ISSN: 0974-8571 Vol.14 No. 1 June, 2022

International Journal of Computational Intelligence in Control

Instantaneous Documents Authentication and Verification based on Robust Digital Signature

Authors

1- Saira Yaqub*, MS Scholar, 2019-uam-2745@mnsuam.edu.pk, *Muhammad Nawaz Shareef University of Agriculture, Multan*

2- Dr. Aamir Hussain, Assistant Professor, aamir.hussain@mnsuam.edu.pk, *Muhammad Nawaz Shareef University of Agriculture, Multan*

3- Dr. Ayesha Hakim, Assistant Professor, ayesha.hakim@mnsuam.edu.pk, *Muhammad Nawaz Shareef University of Agriculture, Multan*

4- Hafiz Abdul Haseeb Khalid, haxeeb786@hotmail.com, *Bahauddin Zakariya University, Multan*

5- Ayesha Yaqub, ayeshayaqub33@gmail.com, *The Women University, Multan*

***Abstract*— Forgery documents are becoming a major concern for confidential documents. Due to the lack of security systems, a large number of documents containing sensitive details such as payment slips, academic degrees, invoices or contracts are continually subject to fraudster handling. In the proposed research, a system has been designed to authenticate and verify the transcript and provisional certificate based on Bcrypt hashing algorithm to secure the document. The model generates an encryption key to uniquely identify and evaluate the document to determine whether it is forged or accredited. We collected dataset from a university in Pakistan. We are comparing the original data with fake data. The system also demonstrates its feasibility. The investigator can clearly differentiate between the input document and the existing document in the repository. Assessments show that system can precisely produce or decrypt digital signatures carrying various sets of transcript and provisional certificates, including images, while increasing memory and processing requirements are quite limited..**

Keywords: Document verification, document forgery, Bcrypt algorithm, Laravel, OpenCV, Imutils, authentication, digital signature

1. INTRODUCTION

Degree certificates have HEI (Higher Education Institution) gives a variety of the most sensitive materials to establish their achievement with a certificate that is particular to them and their accomplishment. Technology for digital printing and scanning is currently advancing more quickly [1]. Due to their availability of access at cheaper costs with little effort, the likelihood of forging crucial papers like a degree certificate and personal identity card has also increased. These certificates must be manually verified, which is a challenging operation because it involves several levels of human contact. Additionally, because every student who graduated from their HEI must be verified, it is a time-consuming procedure that puts an additional burden on the university or college [2].

Document forgery is a way to make fake or copyright documents or file that is used for some process in business or formal use. The manual approach for document authentication that is in use at the moment has the following restrictions. 1) There is no mechanism that is highly centralized that can verify each clearance certificate that each HEI issues. 2) Authentication procedures can be easily avoided by a fake academic degree. 3) The manually verified method is ineffective in promoting good governance in educational institutions in a personnel-effective manner (The few who dispense certifications that are not authorized). 4) The process of authenticating academic diplomas produced by various HEI that takes a lot of time and work.

The study suggests that creating a verification mechanism based on a digitally signed QR code, to verify a degree certificate from any accredited HEI, can help prevent such authentication disruptions and forgeries. The use of forgery is most common in public and government sectors like educational institutes, public private companies, law enforcement and healthcare department. Because it is so easy and cheap to fake documents, Forgery of printed documents and academic qualifications is a well-known issue [3]. The profit, nevertheless, can be substantial. People might fabricate fake academic degrees, for instance in order to gain better employment and fake transaction records in order to gain financial advantages. In technology era, Some documentation have signatures or stamps that serve as authentication, although both of these can be easily counterfeit [4].

In this research study, a paper-based document authentication and integrity assurance system uses a digital signature as a credential. The digital signature, which is printed with the document, contains a digital signature on the copy made with the issuer's private key, along with a copy of the structure and content of the document that needs to be safeguarded. Recipients scan the authorized document to confirm its validity. Digital signature on the document with their scanner device and verify the validated documentation version that was extracted with the content of the original document. The authenticated digital signature this method gives a way to exchange a document between the real and virtual worlds and can be used as a document copy worlds while ensuring authentication and preserving layout. Furthermore, Binary attachments may be physically transferred with paper-based documents and saved in the digital signature. The authenticated system also keeps track of privacy information digital signature and encrypted so that only authorized people can read it.

