https://doi.org/10.2352/EI.2023.35.3.MOBMU-352

Integrity and authenticity verification of printed documents by smartphones

Simon Bugert, Julian Heeger, Waldemar Berchtold; Fraunhofer Institute for Secure Information Technology SIT / ATHENE; Darmstadt, Hesse/Germany

Abstract

To this day, most important documents are still issued on paper. The security is based on the fact that the cost of creating a counterfeit must be unattractive for counterfeiters in relation to the expected profit. This results typically in using expensive printing equipment and substrate. This work introduces an approach which evaluates paper documents using any internet enabled device with a camera and a web browser like smartphones and tablets. Optical character recognition (OCR) is used to make text machine readable after the document is recognized and rectified. Digital signatures are then used to verify the authenticity and integrity of the data. Beyond that, the requirements of privacy, robustness and usability are satisfied. By using JAB Code, a high-capacity matrix code, the data to be verified can be stored directly on the document without having to use a database. This brings key advantages compared to database-bound systems in terms of security and privacy. The use of OCR achieves high usability.

Introduction

People interact with a wide range of different documents on a daily basis, some digital and many printed on paper. While digitization of processes increases continuously, especially documents issued by government agencies are still often printed on paper because of information security and privacy concerns or policies.

The verification of the authenticity and integrity of these documents requires manual inspection or additional time-consuming communication between issuing and verifying parties. These circumstances and also advances in technologies of scanning, printing and imaging tools, make it easy to manipulate and forge documents. It is becoming increasingly easy to create counterfeit documents that are indistinguishable from their original counterpart. Therefore, the verification of authenticity and integrity of paper documents has been an important research topic for decades.

Traditionally, solutions relied on visual features of the document which could be recognized during the verification [1]. The requirements for these techniques include expensive and special printing techniques, watermarks, special ink or holograms [3]. What all methods based on these features have in common is that their security solely relies on the increasing costs of forgery.

In the next section, the related work is discussed, afterwards the requirements of this system are defined. Then, an approach is proposed in detail which is then evaluated according to the previously defined requirements.

Related work

Making printed documents verifiable in their authenticity for everyone addresses some work. Liu et al. [4] propose an approach where an image of an analog seal is digitally signed with a certificate. This way, a bridging technology between digital signatures and traditional seals is introduced. Other methods require manual user input for the verification of integrity of documents by comparing printed text with information presented by the application. Moreover, these security requirements of integrity and authenticity are met by making use of an online service [6].

Winter et al. [7] use cryptographic digital signatures and digitally seal the document by storing all important document features in a matrix code with high capacity. The digital seal provides a high security level, but the user still have to compare the data in the seal with the printed text. Attackers can easy perform social engineering attacks. Berchtold et al. [5] use iOS and Android smartphones to extract text from photographs of documents and embed payload text in a matrix code based. The verification is based on a control sequence which is matched with the output of the Optical character recognition (OCR).

The goal of this paper is to present an approach which can evaluate paper documents using any internet enabled device with a camera and a web browser. OCR is used to make text machine readable after the document is recognized and rectified. Digital signatures are then used to verify the authenticity and integrity of the data. To do so, this work continues the work of Winter et al. [7] and Berchtold et al. [5] so that document verification is possible for everyone by smartphones.

Requirements

For the proposed approach we define six types of requirements: usability, integrity, authenticity, robustness, availability and privacy. The four requirements integrity, authenticity, availability and privacy address the IT security goals and should be always considered in a security application. The robustness and usability are especially important to prevent errors both by the system and the user.

Usability

The application is particularly intended to verify printed documents in an ad-hoc manner. The use of a smartphone for the verification process should be supported instead of needing a scanner or document camera. Therefore, a fast and robust method for the extraction and rectification of smartphone images of documents is crucial. Also, while the user should be prompted for manual review in unclear cases, the accuracy of the automatic document verification should be high. The user should not misunderstand anything and be guided intuitively so that he knows exactly what to do without reading a manual.

Integrity

Verifying a document depends on the unaltered content of the document. Verification of integrity requires high concentration for a human being and accordingly can easily lead to missing errors. A smart device can do the job more precisely.

Authenticity

As the application is intended to verify documents, each document should be tied to an account to verify the that the correct party signed this document. It should not be possible for a person to create an document impersonating another person. Thus we can be sure that the document was not issued by an attacker.

Robustness

The verification of documents should reduce the number of false-positively verified documents, albeit for the cost of more false-negative verification. The environment should have no effect on the result. Neither different light temperature or conditions nor the background on which the document lies or the camera used should influence the results. Likewise, the layout of the document and the position of the JAB code must not influence the results.

