ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 9 (2022) No.4, pp.72-90
DOI:10.33168/LISS.2022.0406

Multi-Factor Verification of International Passports

Wen Dong Ng. Eng-Thiam Yeoh

Multimedia University, Malaysia
etyeoh@mmu.edu.my (Corresponding Author)

Abstract. This paper describes the design and development of a passport verification Web service. This service allows users to check and confirm their passports by submitting a snapshot of the passport's principal data page. The techniques used for developing the verification Web service included Python, Flask, OpenCV, and Tesseract OCR methods. The difficulty of generating a high accuracy verification result owing to numerous environmental elements, such as the quality of the uploaded images, the angle of the uploaded images, content tampering is the research focus of this project. We propose a multi-factor verification to increase the accuracy of verification thus reducing the probability of a fraudulent passport. The multi-factor verification is to combine the landmark detection, security feature detection, and fraud detection. In landmark detection, the algorithm will detect various landmarks on the passport document. Some of the landmarks containing text could be further processed to obtain additional information for verification. For security feature detection, the algorithm will detect security elements on the passport document which varies for different countries. For fraud detection, the algorithm will perform blurriness detection and validity detection to verify the information detected for the authenticity of the passport document. A set of passport images for Malaysia, Singapore, and Indonesia is used to test the algorithms. The results showed that the combined multi-factor verification slightly improved the verification compared to the separate algorithms.

Keywords: passport verification, multi-factor verification, landmark detection, security feature detection, fraud detection, Web service

1. Introduction

Verification of international passports is an important action in many applications, particular for financial and security transactions. It is an essential step to determine the identity of the users performing the transactions in the applications.

In mobile applications, the passport image is captured and processed to determine the validity of the passport. In this process, the images are separated into key features that are used to identify and verify the users based on specific criteria. These key features include the algorithms from three main different aspects such as landmark detection, security feature detection, and fraud detection. This research aims to investigate whether the verification accuracy can be improved by integrating these aspects into a multi-factor verification algorithm. The research will be based on typical passport documents from 3 countries (Malaysia, Singapore, and Indonesia) captured using common mobile devices and processed through a Web service.

2. Literature Review

2.1. Web Service

Web services are becoming increasingly popular and widely used because they enable better connectivity between different computers and applications regardless of the programming language or operating system they are written in, as well as the network communication protocols used to exchange data. Web Service contain 3 entities which are service providers create web services and publish them to the public, service requesters who are responsible for finding required services and requesting to use existing Web services by sending an XML request to be addressed and the registry is responsible for maintaining a registry where Web service providers can publish new services or find existing ones.

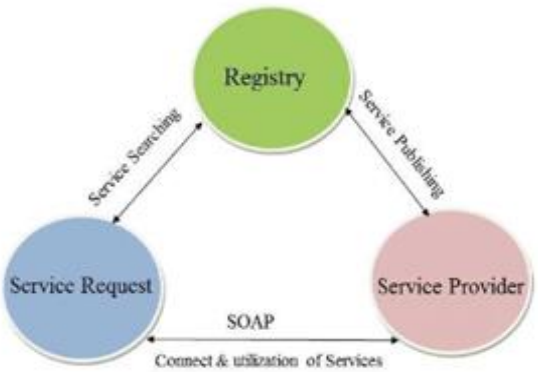

Fig. 1: Web Service Architecture.

The SOAP technique is used to provide a Web service, and it has a very simple form that contains an XML element with two children elements. The header and body

are the two elements, and the elements are expressed in XML. Web Service Description Language (WSDL) which specifies Web Service interfaces and provides users with a point of contact is one of the components. The Universal Description, Discovery, and Integration (UUDI) component is responsible for providing a method for clients to register and identify web services and dynamically interact with them.

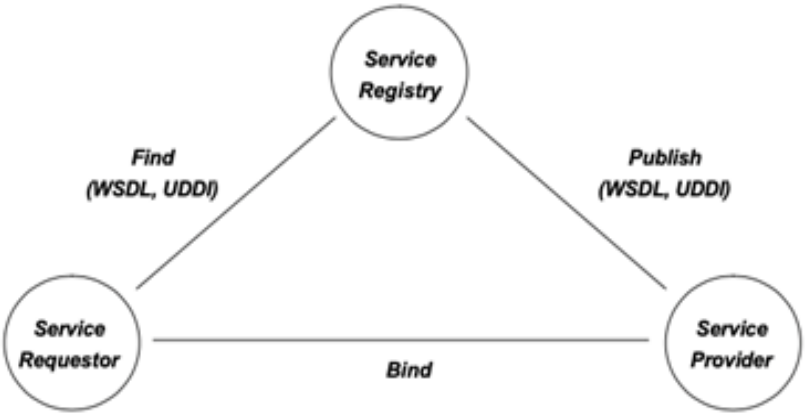

Fig. 2: Web Service Architecture.