Document forgery is still taking the highest scam rate even in advanced countries. An efficient and accurate system or combinations of techniques have to be found to detect forged documents, with higher accuracy and precision. Due to the lack of security systems, a large number of documents containing sensitive details such as degrees, invoices or contracts are continually subject to fraudster handling. The proposed technique has a certain level of accuracy,

Authenticity, verification, and reliability, it has been successfully deployed. The objectives of this paper are:

To encrypt and scan from a single page document by the use of Bcrypt hashing algorithm.

To develop an online system to recognize the document (degree) is authenticated and verified.

2. Related Work

In 1994, to assure the production process, a group invented and developed a 2D barcode known as the QR Code [5]. This could only maintain a finite range of alphanumeric characters at that time. It was then designed to accommodate as much information as possible into a small space. In Japan, in 2000, the QR Code experienced a surge in popularity. Then, ISO certified it as a global standard [6]. A QR code is a rapid and inexpensive way to transmit data. It is regularly utilized by many people. The data in the document can be easily decoded by any QR code reader.

The authentication of paper-based documents was introduced; nevertheless, their technique does not encrypt the original text [7]. When distributing the QR-coded documents, this results in privacy and security violations. As a result, before embedding a QR code, the content of the document must be encrypted [8]. Furthermore, a hashed value was produced using optical character recognition (OCR), however It disregarded right-to-left languages as well as those that OCR could not read. As a workaround for encrypted authentication, paper-based document authentication was suggested [9].

Moreover, its business strategy required the employment of a 3rd party to vouch for any documents or credentials that the algorithm relied upon [10]. Information was stored using a system in the right repository. The original text was not encrypted or compressed, indicating that a non-offline solution was used. Because of this, it is unable to protect data privacy and manage massive amounts of information. In addition to data and information privacy, the volume of data may affect the size of the QR code that is used. Using QR codes and incorporated digital watermarking, a color document authentication process was put into place [11], where storing a signature necessarily involved the use of multiple QR codes. Their method made use Therefore; the size of the signature was influenced by the size of the document image's color map. The information on the document can frequently be changed by altering the QR code.

By encapsulating encrypted user information and digital watermarks, which were then retrieved and decrypted and compared jointly for document verification, to verify the legitimacy of users and document copyrights, dual anti-counterfeiting [12] was launched. RVDS, or robust visible digital stamp, was a new approach for securing and protecting essential/sensitive information. The proposed model encodes the information in the text in a coded variation of a QR code, or quick response code. In the end, this code was connected to the document for the verification process. A mix of keys was utilized in this architecture for both encryption and authentication testing. The approach safeguards the confidentiality of users [13].

The one of the previous study was using 2 algorithms for encrypting the password to login in one system. The 2 algorithms were taking time that is ultimately affecting its decryption speed. But in proposed system, we are using Bcrypt hashing algorithm for the whole document security to prevent it to getting forged. In purposed system, it is detecting the document forgery instantaneously. According to the previous research studies, data verification takes too much time for generating the encryption key and overall execution time of the system. Also the encryption key size was very long, so took more space to have in the database [14]. In the purposed system we can scan the digital signature from the hard copy, for more authentications we can give the soft copy to the system to check which regions are authenticated and verified or not.

RDS, robust digital signature, does not require the use of a third party or any distributors who stand between the sender and the recipient. Additionally, the generated QR code is nearly always the same size. The QR code must be scanned in order to extract the original content for verification. from the database on the behalf of encryption key.