Availability

The required data to perform the verification of the data integrity and authenticity needs to be available as well as the application. Systems based on databases cause high costs for high uptime, maintenance and security, where a solution based on a barcode provide the data whenever it is needed without any cost intensive infrastructure. The approach should perform as few network requests as possible.

Privacy

Last but not least, privacy is an important concern whenever documents with personal data are processed. Systems for document verification typically utilize online services which implies that personal data is stored in a database which can be a target for hacking and data leaks as well as the operator has to be compliant in data collection and provide evidence to authorities and individuals according to the privacy regulations of each country and region. This is why, an approach for offline integrity and authenticity verification is needed for this requirement. One crucial challenge in the design of the approach is how to store the signature and signed data on paper.

Proposed Approach

In this section the proposed approach is described. We developed a web application with an api server handling the public key infrastructure (PKI). After some general implementation notes on the web application, the processes of user registration, document signing, document detection and rectification and finally document verification are described.

Web app

To achieve best portability across different types of devices, we developed an application using standard web technology. All signing and verification processes are run client-side on the user's device for privacy reasons. Cryptographic functions are implemented in C++ using the OpenSSL library[1] and compiled to WebAssembly[2] using the Emscripten[3] toolchain. Similarly, OpenCV[4] is used for image processing when extracting documents from photographs.

Registration

When registering for the service, a user must decide between a registration for a company or an individual person. Both types of registration require an additional two-stage verification process. This consists of the submission of two activation codes – one sent by post and the other sent by email.

After the account creation the user has to generate a certificate to complete the registration process. The certificate is used in all later steps to identify the account used to sign an document. During the certificate generation the user can either use existing asymmetric keys or let the application generate them offline in the user's browser. After the generation the certificate is either signed with the intermediate certificate or the root certificate. This depends on the account type described earlier. A company can have multiple end-user certificates and each of them is signed with the companies certificate, which is an intermediate certificate between the end-user and the root certificate.

Document signing

Transcript of Records
Degree Program Chemie, B.Sc. Chemie

Name: Muster, Doku
Date of birth: 1997-01-01
Registration number: 44287597

Technische Universität Darmstadt
Karolinenplatz 5
64289 Darmstadt
Printed: 2021-07-13

Examination	Grade	CP*	Examiner	Date
B.Sc. Chemie (2012)	**2,41**	**180,0**		
Physics II	3,30	8,0	Trocholepczy, C.	2016-02-20
Physics I	1,30	10,0	Rud, M.	2019-09-30
Physics Laboratory Course	1,70	3,0	Guenther, M.	2017-02-17
General Chemistry	2,70	8,0	Gaebel, T.	2016-02-06
Laboratory Course in General Chemistry	passed	2,0	Thüsing, A.	2016-03-31
Analytic Chemistry	2,30	3,0	Oligmueller, P.	2016-03-03
Inorganic Chemistry II	3,70	5,0	Hasenzahl, A.	2016-03-31
Inorganic Chemistry I	3,30	8,0	Hasenzahl, A.	2017-08-01

Figure 1. *Selectable OCR output.*

When signing a PDF document, the selected file is first rasterized to a bitmap. Then, an OCR algorithm is applied to this image. The result contains detected text blocks which are used to overlay each recognized word on the document with a selectable box, as seen in figure 1. The user can pick each significant text on the document by clicking on it. In a final step, the user loads their private key and optionally enters the passphrase if the key is encrypted. To circumvent the need of an online database, the document must encode the following data fields:

1. User certificate serial number
2. TSP certificate serial number (intermediate certificate)

[1] OpenSSL: `https://www.openssl.org/`
[2] WebAssembly: `https://webassembly.org/`
[3] Emscripten: `https://emscripten.org/`
[4] OpenCV: `https://opencv.org/`

3. Selected text content with coordinates relative to document bounds
4. Signature of the selected text blocks

For data capacity reasons, only the certificate serial numbers and not the certificates are stored.

To meet the high capacity needs of this application, a monochrome barcode uses too much space on the document. Hence, the JAB Code [2] is used and placed on the document in an unused space (see figure 3.

Figure 2 shows an overview of the signing process. The message M contains the selected text blocks and is hashed using SHA256. The hash C is then signed using the user's private key $Priv$ and the result CK and message M is encoded in a JAB Code.