A series of messages is used to accomplish Web Services interactions between nodes that may either send or receive messages, or both send and receive messages. It's a piece of software that sits in between a customer and a service provider, passing information and providing some form of value-added functionality. Discovery is the process of determining the location of a Web service to which a connection will be made, and the description includes the structural metadata about the interface used as well as textual document contents. The message format is required for encoding the communication between the client and the Web service, whereas transport is a platform for sending the message between partners.

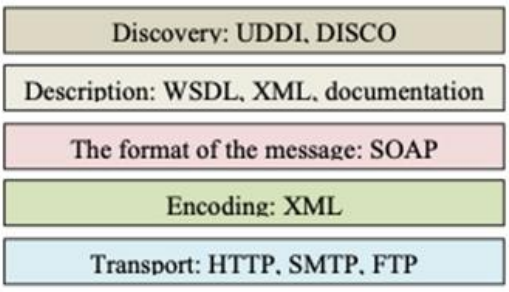

Fig 3: Main building blocks of web services.

2.2. Landmark Detection

Landmark detection is one of the techniques used in verifying the passport as it is essential for detecting and tracking key points from a human face. For example, a human's head position and rotation may be detected by using the key points. Face landmark identification may be accomplished with the help of Dlib, which is a library for implementing machine learning and computer vision solutions. However, even though it is a C++-based library, it may be used in conjunction with Python as well. On the other hand, landmarks in image processing may be described as visual characteristics that are chosen for a number of computer vision related to image measurement, registrations, camera calibration, and motion tracking, amongst other things. Landmark detection also can be done by using OpenCV. The functions in the OpenCV library can be applied to mark the essential information on the passport images.

2.3. Security Feature Detection

Each passport designed by a country across the world has certain security elements. The holographic pictures are a standard characteristic of passports. International Civil Aviation Organisation (ICAO) Doc 9303 specifies that structural characteristics comprise verifiable information based on their physical structure and can be read by machines. Examples of the security features on the passport are UV dull paper, a watermark, machine-readable optically variable ink, guilloche design, invisible fluorescent threads, and more. Moreover, another examples of security features printed on passports include holograms and microprint. This is to prevent anyone from readily counterfeiting the passport and using it for ill and improper reasons. Holograms are one such example. It is printed on the personal information page and will be seen when the passport is slanted from left to right. Aside from the hologram, the passport's data information page also had a microprint printed on it. The reproduction procedure is made more difficult by the microprint printed on the passport.

Fig. 4: Microprinting applied on the passport.

2.4. Fraud Detection

Fraud detection is a technique which attempts to prevent someone's property from

being falsified or acquired through false pretences. The phases of the fraud detection include the font checking, photocopy detection and blurriness detection. For example, the typeface used on the United States' data page is written in special protection fonts with characteristics such as small bleeds, bumps, and other defects that make it difficult to forge. Furthermore, photocopy detection ensures that the passport picture provided by the user is from the genuine holder and not a forgery. The blurriness detection in the fraud detection is used to ensure the image submitted by the user is clear to be seen and it can be achieved by using Python and with OpenCV.

3. International Passports

A passport is a government's official document that contains information about an individual's identification and allows them to travel abroad without being detained. The document certifies the holder's personal identity as well as his or her nationality. The design and format of a passport are distinct. When it comes to passport information, the most fundamental pieces of information to include are the complete name, picture, birthplace and birthdate, signature, and the expiry date of the passport. ICAO publishes passport standards which are considered suggestions to national governments by the international community. Passport booklets are normally sized in line with the ISO/IEC 7810 ID-3 standard, which specifies a dimension of 125, 88 mm for the booklets itself. A format known as B7 is used for this size. Personal information on a passport comprises the kind of passport, country code, name, nationality, birthdate, personal identification number which is optional, sex, birthplace, date of issuance, authority, date of expiration, and the holder's signature. The code "P" for passport, the code for the issuing nation and the passport number are all located at the top of the identification page. The primary photo is on the left side. Other countries may optionally include the passport holder's height and security elements, such as a smaller, see-through photo.

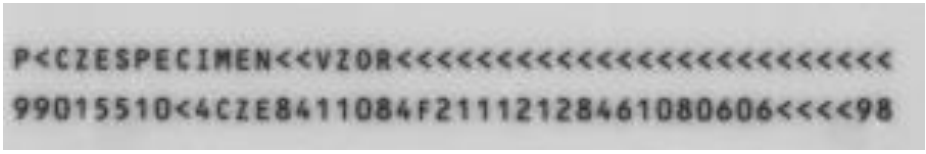

Fig. 5: Microprinting applied on the passport.

