Authentication of Physical Objects with Dot-Based 2D Code

Michał Glet, Kamil Kaczyński

***Abstract*—**Counterfeit goods and documents are a global problem, which needs more and more sophisticated methods of resolving it. Existing techniques using watermarking or embedding symbols on objects are not suitable for all use cases. To address those special needs, we created complete system allowing authentication of paper documents and physical objects with flat surface. Objects are marked using orientation independent and resistant to camera noise 2D graphic codes, named DotAuth. Based on the identifier stored in 2D code, the system is able to perform basic authentication and allows to conduct more sophisticated analysis methods, e.g., relying on augmented reality and physical properties of the object. In this paper, we present the complete architecture, algorithms and applications of the proposed system. Results of the features comparison of the proposed solution and other products are presented as well, pointing to the existence of many advantages that increase usability and efficiency in the means of protecting physical objects.

***Keywords*—**Authentication, paper documents, security, anti-forgery.

I. Introduction

PAPER documents still play an important role in communications between governmental agencies, citizens and businesses. Many organizations continue using paper documents for invoicing, creating and signing contracts, as well as for communicating with their business partners and clients. It is easy to imagine a situation in which someone creates a falsified document to discredit an organization, e.g. by providing false information to its customers. Nowadays, falsified documents are easier to create than ever before – a PC with a printer and a text editing software is all it takes. Anyone is capable of creating a document pretending to be a company headletter, with any text published thereon. Such a falsified document may be sent to the company's customers who, being convinced of its genuine character, may draw false conclusions about the alleged sender.

In [1], the authors conducted a study which resulted in determining three different approaches to falsifying documents in order to fraudulently receive money from an insurance company: The first one - Print, Paste and Copy (PPC) – consisting in printing a new text on an empty sheet, and then pasting it onto a part of the genuine document. The next step was to copy the document using a color copy machine. The second approach was known as Reverse Engineered Imitation (REI) forgeries. In this approach, the forger creates a new, editable document based on the genuine copy. In the case of that study, people were imitating genuine invoices, retyping all the text and placing the logos, dates, etc. at the proper locations. The third approach was named Scan, Edit and Print (SEP). The forger scanned the original document and then manipulated the digital image thereof.

There are many works dealing with counterfeiting digital and paper documents. In [2], the authors are focusing on documents which were digitalized, and the digital copies are protected by using a 1D hash algorithm and 2D iFFT encrypting documents in the 2D spatial domain. In [3], one may find a method for identification of the source printer that was used for creating the forged document. The authors claim that accuracy of 76.75% may be achieved. The authors of [4] propose a text-line examination method which may be relied upon in high-volume environments. The method requires that each analyzed document be digitized, and that feature points be collected from the binarized images.

The methods mentioned above are truly effective, but they cannot be used for authenticating documents by parties without special equipment. Our system – DotAuth - is a solution dedicated for individuals who are also widely affected by forged documents. The proposed system does not require any special hardware – all verification steps are performed with the user's smartphone. A dedicated DotAuth app analyzes document contents using the smartphone camera and computer vision algorithms. Such an approach makes it easy to deploy the solution on the mass scale. The system may be used for authentication of paper documents or items with a flat surface – e.g. product packaging. The DotAuth authentication symbol comprises several points located along the line of a circle. The document does not have to be placed in one correct position for the purpose of authentication. The symbol will be calculated correctly regardless of the orientation of the image. The document is divided into several areas with different authentication circles. The user has to scan the entire document or only its selected areas, providing enough data to verify the authenticity of the document. Unlike classic methods, such as watermarks, our solution is much harder to copy into the falsified document, simultaneously being much easier to read with the use of computer vision mechanisms.

A somewhat similar approach may be found in [5]. The authors describe a visual information concealment technique which may be deployed for document authentication purposes. The main disadvantage of this method, compared to the one proposed in this paper, consists in the lack of a fast and easy mechanism for reading the authentication-related information. This renders the method in question unsuitable for commercial applications in which no sophisticated devices performing the

M. Glet and K. Kaczyński are with Military University of Technology, Faculty of Cybernetics, Institute of Mathematics of Cryptology (e-mail: michal.glet@wat.edu.pl, kamil.kaczynski@wat.edu.pl)

ISSN: 2692-5079

the current designs and applications.