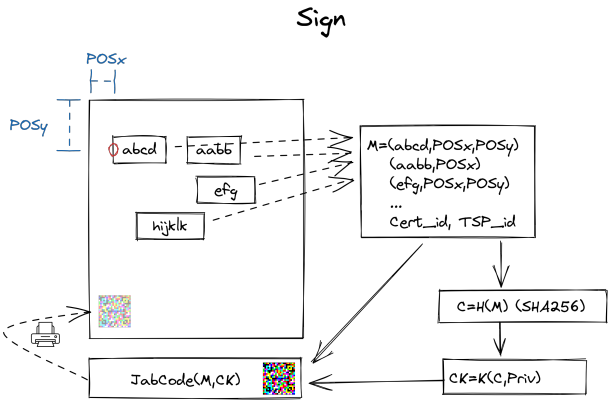


Figure 2. *Document signing process.*

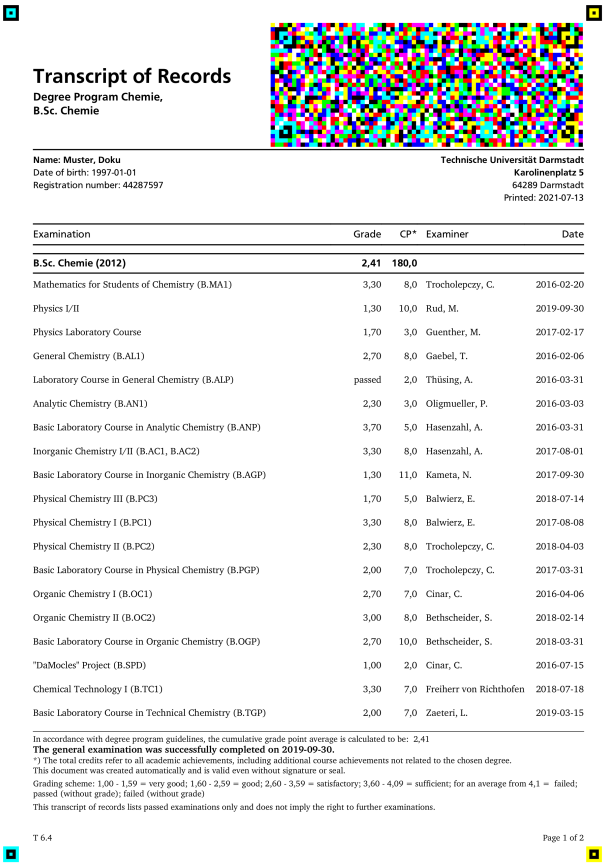
To save additional bytes, the payload is compressed using the Zstandard[5] algorithm.

Now, the original PDF file is modified to include document marks in the four corners and a JAB Code like shown in figure 3. The document can now be downloaded an printed.

Document detection and rectification

When using a photograph of a document as the input, the JAB Code library detects the modified finder patterns (introduced in the previous section) on the captured image. Because we know the exact positions of the finder patterns on the document and also know the aspect ratio, we can calculate the homography matrix (or perspective transformation matrix) from this pair of four points. When applied to the input image, this matrix transforms the image into the document plane which results in a rectified document with no background.

We use four finder patterns, each consisting of a square of 5x5 modules. The finder patterns are placed close to the corners. This has the advantage that distortions can be easily corrected. Each of the four finder patterns has its own color order. This allows to correct rotations. The design of the finder pattern lets us achieve a high performance and accuracy in the finder process. Figure 3 shows an example of a document with the finder patterns and their positions in the corner. Figure 4 shows the basic idea of the finder pattern detector. The detector binarizes the obtained image into one of the three color channels and smoothes it. The detector then searches for an alternating sequence starting in the green channel. If one is found, the center point is determined and at this point it is checked horizontally and in both diagonals whether the same pattern also occurs in all the cases. If this test is successful, it is carried out equally in the two remaining color channels. If and only if an alternating pattern in all four directions can be found only in two of the three color channels it is considered a valid finder pattern.