The bottom’s serial number and the symbols are the machine-readable zone. The newest EU passports, like other biometric passports, have a machine-readable zone that includes the name, nationality, and the majority of the information on the identification page. It is created in this format so that computers can read the information reasonably quickly while also being human readable because it comprises only letters (A–Z), numbers, and "<" as a space character. Non-English

letter names are normally printed properly in the visible zone of the passport, which is non-machine-readable, but are mapped into A-Z in the machine-readable zone according to ICAO requirements.

3.1. Difference between Malaysia, Singapore and Indonesia Passports

This research studies passport images from three countries - Malaysia, Singapore and Indonesia. The Malaysia passport is a passport issued by Malaysia's Immigration Department to Malaysian nationals. The Passport Act of 1966 is the major piece of legislation that governs the creation of passports and travel documents, as well as their ownership by anyone entering and exiting Malaysia.

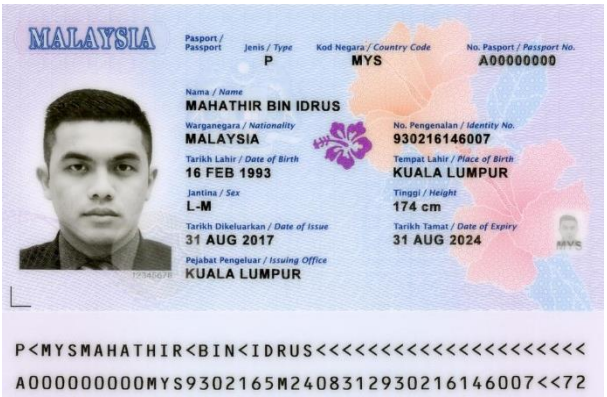

Fig. 6: Example of Malaysia Passport

The Singapore passport is a travel document and passport issued by the Republic of Singapore to its residents and nationalities. It allows the holder to freely enter and depart Singapore, as well as travel to and from other countries, subject to visa regulations. On behalf of the Ministry of Home Affairs, the Immigration and Checkpoints Authority (ICA) issues all Singapore passports.

Fig. 7: Example of Singapore Passport

The Indonesia passport is a travel document provided by the Indonesian government to Indonesian nationals who live in the country or abroad. The Directorate General of Immigration, which is part of the Ministry of Law and Human Rights, is the principal governmental authority in charge of passport issuing, possession, withdrawal, and other connected affairs.

Fig. 8: Example of Singapore Passport

All passports contain the necessary personal details on the identification page but there are some additional information or landmarks displayed for every different country. The table below shows the difference of the landmarks printed on the Malaysia, Singapore and Indonesia passports.

Table 1: Difference Landmarks of 3 Countries Passports

Country ---------- Landmarks	Malaysia	Singapore	Indonesia
Malaysia Word	✔	✖	✖
Singapore Word	✖	✔	✖
Indonesia Word	✖	✖	✔
Bunga raya	✔	✖	✖
Height	✔	✖	✖
Modification	✖	✔	✖
Multiple Laser Image	✖	✔	✖
Registration Number	✖	✖	✔
Nikim Number	✖	✖	✔

The additional personal information in Malaysia passports are the holder's height. The modification and multiple laser image is only printed on the Singapore passports while the Indonesia passports contain the registration number and nikim number. Besides that, the position of country word is different for each country. Figure below shows the position of the printed country name for Malaysia, Singapore and Indonesia passports.

Fig. 9: Position of Country Word for 3 Countries

4. Verification Factors

Multi-factor verification is a process which combines the results of three detection algorithms when processing passport images. The detections included in this verification are the landmark detection, security features detection and fraud detection.

4.1. Landmark Detection

In the landmark detection, a block will be generated to detect the information and extract it from the image. For different country passport, the data extracted from the information page will be slightly different. The data require to be extracted from the passport images is shown in Table 2. After labelling the landmarks, OCR will be performed on textual landmarks. Then, the extracted information will be stored and displayed to the users.

Aside from the essential information, some other features on the passport's information page will be detected during this detection. For example, the country name printed on the top left corner of the page as well as the machine readable zone printed beneath the passport, will be processed. Some other landmarks will also be detected so to be used in the next detection such as the coats of arms logo of each country.

4.2. Security Feature Detection

After the landmark detection, the passport images will undergo another verification process which is to check on the passport security features. After the system has obtained the resized passport image and has printed security features of the passport, the image will be compared with the template stored using template matching method in OpenCV which is the mse function. This function will match the submitted

passport images with the template stored and compare the patch of the input image under the template image. The comparison results will then be saved and are shown to the users at the end of the verification.