3. Methodology

This research is following the active protection approach; a verification code is implanted or attached on the original document, so that when authentication is required, the verification code is used to check the document's originality. The two active approaches for digital forgery are digital watermarking and digital signature. A complete description of the system services in a structured document. It's written in the form of a contract between the client and the developer. Hardware and software requirements may be included in the system requirements. Initially, the first is the login page. The system authenticates that the user is verified or not while login. Only authenticated persons can generate a login for the staff who is assigned to run the system.

It checks that login information is correct or not. If the login check is false then it will redirect back to the login page. On the other hand, if the login check is correct then it shows the dashboard as well as the admin panel listing. Admin Panel listing will have all the forms and previous records. After provisional certificate/ transcript submission, i automatically send the data of the certificate to the database, from now to till the final display of PDF, each step store within the database. The system generates an encryption key by using the Bcrypt encryption algorithm and saves the encryption key to the database under the same record id. Then the system gets the record id from the database. Now the system has 2 things,

1. Encryption key
2. Record ID from the database

3.1 Authentication Phase

The step is carried out at the document issuer's end, where the document is produced, a QR code is added, and then it is printed in accordance with governmental, academic, and institutional requirements. As illustrated in the fig. 1, this stage consists of different four to five major steps.

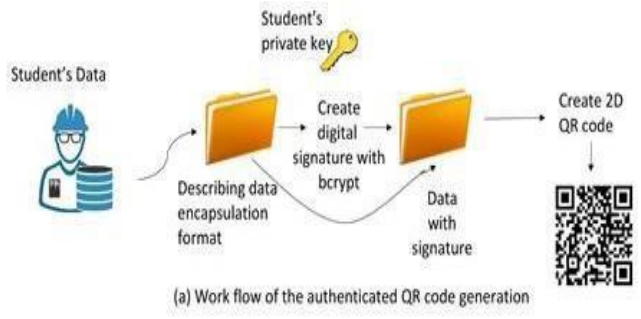

Fig.1 Authentication phase

Initially the system requirement is to create the record of the student. Then the system goes to the generation of authenticated student certificate and transcript. There are different stages in which we work on student authentication having certificate or transcript. At the most initial stage is student enrollment stage within documents authentication and verification system that is based on robust digital signature. After enrolling the student within the system, student record saves in database automatically; the system will apply the bcrypt hashing key on the universally unique identifier (UUID) of the student record. The structure of universally unique identifier (UUID) is explained in fig.2.

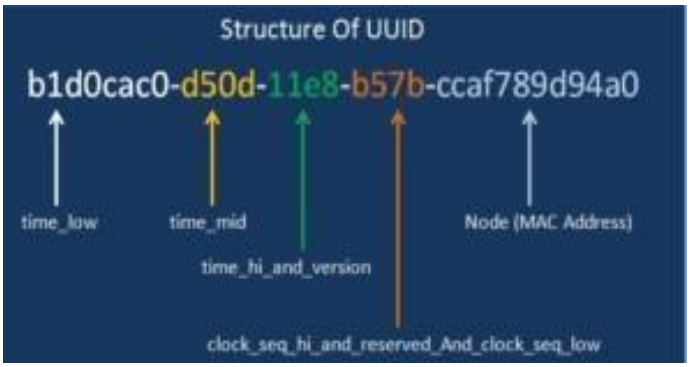

Fig.2 Structure of Universally Unique Identifier

OpenCV

We used OpenCV for features extraction. Following are the features extracting from an image of the document after Digital Stamp having on it:

- Width
- Height
- Shape
- Angle
- Size of fonts
- Location of contents on image

Digital signature creates on the behalf of this encrypted universally unique identifier (UUID) and saves into the database for all the next processing related to this specific student. Our system use universally unique identifier (UUID) and apply Bcrypt encryption on it. The system automatically gives us the encrypted key that uses for having in Digital Signature to authenticate the generated document. Bcrypt increases the size and cost of a hardware implementation of these hash functions, effectively restricting the amount of parallelism an attacker may employ. The structure of bcrypt encryption key is explained in fig.3.