Transcript of Records

Degree Program Chemie,
B.Sc. Chemie

Name: Muster, Doku
Date of birth: 1997-01-01
Registration number: 44287597

Technische Universität Darmstadt
Karolinenplatz 5
64289 Darmstadt
Printed: 2021-07-13

Examination	Grade	CP*	Examiner	Date
B.Sc. Chemie (2012)	**2,41**	**180,0**		
Mathematics for Students of Chemistry (B.MA1)	3,30	8,0	Trocholepczy, C.	2016-02-20
Physics I/II	1,30	10,0	Rud, M.	2019-09-30
Physics Laboratory Course	1,70	3,0	Guenther, M.	2017-02-17
General Chemistry (B.AL1)	2,70	8,0	Gaebel, T.	2016-02-06
Laboratory Course in General Chemistry (B.ALP)	passed	2,0	Thüsing, A.	2016-03-31
Analytic Chemistry (B.AN1)	2,30	3,0	Oligmueller, P.	2016-03-03
Basic Laboratory Course in Analytic Chemistry (B.ANP)	3,70	5,0	Hasenzahl, A.	2016-03-31
Inorganic Chemistry I/II (B.AC1, B.AC2)	3,30	8,0	Hasenzahl, A.	2017-08-01
Basic Laboratory Course in Inorganic Chemistry (B.AGP)	1,30	11,0	Kameta, N.	2017-09-30
Physical Chemistry III (B.PC3)	1,70	5,0	Balwierz, E.	2018-07-14
Physical Chemistry I (B.PC1)	3,30	8,0	Balwierz, E.	2017-08-08
Physical Chemistry II (B.PC2)	2,30	8,0	Trocholepczy, C.	2018-04-03
Basic Laboratory Course in Physical Chemistry (B.PGP)	2,00	7,0	Trocholepczy, C.	2017-03-31
Organic Chemistry I (B.OC1)	2,70	7,0	Cinar, C.	2016-04-06
Organic Chemistry II (B.OC2)	3,00	8,0	Bethscheider, S.	2018-02-14
Basic Laboratory Course in Organic Chemistry (B.OGP)	2,70	10,0	Bethscheider, S.	2018-03-31
"DaMocles" Project (B.SPD)	1,00	2,0	Cinar, C.	2016-07-15
Chemical Technology I (B.TC1)	3,30	7,0	Freiherr von Richthofen	2018-07-18
Basic Laboratory Course in Technical Chemistry (B.TGP)	2,00	7,0	Zaeteri, L.	2019-03-15

In accordance with degree program guidelines, the cumulative grade point average is calculated to be: 2,41
The general examination was successfully completed on 2019-09-30.
*) The total credits refer to all academic achievements, including additional course achievements not related to the chosen degree.
This document was created automatically and is valid even without signature or seal.
Grading scheme: 1,00 - 1,59 = very good; 1,60 - 2,59 = good; 2,60 - 3,59 = satisfactory; 3,60 - 4,09 = sufficient; for an average from 4,1 = failed; passed (without grade); failed (without grade)
This transcript of records lists passed examinations only and does not imply the right to further examinations.

T 6.4

Page 1 of 2

Figure 3. *Example of signed document with JAB Code seal and document finder patterns in all corners.*

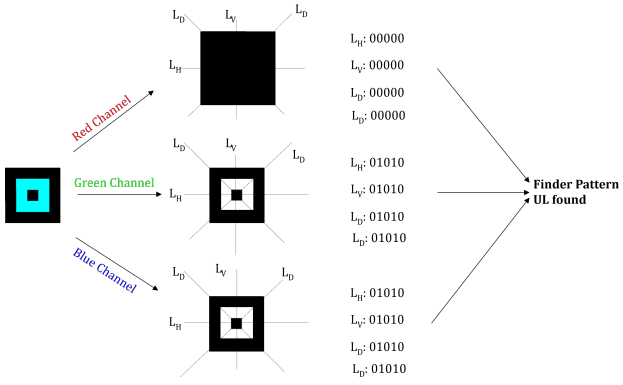


Figure 4. *Example of finder pattern search algorithm.*

[5]Zstandard: `https://facebook.github.io/zstd/`

Document verification

When verifying a document, the user can either use a image captured by a smartphone camera or a scanned document. When using a photograph, the document is detected and rectified as described in the previous section, else the input is used as is.

Next, the JAB Code is decoded and the encoded data (listed in section) is obtained. Using the user certificate serial number and the TSP certificate serial number, the corresponding certificates are fetched. Now, the Online Certificate Status Protocol (OCSP) is used as an alternative to certificate revocation lists (CRL) to get the revocation status of both certificates. Using this information, the complete certificate chain is now ready to be validated. If the validation was successful, the integrity and authenticity of the signed data can now be verified by using the public key extracted from the user certificate.

For privacy reasons, when fetching certificates from the server, the last digit of the certificate serial number is omitted. As a result, the server returns 10 certificates. This way, we achieve k-anonymity with a value k of 10 and the party hosting the server cannot determine the requested certificate.