Table 2: Extracted data from 3 Countries Passports

Information	Malaysia	Singapore	Indonesia
Nationality	✔	✔	✔
Passport Type	✔	✔	✔
Height	✔	✖	✖
Date of Birth	✔	✔	✔
Sex	✔	✔	✔
Issuing Office	✔	✔	✔
Machine-Readable Zone	✔	✔	✔
Country Code	✔	✔	✔
Passport Number	✔	✔	✔
Name	✔	✔	✔
Identity Number	✔	✔	✖
Place of Birth	✔	✔	✔
Date of Expiry	✔	✔	✔
Date of Issue	✔	✔	✔
Modification	✖	✔	✖
Registration Number	✖	✖	✔
Nikim Number	✖	✖	✔

4.3. Fraud Detection

Following the security feature detection, fraud detection is the next. Blurriness detection is the part of the fraud detection process. A blurriness detecting algorithm will be used to guarantee that the image submitted is viewable. If the user uploads an image that is blurry, the system will return an error notice to the user. The system will define a function to determine the image blurriness. While the percentage of the blurriness is high, the system will return a result showing that the image is blurred and vice versa. After that, the overall percentage of blurriness is saved. At the

conclusion of the verification procedure, the user will be able to see the percentage of blurriness present.

5. Experimental Design

Figure 10 shows the flow chart for the passport verification procedure. The system will first take a picture of the user's passport information page and send it for verification. The image is initially subjected to landmark detection, which is a procedure that extracts the necessary information from the passport for the verification process. The information retrieved from the passport data page contains all of the personal information as well as the holder image on the passport and MRZ. The retrieved information from the passport is then stored and displayed to the users at the end of the verification process. Then, the security features detection will be carried out. The overall verification result will be stored and displayed to the user at the end of the verification process. The templates used for the template matching are taken from the sample data. The security features of each country passport images are cropped and applied in the mse function.

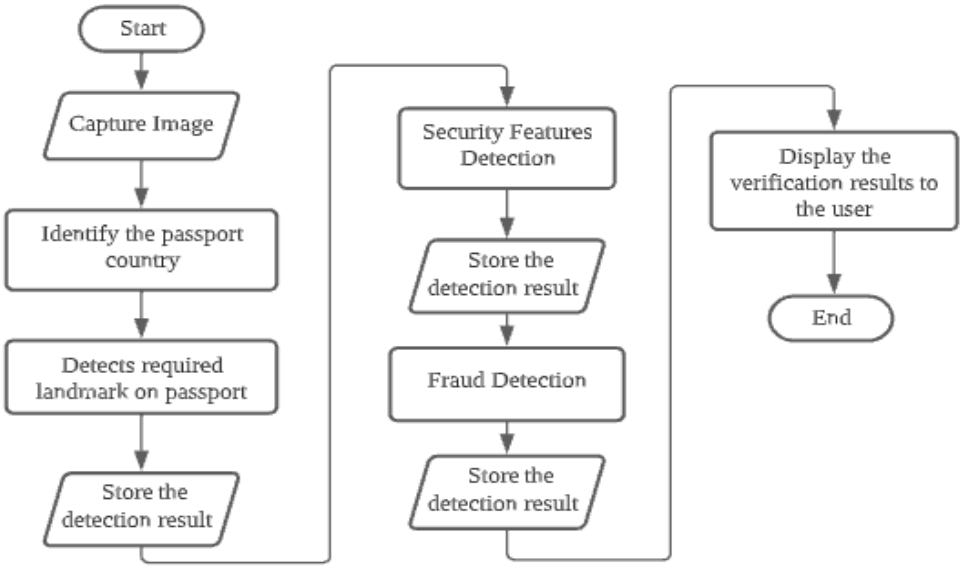

Fig. 10: Verification Process Flow Chart

Following this procedure, the passport image will go to the next phase, which is the fraud detection. This is to verify that the passport image submitted is genuine and not acquired under fraudulent pretenses. The steps to be performed in the fraud detection process are blurriness detection followed by format validity. In format validity, the items such as face image and iconic landmarks are checked for

conformance to the passport format. At the end of the passport verification, all of the results obtained and the status of the verification process are shown to the users in the Web service. There are 22 sample data utilised in the testing to test on the developed passport verification.

Fig. 11: Example of Template for Image Matching

Fig. 12: Sample Data Used for Verification

To calculate the score for each detection, the following equations are created and applied. All the results will be displayed in percentage.