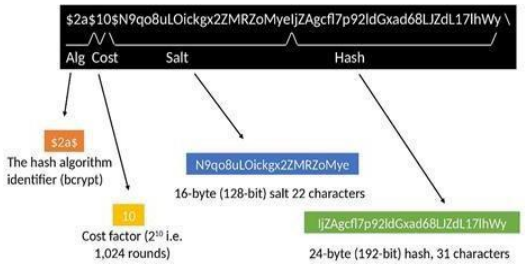

Fig.3 Structure of Bcrypt encryption key

A digital signature is created by encrypting the universally unique identifier (UUID) from the database. That digital signature is always carried along with the original document. Whenever authentication is required, the digital signature is scanned using the appropriate key. Digital signature have the encrypted key as a verification code within it so that the encrypted key cannot be seen with human eye. The original document after embedding the digital signature converts into image using spatie, PDF to image convertor library. The QR Code structure has been explained in fig.4.

Fig.4 Structure of QR code

If it is necessary to test the authentication of the document, the hashed key is extracted from the digital signature that is embedded on the document and compared to the original document already placed in repository. If both are the same, the document is considered authentic; otherwise, it is considered tampered. The information about the document and features of the image of the document is included in the digital signature. This digital signature can also be used to identify the tampered region and to recover the original content from the tampered document. This robust digital signature system can benefit in authentication, tamper localization, and retrieval of original content.

Auto Loader

The class **"Illuminate \ Foundation \ Http \ Kernel "** is the basic component that drives Laravel. **The public/index.php** file is the entry point for all Laravel authentication system requests. Our web server **(Apache / Nginx)** setup is responsible for all requests to this file. There is not much code in the **index.php** file. Rather, the rest of the structure is a starting point for loading. It loads the composer generating auto loader files. It then fetches an instance from the **bootstrap/app.php** script of this Laravel authentication system. Laravel itself creates the initial/first step instance of this Laravel authentication mechanism.

Laravel creates a **Certificate.php** file in the app directory when we run this command. There is the model for our Certificate table in the database, and it is a PHP class called Certificate. ORM is the object relational mapper. It help us to make the relations with the database, ORM is the built in function that laravel provides. We used ORM, for making the relations with the database; we can mapp our database tables easily by the use of ORM. The complete workflow of laravel framework is explained in fig.5.

Python

For the sake of integrating libraries that are python base, we integrated python with laravel. By the integration procedure, we abled to integrate python libraries like OpenCV, OpenCV rectangle method within laravel to make the use of image processing and features extraction efficient.

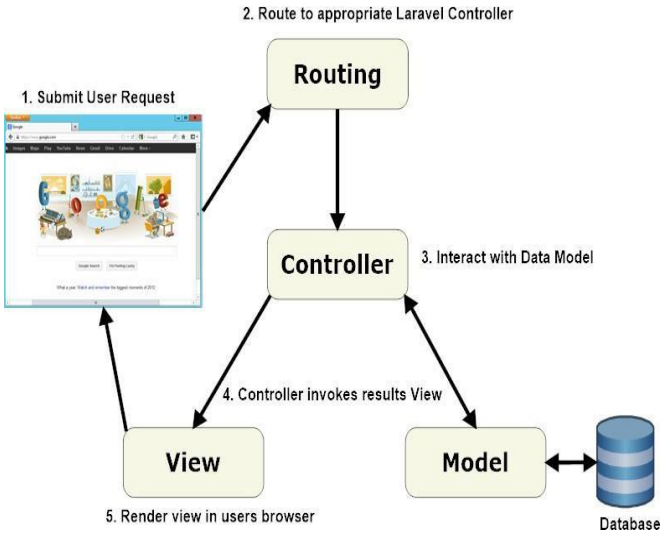

Fig.5 Laravel Workflow

MySQL Database

We used MySQL database server. The use of Laravel authentication made it easier to set up authentication of website users acquires access to information on a website through website authentication. The Laravel framework's authentication method is best to deal with the security threats issues including dictionary and brute force attacks. The authentication procedure created by Laravel is capable of preventing both dictionary and brute force attacks [19].