Finally, OCR is performed on the image which uses exactly the same method as during the signing process to minimize deviations. The recognized text is now compared to the signed text data and the result is presented to the user for review. The review screen (see figure 6) highlights all signed text blocks. Each text block whose recognized text matches the signed text is highlighted with a green background. Text blocks with mismatching texts are presented with an orange background and require input from the user. When clicking on an orange text block, the user decides whether the two texts match, as shown in figure 5. For better usability, the texts are vertically aligned. If at least one text block does not match after the user review, the document is considered forged and the user is informed with a red overlay screen that the document is not to be trusted.

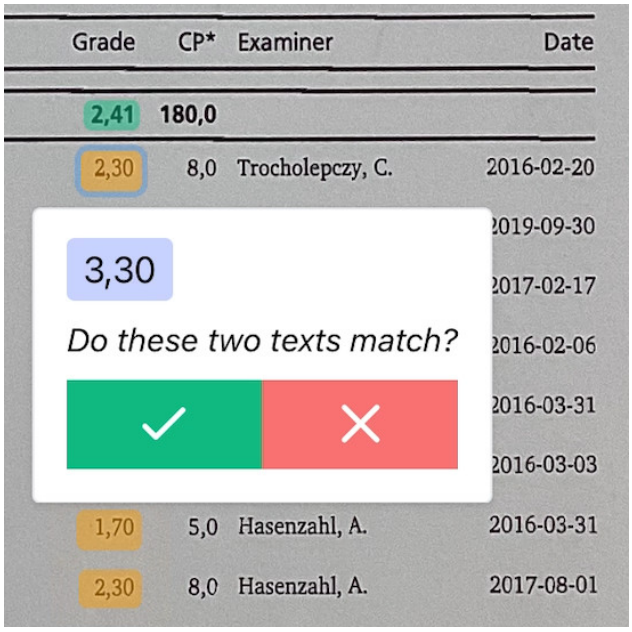


Figure 5. *Example verification review of OCR text differing from signed text block.*

Figure 7 summarizes the verification process. It also demonstrates that it is designed as a fail-fast system which means that the document is considered fake when any step in the verification fails.

Evaluation

In this section we assess the proposed solution based on the defined requirements.

Test setup

For the evaluation of the proposed solution, we use two versions of a document which is shown in figure 3. The scenario is a student's transcript of records issued by a university. Next, we sign the document by selecting significant text blocks, namely

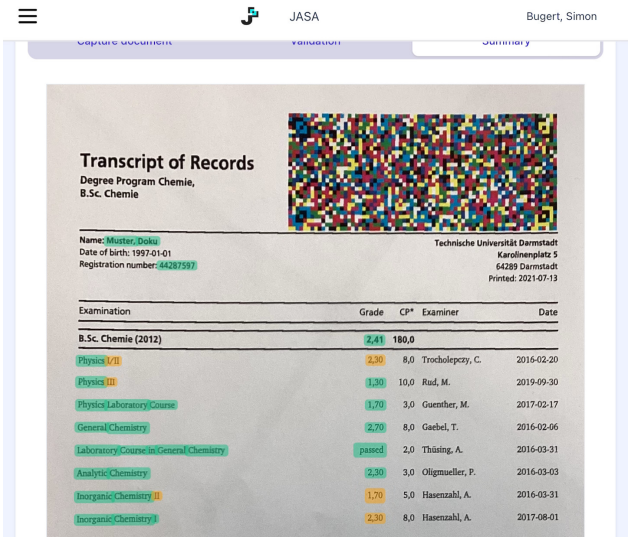


Figure 6. *Example of verification screen with correctly detected text blocks (green) and text blocks which require user review (orange).*

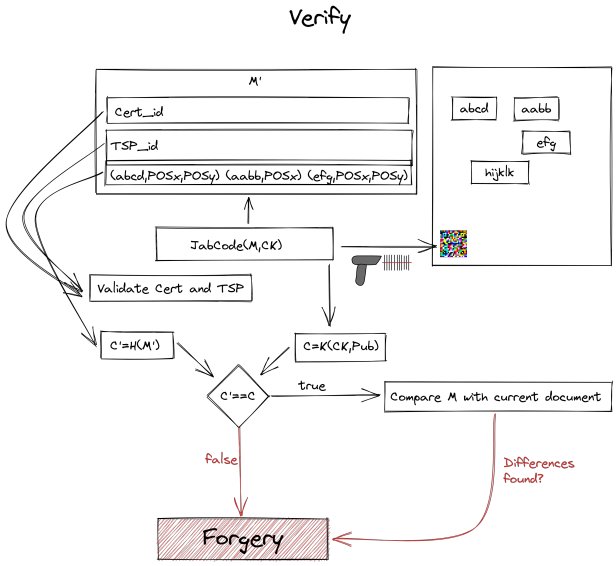


Figure 7. *Document verification process.*

the course titles, grades, the student's name and registration number. After producing a signed version, we forge a copy of it by changing individual grades using a PDF editor.