For landmark detection, the score of the detected landmarks and the accuracy of the extracted landmarks will be calculated. In order to get the percentage of the detected landmarks, Equation (1) is applied.

$$Total\ detected\ score = \frac{Total\ detected\ landmarks}{Total\ landmarks\ to\ be\ detected} * 100 \quad (1)$$

Then, the total score achieved while checking the accuracy of the landmark detection can be calculated by using Equation (2) as follows:

$$Total\ extracted\ score = \frac{Total\ extracted\ landmarks}{Total\ landmarks\ to\ be\ extracted} * 100 \quad (2)$$

After getting the detected score and the extracted score, the overall score of the landmark detection need to be calculated. The overall score is shown in Equation (3) as follows:

$$Overall\ score = \frac{Total\ detected\ landmarks\ score}{Total\ extracted\ landmarks\ score} * 100 \quad (3)$$

Beside getting the landmark detection score, the security feature detection and fraud detection total score are also calculated. For calculating the overall score for security feature detection, Equation (4) is applied while Equation (5) is used to calculate the total score for fraud detection.

$$Overall\ score = \frac{Total\ detected + Total\ matched}{(Total\ to\ be\ detected\ and\ matched) * 2} * 100 \quad (4)$$

$$Overall\ score = \frac{Total\ detected}{Total\ to\ be\ detected} * 100 \quad (5)$$

After getting all the score for each detection, the overall score of the passport verification is calculated. To calculate the overall score, Equation (6) is applied.

$$Overall\ score = \frac{Lm(t) + Sf(t) + Fd(t)}{D} \quad (6)$$

where Lm(t) represents the landmark detection total score, Sf(t) represents the security feature total score, Fd(t) represents the fraud detection total score and D represents the total number of detections taken during the verification process. The cumulated scores from every detection are added together and divided by the total number of detections taken during the verification. The overall score is the final verification score which is used to determine whether the whole passport verification is passed or failed.

6. Results and Analysis

The sample data used to test the verification consists of 5 Malaysia passports images, 5 Singapore passport images and 12 Indonesia passport images. These 22 sample data do not include defective passport images. This section discusses the results of the overall verification process.

6.1. Landmark Detection

Figure 13 shows the landmarks detected and accuracy of data extracted from 3 countries passport images. The blue, yellow and orange lines represent the percentage

of the detected landmarks and all of the three percentage are 100%. This indicates that all the landmarks printed on the passport images are detected. The red line shows the percentage of accuracy for the extracted data from Malaysia passport images while the green line represents the Singapore accuracy percentage and sapphire blue line represents the Indonesia ones. The total average accuracy for data retrieved from Malaysia passports is 32.86 %, whereas it is 28.57 % for Singapore passports and 17.38 % for Indonesia passports. The angle of the passport images provided is the most important factor for the low accuracy rate. This caused a slightly mispositioning of the images which affected the accuracy of data extracted. The inaccuracy of the extracted data from landmark detection has also impacted machine-readable zone information checking.

Other landmarks such as the coat of arms logo of the country and iconic landmarks on the passport images are also identified. The higher the percentage, the more precise and well-matched the landmarks are. Figure 14 shows the statistics of fraud detection where the red bar represents the Malaysia landmarks matched percentage, purple bar represents Singapore and blue bar represents the Indonesia ones. The average of matched landmarks in Malaysia passports is around 66.67% while is 100% for the Singapore passport images and 69.44% for the Indonesia passport images.