Imutils

Imutils is being used to find the center of a contour/shape region in the document. Only contour attributes are used by Imutils to detect many shapes, including pentagons, triangles, squares, and rectangles. The color of a shape in a document is labeled by Imutils. A piece of code of imutils is explained in fig.6.

```
from skimage.metrics import structural_similarity as compare_ssim
import argparse
import imutils
import cv2
import sys
```

Imutils Import Code

```
Import Imutils from skimage.metrics

cnts = imutils.grab_contours(cnts) for c in cnts:

                    (x, y, w, h) = cv2.boundingRect(c)

cv2.rectangle(imageA, (x, y), (x + w, y + h), (0, 0, 255), 2)

cv2.rectangle(imageB, (x, y), (x + w, y + h), (0, 0, 255), 2)
```

Fig.6 Query to import Imutils

The system generates the digital signature on the behalf of these 2 things, encryption key and record id from the database. Now the system generates the PDF of the form with generated digital signature on it. The system saves the copy of the PDF to the database. Then it converts the PDF to an image, so image processing could be applied. The path of the image saves to the database also. The system applies image processing so we can have extracted features of the converted image. The results of the extracted features are in the form of an array, so the system saves the array to the database. In the end, it shows the final PDF of the form.

Verification Phase

The receiver side of the document is where this stage is implemented, and here is where the document is authenticated. When received documents with QR codes written on them are sent in for verification, such as degree certificates submitted with employment applications, this stage is usually completed. Verification and decryption are the two main stages that make up this level. Figure 7 below provides a detailed explanation of these steps.

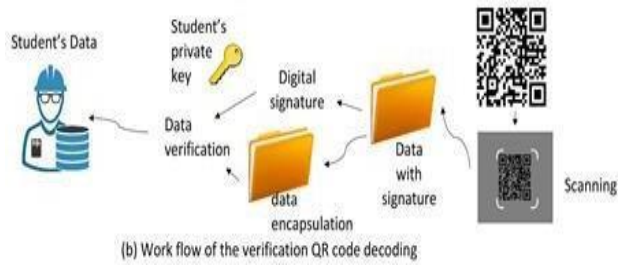

Fig.7 Verification Phase QR Code Decoding

Scan the digital signature from the document to verify it. It gets the record id and encryption key from QR Code and compare it with the already having the same details within the database. Even if one piece of information from 2 of them is incorrect, it will analyze it as a false result and show the given document is forged. But if the given information shows the true result after scanning then it asks for the image of the given document. After having the image of the given document, the system applies image processing on it to extract the features.

The results of the extracted features are in the form of an array, so the system compares the array with already having the same array under the same record id in the database. After comparing the whole record, it analyzes the result. If the result is false then it shows that the given document is forged, if the result is true then it gets the already having PDF under the same record id from the database and display it.

So even at the final step we can detect the difference of displaying PDF from the database and having the document in our hand. In this way, there are different automatic checks that have been applied to check whether the document is forged or not and at the end we can compare the important information manually. This is the complete system that works on the authentication and verification of the document. That's why it calls Instantaneous Documents Authentication and Verification based on the Robust Digital Signature system.

Results & Discussion

When it comes to identifying between modified and authentic documents. Because it uses Bcrypt hash functions applying on universally unique identifier (UUID) to describe all of the document information, it makes a significant contribution to document counterfeit detection. As a result, even if a single letter is changed, the results show that part of document by highlighting it. Because while scanning the digital signature, match the hashed key with the hashed key already having in the database. That shows that this part of document is different from the originals document. This study is also useful for document analysis in forensics. The given is the example of provisional certificate having Digital Signature on it. Fig. 8 having the green line is representing that nothing is forged in the given document; it means document is 100% verified.

Figure 9 is showing the graphical representation of verification of the provisional certificate. X axis showing the pixels of the provisional certificate in width. Y axis showing the pixels of the provisional certificate in height.

