. Bertrand, O. R. Terrades, P. Gomez-Kramer, P. Franco, and J.-M. Ogier, “A conditional random field model for font forgery detection,” in Document Analysis and Recognition (ICDAR), 2015 13th International Conference on. IEEE, 2015, pp. 576–580
9. VeriDoc Global, "What can be done about passport fraud right now?", https://veridocglobal.medium.com/what-can-be-done-about-passport-fraud-b6d5cb5e0370
10. dtos-mu.com, "UnderstandingThe BasicsofPublic Key Cryptography", https://www.dtos-mu.com/understanding-the-basics-of-public-key-cryptography/
11. Scanova Blog, "What is a QR Code: A Beginner’s Guide", https://scanova.io/blog/what-is-a-qr-code/
12. Chinmay Jathar, Swapnil Gurav, and KranteeJamdaade, "A Review on QR Code Analysis", International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 8, Issue 7, July 2019
13. uQR.me, "30 Things You Should Know About QR Codes", https://uqr.me/blog/things-you-should-know-about-qr-codes/

AUTHOR

Cheman Shaik is a Research & Development professional in Computer Science and Information Technology for the last twenty years. He has been an inventor in these areas of technology with eight U.S Patents for his inventions in Cryptography, Password Security, Codeless Dynamic Websites, Text Generation in Foreign Languages, Anti-phishing Techniques and 3D Mouse for Computers. He is the pioneer of the Absolute Public Key Cryptography in 1999. He is well known for his Password Self Encryption Method which has earned him three U.S Patents. He has published research papers in the international journals – IJCSEA, IJCIS, IJNSA and the proceedings of EC2ND 2006 and CSC 2008.