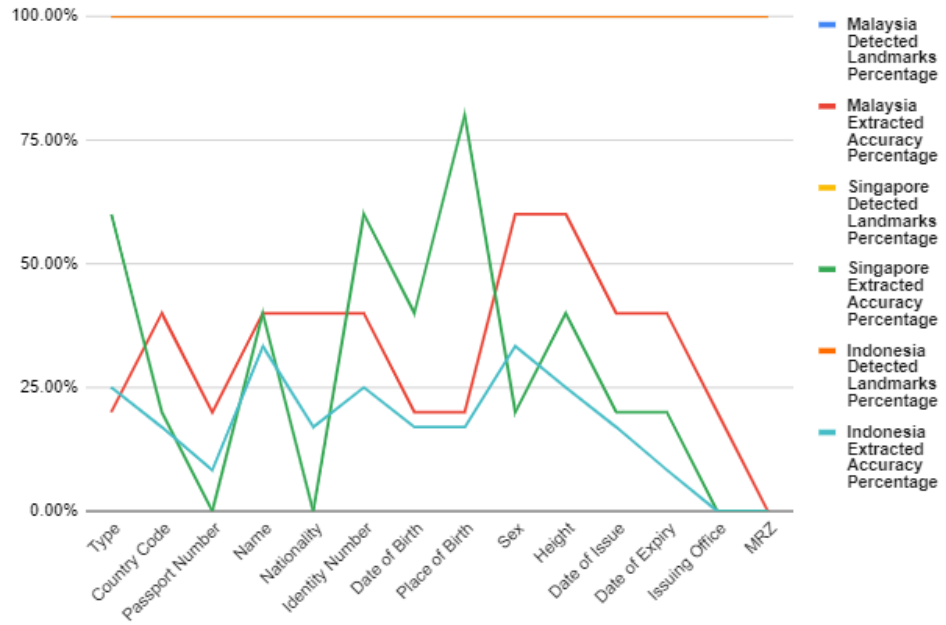

Fig. 13: Passport Landmarks Detected and Extracted Accuracy of 3 Countries

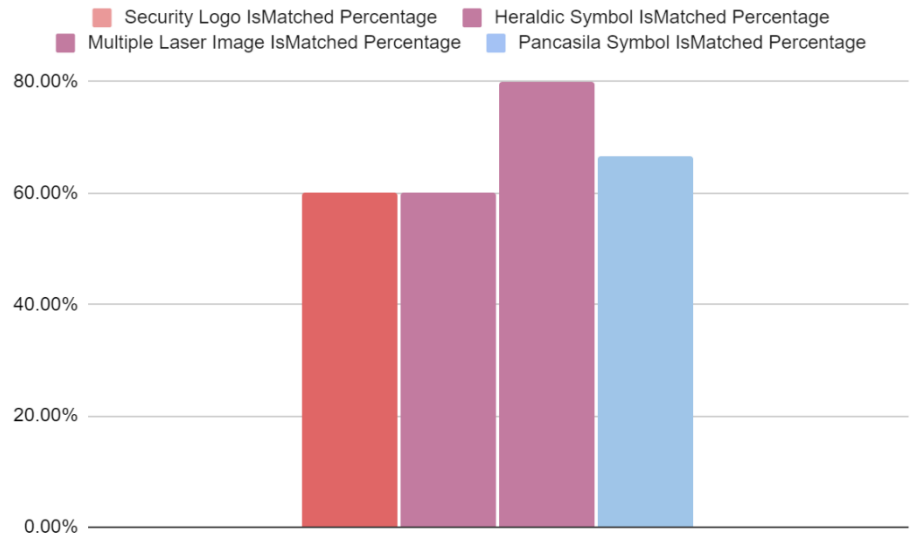

Fig. 14: Others Landmarks Matched Percentage of 3 Countries Passports

6.2. Security Feature Detection

The total score for the identification of security features on each country's passports is calculated. There is no microprint on the three nation passport information page. All the three countries' passport images have achieved positive results in the detected security features. This indicates that all the security features printed on the passport images are detected. Besides that, the matched percentage of the security features with the template are recorded. The security logo printed on the information page of Malaysia passports are 60% matched with the template saved, whereas the threshold value of the security logo is 20 and this is shown in Figure 15 where the purple bar represents the percentage for security logo matched percentage of Malaysia passports.

The two yellow bars represent the matched percentage of heraldic symbol and multiple laser images. The matching proportion of the heraldic symbol identified on passport images is 60%, while the matched percentage of the multiple laser image is 80%. The security elements of Singapore passports have both threshold levels of 20. This means the Web service will determine that the security features are matched with the template store while the compared result is equal to or greater than 20. For the Indonesia passports, they obtained quite good experimental results for the security features with a value of 66.67% shown by the green bar.

6.3. Fraud Detection

The results obtained from the fraud detection of the three countries passport images is shown in Figure 16. The blue bar represents the percentage for Malaysia passport images, the pink bar represents the percentage for Singapore passport images while the green bar holds the percentage of the Indonesia passport images obtained front

the fraud detection.