Fig.8 Original and given document comparison

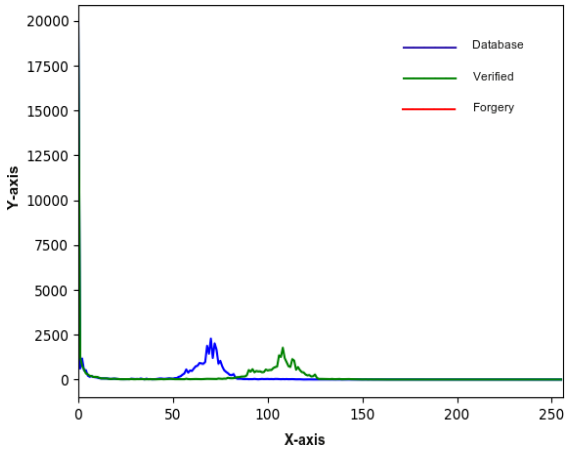

Fig.9 Graphical representation of Verified Provisional Certificate

In Figure 10, that is showing forgery is detected in somewhere in the provisional certificate having the red line with 2% detection of forgery The red highlighted regions are representing the regions applied forgery; it means document is not completely verified. The comparison is also representing in the form of graph in fig. 11. The red curve is representing forgery on the other hand blue curve is representing original. X axis is showing the pixels of the provisional certificate in width. Y axis is showing the pixels of the provisional certificate in height.

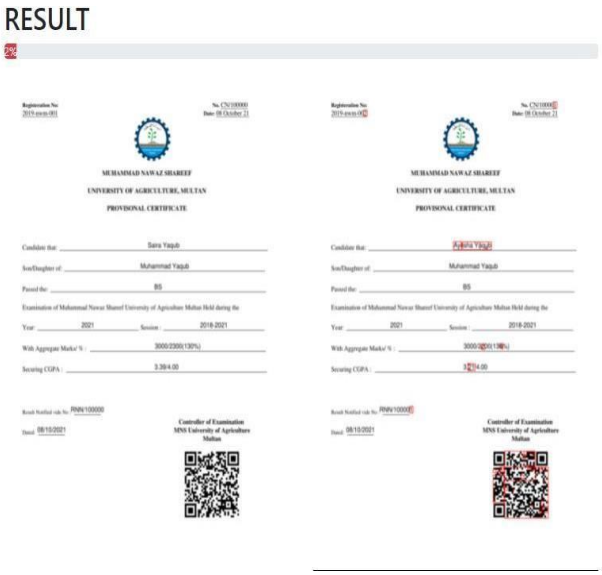

Fig.10 Original and given document comparison

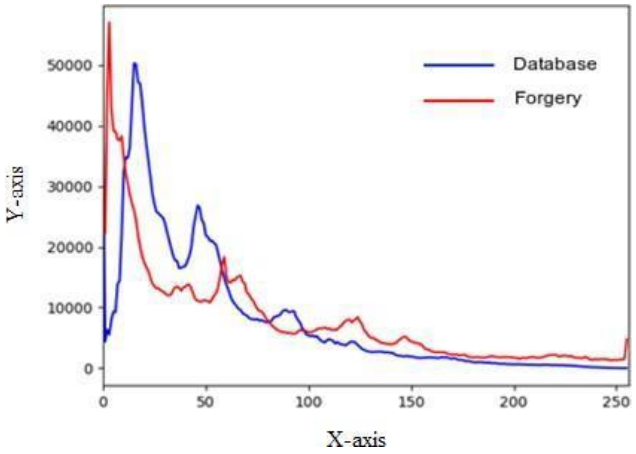

Fig.11 Graphical representation of Forged Provisional Certificate

The following is the comparison of previous techniques used in research studies with our developed system in which we observed the time, size and security. SHA works fast because there not much security is provided. That is why SHA requires less time for encryption generation but little more than Bcrypt. The size of the encryption key is more than Bcrypt encryption key. The time of encryption, encrypted key and the encryption key size of SHA encryption algorithm is given in Fig. 12.