- The system may contain data used, for instance, to perform simple offline authentication of the marked objects.
- Error correction outputs and other security algorithms may be added to the stored data.

V. Conclusion

In this paper, we have proposed a complete system for authentication of paper documents and other physical objects with a flat surface. The main part of the system has the form of a 2D code – DotAuth code – which may be placed under the text, rendering our solution suitable for existing document templates. We have provided complete algorithms for creating and reading the 2D code developed and come up with its high capacity version that may be used in other applications, also those of a special character. The codes developed are characterized by some very unique features that make them suitable for scenarios in which other 2D codes fail – e.g. they may be used to mark existing objects with a code that is seamlessly integrated with the existing layout and graphical design, or to place marks under the text in existing documents. We have described the architecture of the DotAuth system, capable of supporting all functionalities related to authentication and creation of the marked objects.

The architecture of the DotAuth system and the 2D code are the foundations of a user-friendly process used for authenticating products and documents, facilitating its widespread use. In our future work, we will focus mainly on analyzing security-related aspects of DotAuth/hcDotAuth codes and on validating DotAuth readability under different environmental conditions. Specifically, we will develop a version of the DotAuth code employing error correcting techniques to decrease the misread data rate. We will also provide a sample payload format – for the identifier and the local secret – used in the authentication process. Our future work will also tackle such issues as choosing the color of the code elements in order to adapt them to the medium on which they are used, maximizing legibility of text to the user, as well as maximizing readability of the code to vision recognition algorithms.

The DotAuth/hcDotAuth code proposed paves way to a way of thinking about 2D codes and their utilization. Currently, 2D codes are not integrated and form separate elements that fail to match, in many cases, the rest of the object (document) – the DotAuth/hcDotAuth code may be added without disturbing the graphical style and layout of the object concerned. Additionally, the 2D code proposed may be easily adapted to applications other than those concerned with object authentication. As long as a flat surface is available, the DotAuth/hcDotAuth code relying on custom symbols (dots) to store custom types of data may be used. Such a high degree of customization may be particularly useful in scenarios in which brand recognition is being established.

References

[1] Lindblom, B.S., Gervais, R.: Scientific Examination of Questioned Documents. pp. 238–241. Taylor and Francis, Boca Raton, FL (2006).
[2] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2009). A secure and improved self-embedding algorithm to combat digital document forgery. *Signal Processing*, *89*(12), 2324-2332.
[3] Elkasrawi, S., & Shafait, F. (2014, April). Printer identification using supervised learning for document forgery detection. In *2014 11th IAPR International Workshop on Document Analysis Systems* (pp. 146-150). IEEE.
[4] Van Beusekom, J., Shafait, F., & Breuel, T. M. (2013). Text-line examination for document forgery detection. *International Journal on Document Analysis and Recognition (IJDAR)*, *16*(2), 189-207.
[5] Huang, S., & Wu, J. K. (2007). Optical watermarking for printed document authentication. *IEEE Transactions on Information Forensics and Security*, *2*(2), 164-173.
[6] Warasart, M., & Kuacharoen, P. (2012, May). Paper-based document authentication using digital signature and QR code. In *4th International Conference on Computer Engineering and Tecnology (ICCET 2012)*.
[7] Jumio homepage, https://www.jumio.com/trusted-identity/netverify/document-verification/, last accesed 02/05/2020
[8] Soon, T. J. (2008). QR code. *Synthesis Journal*, *2008*, pp. 59-78.
[9] Image retrieved at 02/17/2020 from https://www.freelancer.com/contest/Label-for-toy-1403253-byentry-23008342.

Michał Glet – is an Assistant at the Faculty of Cybernetics at the Military University of Technology in Warsaw, Poland. His research interests include cybersecurity, cryptography, cryptoanalysis, malware analysis, software reverse engineering, and software development.

Kamil Kaczyński – Military University of Technology, R&D assistant, Cryptography, Steganography, Blockchain, Cryptanalysis, Steganalysis, Mobile applications, Internet of Things (IoT)