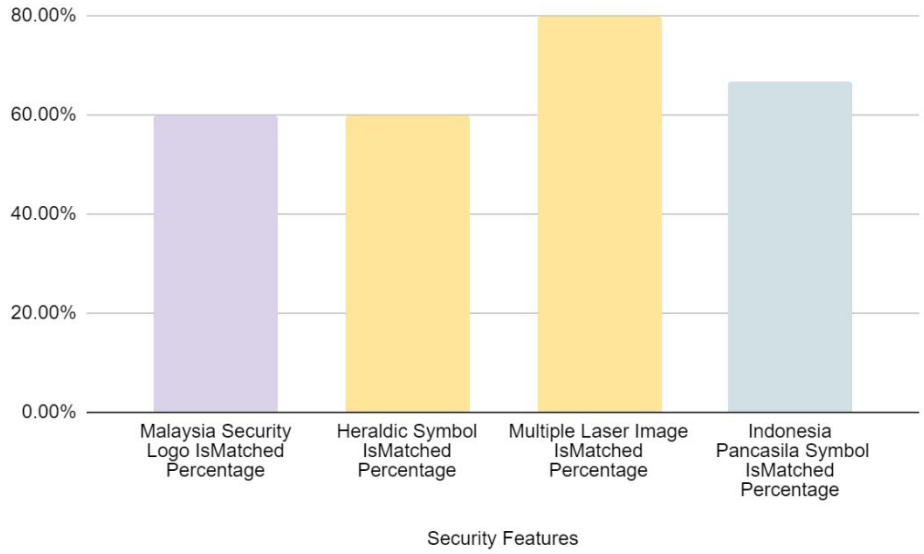

Fig. 15: Security Features Matched Percentage of 3 Countries Passports

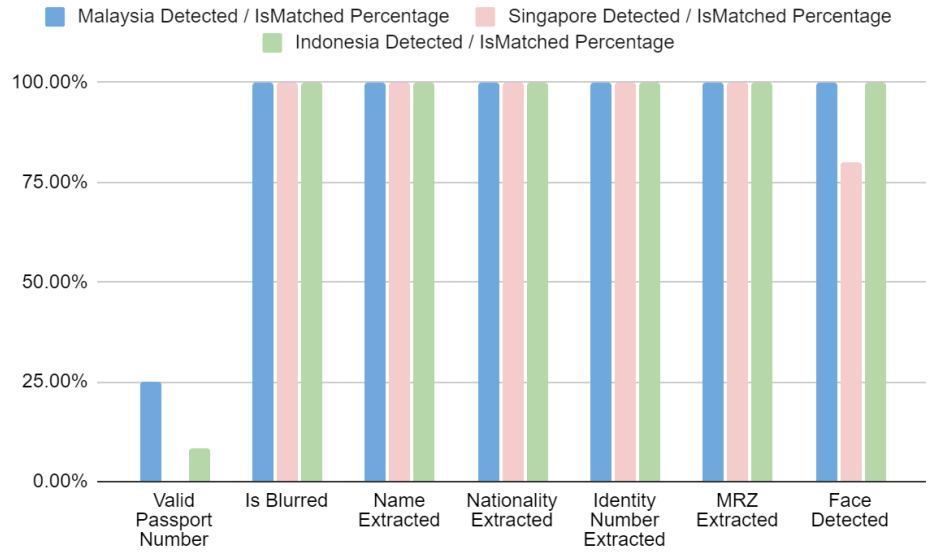

Fig. 16: Column Chart for Fraud Detection Accuracy

The information gathered throughout the passports fraud detection process comprised name, nationality, identity number and machine-readable zone, passport number validity, and face existence. The column chart only shows that the landmarks have been successfully detected while also determining the passport number validity.

The matching percentage for Malaysia passport number validity is only 25% while Singapore passport numbers' validity is also not optimal. This situation also is the same for the Indonesia passport validity percentage which is only 8.33%. This is because the outcome of the OCR process affected where the inaccuracy of the extracted passport number also has affected the percentage of the passport number validity.

During the fraud detection process, the presence of a face on the passport images is also examined. The face detection percentage for Malaysia and Indonesia passport images is 100%, whereas it is 80% for Singapore passport images. In addition, the Web service will also verify the presence of retrieved data during landmark detection. Since all of the information written on the passport images has been extracted, the majority of the detected data in fraud detection is 100%.

6.4. Overall Verification Results

Figure 17 shows a radar chart for the multi-factor verification average results. In conclusion, all the landmarks on the passport images are detectable and give out appropriate accuracy when matching with the landmark templates. However, some of the landmark detection results are not ideal by giving out a lower accuracy since the images in the training data and the landmark template used are not perfect. The overall score indicates nearly 65% for landmark detection and security features detection and 85% for fraud detection. The fraud detection has achieved a better accuracy compared to another two detections as it only indicates the existence of some landmarks, face existence and passport number validity.