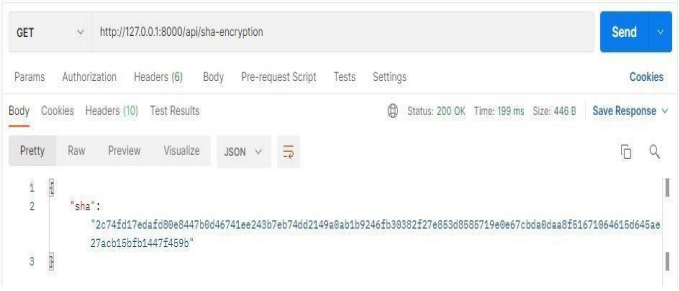

Fig.12 SHA Analysis

In other hand, RSA is asymmetric algorithm so it is secure but encrypts data slowly. As far as Bcrypt is concerned, its uses a strong hashing algorithm which requires a bit of time for encryption because of the encryption rounds but it is more secure and faster than RSA encryption algorithm as well as the encryption key size is more than Bcrypt hashing algorithm. RSA is deterministic: encrypting the same plaintext always yields the larger encrypted text also used to transfer the small data. The time of encryption, encrypted key and the encryption key size of RSA encryption algorithm is given in Fig 13.

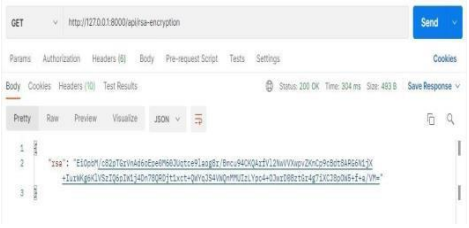

Fig.13 RSA Analysis

Bcrypt is applied which is secure and fast in generating the encrypted key then SHA and RSA. For this very problematic scenario we have only used Bcrypt. Because we wanted our encryption key to be strong and requires less encrypted key size, less encryption and processing time. The time of encryption, encrypted key and the encryption key size of Bcrypt hashing algorithm is given in Fig. 14.

Fig.14 Bcrypt Analysis

Therefore the overall encryption key size, encryption key generation time and execution time requires less time with more security using Bcrypt hashing algorithm. Following comparison table is clearly describing that we improved the encryption key generation time and overall execution time also Bcrypt encrypted key requires the less space means the size of the key is also less than other key sizes.

Factors	Cheng, *et al.,* 2019	Al-maksousy *et al.,* 2020	Proposed Methodology
Technique	SHA encryption algorithm	RSA encryption algorithm.	Bcrypt hashing algorithm
Encryption Time in ms	199	304	197
Execution time in ms	3.13	4.90	2.16
Key Size	446 B	493 B	382 B
Protection	Fast but least secure	Slow but secure	Fast and more secure

Table 1: Encryption and Execution time analysis

Conclusion

Authentication and verification of documents are critical. Documents can be altered, leaked, or accessed without proper authorization in a variety of situations. Furthermore, regardless of how the data changes, the QR code (the stamp), has almost always the same size. As a result, RDS is proposed as a solution for securing and protecting transcript and provisional certificate. This technique generates a digital authentication stamp that is printed within the document itself and verification occurs instantly, with no prior knowledge of the document's contents. This method is robust and extremely fast than previous research studies. The time is improved which is a significant achievement especially when certain level of accuracy, precision is maintained and provides high reliability with fewer features. The proposed technique has given a good confidence with extraction of features and improved time. The system strategy is used while keeping accuracy, precision, well above the required level of document forgery detection while checking the given document is authenticated. This method does not use of third-party solutions to provide encryption / decryption key transfers.

Future work

The future research will focus on the pixels of the degree like documents and other updates like biometric system that will work with the maximum human interpretable features.

REFERENCES

[1] Abd, M., U. Naser, E.T. Jasim and H.M. Al-mashhadi. 2020. QR code based two-factor authentication to verify paper-based documents. 18:1834–1842.

[2] Li, C.M., P. Hu and W.C. Lau. 2015. AuthPaper: Protecting paper-based documents and credentials using Authenticated 2D barcodes. *IEEE Int. Conf. Commun.* 2015-Septe:7400–7406.