Usability

The design as a browser-based application improves the usability because any smartphone and computer with a webcam can be used. The application is responsive and fast due to the use of WebAssembly and WebWorkers for long running processes. This way, the main UI thread is never blocked and the user is constantly given feedback of progress. The design of the review process provides a good overview while showing enough detail when processing the data points which require user input.

Robustness

The design of the system ensures that during verification the system fails as soon as one single aspect fails. For slight differences in the recognized text from the signed data, the UI asks the user for manual review and disables the automatic mapping. This way, false positives are less likely. The robustness is highly dependent on the quality of the captured image and the document rectification.

Privacy

The fetching of certificates from the server is implemented in a privacy-preserving manner by using k-anonymity. Also, the general design of the signature makes the signed data available offline. No data leaves the browser and all steps besides the fetching of certificates are carried out locally in the browser. This way, the server cannot gain information about which document is being verified by the user.

Integrity, authenticity and availability

Using digital signatures as part of the data included in the JAB Code, both integrity and authenticity can be achieved. The JAB Code contains the data which should not be modified on the document. The data in the JAB Code is compared to the printed text and accordingly, a modification of it must be noticeable during an examination. It is not possible to impersonate another person, by changing the certificate id in the JAB Code, because during verification another certificate would be loaded, which cannot verify the signature. While the availability is high due to most data embedded in the JAB Code, the certificates still have to be fetched. Still, the web app can be used offline and none of the remaining processes require a internet connection. During the verification process, information about the issuing certificate (e.g. the name of the issuer) will be presented to the user. While this is not yet integrated as described, we will have implemented it in the web app by the time the full paper is submitted. This is closely tied with the authenticity, as only the public key of the issuer can verify the signature and thus the identify of the issuer is obvious.

Conclusion and future work

In this paper, a system for the verification of integrity and authenticity of printed digital documents using a browser-based application has been proposed. The introduced approach is designed to achieve the requirements of usability, integrity, authenticity, robustness, availability and privacy. For special availability needs which require full offline usage, the approach can be extended in future work. The validity of certificates could be checked periodically when internet connection is given to be used in offline situations.

Acknowledgments

This work has been funded by the German Federal Ministry of Education and Research (BMBF) and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] A. Masoud, S. Ibrahim, and M. Salleh, Printed Document Authentication Using Watermarking Technique", In: 2010 Second International Conference on Computational Intelligence, Modelling and Simulation. Oct. 2010, pp. 367–370.

[2] ISO/IEC 23634:2022 (2022). Information technology — Automatic identification and data capture techniques — JAB Code polychrome bar code symbology specification. Standard, International Organization for Standardization, Geneva, CH.

[3] Q. B. Sun, P. R. Feng and R. Deng, An optical watermarking solution for authenticating printed documents, Proceedings International Conference on Information Technology: Coding and Computing, 2001, pp. 65-70.

[4] Liu, Vicky, Caelli, William, Foo, Ernest, & Russell, Selwyn (2004) Visually Sealed and Digitally Signed Documents. In Estivill-Castro, V (Ed.) Computer Science 2004. Proceedings of the Twenty-Seventh Australasian Computer Science Conference (ACSC2004). Australian Computer Society, Sydney, New South Wales, pp. 287-294.

[5] Waldemar Berchtold, Dani El-soufi, Martin Steinebach, "Smartphone-supported integrity verification of printed documents" in Proc. IST Int'l. Symp. on Electronic Imaging: Media Watermarking, Security, and Forensics, 2022, pp 325-1 - 325-5, https://doi.org/10.2352/EI.2022.34.4.MWSF-325.

[6] Zahrah Yahya et al. A New Academic Certificate Authentication Using Leading Edge Technology, ICEEG 2017: Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government 2017, pp. 82–85.

[7] C. Winter, W. Berchtold, J. N. Hollenbeck, Securing Physical Documents with Digital Signatures, In: 2019 IEEE 21st International Workshop on Multimedia Signal Processing (MMSP). Vol. 09. 2019, pp. 1–6.