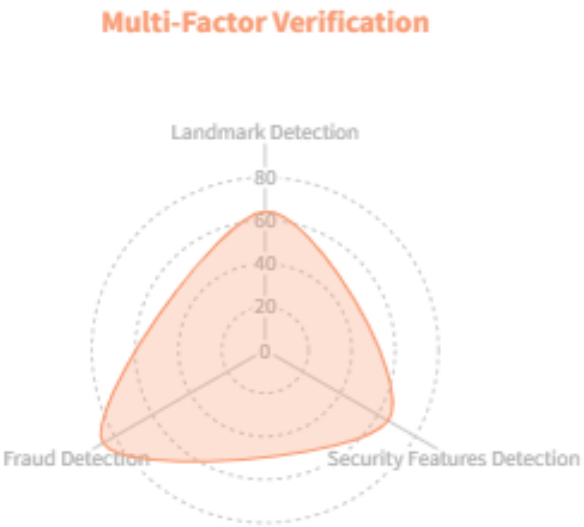

Fig. 17: Overall Passport Verification Results

7. Conclusion and Future Work

A Web service for passport verification has been built and implemented as a result of completing this project. The methods used in creating the Web service included Python, OpenCV, Tesseract OCR and Flask. The objective and goals of this research can be said to be achieved as the prototype application to demonstrate the algorithms has been developed and the passport images features for verification purpose also have been identified. Moreover, the project has met the research hypothesis which is to increase the accuracy of identifying the passport images by applying the multi-factor verification.

In the future, the passport verification can be improved by training the system to recognize the face and landmarks printed on the passport images with the deep learning datasets. The improvement of the image processing may help the system to react faster when detecting the human face existence and also landmarks detection. The template passport images and test data used can be improved by changing to clearer ones. In addition, to raise the accuracy and capabilities of the passport verification Web service, the approach on labelling the landmarks needs to be improved as this improvement would also increase the accuracy while extracting the data from the passport information page. The OCR configuration method can also be considered as one of the improvements that could be done.

AUTHORS' CONTRIBUTIONS

The authors carried out the literature review, experimental design, data collection, developed the prototype application, performed the analysis, drafted the manuscript, and wrote the paper.

Acknowledgements

We would like to thank Azure Innovations and Multimedia University for their support and guidance in this research project.

References

Islam, Shahidul & Kumar, Ramesh & Dar, Ab. (2018). A Comprehensive Study On Web Services Basics : IJARSE

Anders Toms. (2004). Threats, Challenges and Emerging Standards in Web Services Security : DIVA PORTAL

Eric Newcomer and Greg Lomow (2007), Understanding SOA with Web Services. ldap-directories-explained-an-introduction-and-analysis-6th-printingnbsped-020178792x-0321194047-0321180860-0201750813-9780321180865-0785342787924-9780201787924_compress.pdf

Clark, M. & Irani, R. (2002) Web Services Intermediaries. Fletcher, P. & Waterhouse, M. (ed.) (2002) Web Services Business Strategies and Architectures. Chapter 12. UK: Expert Press Ltd. ISBN: 1-59059-179-8.

Dospinescu, Octavian & Perca, Marian. (2013). Web Services in Mobile Applications. Informatica Economica Journal. 17. 17. 10.12948/issn14531305/17.2.2013.02.

ByPassportIndex PassePort (2017) What Secrets Is Your Passport Hiding? (Security) https://discover.passportindex.org/security/what-secrets-is-your-passport-hiding/

GovUK (2016) : Introducing the new UK Passport Design https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473495/HMPO_magazine.pdf

Joel Zlotnick, Tyra McConnell and Traci Moran (October, 2020) : Microprinting Placement. https://platform.keesingtechnologies.com/microprinting-3/

Ivan's Software Engineering Blog (2021) How to Detect A Hologram with OpenCV https://ai-facets.org/how-to-detect-a-hologram-with-opencv/Rush MyPassport (2015) Did You Know that Each US Passport is Made of At Least 60 Different Materials

Merriam-Webster Incorporated "Passport" (2022), Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/passport. Accessed 5 Sep. 2021.

International Civil Aviation Organization(2015), Doc 9303 : Machine Readable Travel Documents, Part 1: Introduction, Seventh Edition,2015 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7.

Thales, "The Electronic Passport in 2021 and Beyond",https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/passport/electronic-passport-trends.

International Civil Aviation Organization(2015), Doc 9303 : Machine Readable Travel Documents, Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs, Seventh Edition,2015 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7.

International Civil Aviation Organization(2015), Doc 9303 : Machine Readable Travel Documents, Part 2: Specifications for TD1 Size Machine Readable Official Travel Documents(MROTDs), Seventh Edition,2015 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7.

EdisonTD.net (Dec 2020): Documents of identity Port Security Center http://edisontd.net/8CFBC2B2646F6940

Wikipedia (2022): Malaysian Passport https://en.wikipedia.org/wiki/Malaysian_passport

Wikipedia (2022): Singaporean Passport https://en.wikipedia.org/wiki/Singapore_passport

Wikipedia (2022): Indonesian Passport https://en.wikipedia.org/wiki/Indonesian_passport