[3] Winter, C., W. Berchtold and J.N. Hollenbeck. 2019. Securing physical documents with digital signatures. 2019 IEEE 21st Int. Work. Multimed. Signal Process. 1– 6.

[4] Al-maksousy, H. and H. Abdulhussein. 2020. Robust Visible Digital Stamp for Instant Documents Authentication and Verification Robust Visible Digital Stamp for Instant Documents Authentication and Verification. , doi: 10.1088/1757-899X/765/1/012071.

[5] Bashir, A., X. Han and L.S. Davis. 2018. Techniques of Detecting Forgery in Identity Documents. *Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '17* 1313–1328.

[6] ISO. ISO/IEC 18004:2000 - Information technology - Automatic identification and data capture techniques - Bar code symbology - QR Code. ISO Standards. 2000;2000:122.

[7] Warasart M, Kuacharoen P. Paper-based Document Authentication using Digital Signature and QR Code. 4TH International Conference on Computer Engineering and Technology. 2012;40(January):94-- 98.

[8] Li CM, Hu P, Lau WC. AuthPaper: Protecting paper- based documents and credentials using Authenticated 2D barcodes. In: IEEE International Conference on Communications. vol. 2015-Septe. Institute of Electrical and Electronics Engineers Inc.; 2015. p. 7400--7406.

[9] Ahmed HA, Jang JW. Document certificate authentication system using digitally signed QR code tag. In: ACM International Conference Proceeding Series. Association for Computing Machinery; 2018.

[10] Singhal A, S Pavithr R. Degree Certificate Authentication using QR Code and Smartphone. International Journal of Computer Applications. 2015 jun;120(16):38--43.

[11] Mohsin Arkah Z, Alzubaidi L, Ali AA, Abdulameer AT. Digital color documents authentication using QR code based on digital watermarking. In: *Advances in Intelligent Systems and Computing.* vol. 940. Springer Verlag; 2020. p. 1093--1101.

[12] Xun Y, Li Z, Zhong X, Li S, Su J, Zhang K. Dual Anti- counterfeiting of QR Code Based on Information Encryption and Digital Watermarking. In: Lecture Notes in Electrical Engineering. vol. 543. Springer Verlag; 2019. p. 187--196Kumar, N. andP. Chaudhary. 2018. Password security using bcrypt with AES encryption algorithm. *Smart Innov. Syst. Technol.* 77:385–392.

[13] Cheng, J.-C., N.-Y. Lee, C. Chi and Y.-H. Chen. 2018. Blockchain and smart contract for digital certificate - IEEE Conference Publication. *Proc. IEEE Int. Conf. Appl. Syst. Innov. 2018* 1046–1051.

[14] Dlamini, N., S. Mthethwa and G. Barbour. 2018. Mitigating the Challenge of Hardcopy Document Forgery. 2018 Int. Conf. Adv. Big Data, Comput. Data Commun. Syst. icABCD 2018 1–6.

[15] Hangün, B. and Ö. Eyecioğlu. 2019. Performance Comparison Between OpenCV Built in CPU and GPU Functions on Image Processing Operations. arXiv 1.Guhan, T. and S. Sebastian. 2017. Certificate Authentication Using QR Code and Smart Phone. *Int. J. Emerg. Technol. Eng. Res.* 5:1–4.

[16] Marti, U. V., R. Messerli and H. Bunke. 2010. Writer identification using text line based features. *Proc. Int. Conf. Doc. Anal. Recognition, ICDAR* 2001- January:101–105.

[17] Minarno, A.E., L. Syafa, D. Anggraini and P. Rahayu. 2021. Science and Technology for Community : Improving Web Programming Skills using Laravel Framework. 18:21–26.

[18] Warasart, M. and P. Kuacharoen. 2012. Paper-based Document Authentication using Digital Signature and QR Code. *4TH Int. Conf. Comput. Eng. Technol.* 40:94