ORIGINAL ARTICLE
DOI: 10.5433/1679-0375.2020v41n2p117

Alternative product authentication system using visual cryptography

Um sistema alternativo para a verificação da autenticidade de produtos utilizando criptografia visual

Rodrigo dos Santos Cicareli[1]; José Carlos Pizolato Junior[2]

Abstract

Fraud and counterfeiting have caused various inconveniences to manufacturers and the product consumer market. To avoid counterfeiting and, therefore, bring a higher level of trust and security in commercial transactions, several authentication techniques for physical products have been proposed. Among the techniques commonly employed, the most popular are QR codes (Quick Response Code), Holographic Seals, and RFID (Radio Frequency Identification) tags. This paper aims to propose an alternative product authentication system that applies the visual cryptography technique (NAOR; SHAMIR, 1995). This system employs two masks that, when overlaid, allow visual authentication by the user, without the need for any computational processing. The use of this authentication system for the need in question has not yet been reported in the literature.

Keywords: Systems. Safety. Authentication. Visual Cryptography. Masks.

Resumo

No âmbito comercial as tentativas de fraudes e falsificações têm provocado diversos inconvenientes aos fabricantes e mercado consumidor de produtos. Diante deste panorama, para evitar as falsificações e, portanto, trazer um maior nível de confiança e segurança nas transações comerciais foram propostas diversas técnicas de autenticação em produtos físicos. Dentre as técnicas empregadas destacam-se a utilização de QR codes (Quick Response Code), selos holográficos e RFID (Radio Frequency Identification). Este trabalho tem por objetivo propor um sistema alternativo de autenticação de produtos que aplica a técnica de criptografia visual (NAOR; SHAMIR, 1995). Este sistema emprega duas máscaras que quando sobrepostas permitem a autenticação visual por parte do usuário sem a necessidade de qualquer processo computacional. O sistema proposto, nunca foi anteriormente proposto para a necessidade em questão.

Palavras-chave: Sistemas. Segurança. Autenticação. Criptografia visual. Máscaras.

[1] Mr., Depto. Engenharia Elétrica, Instituição, UFSCar, São Carlos, SP, Brasil, E-mail: rodrigo.cicareli@gmail.com
[2] Prof. Dr., Depto. Engenharia Elétrica, UFSCar, São Carlos, SP, Brasil, E-mail: jcpizolato@yahoo.com.br

Introduction

Globalization has intensified the commercialization of products in the world market and has increased the presence of counterfeit products sold online and in physical stores. According to the Brazilian Association to Combat Counterfeiting (ABCF, 2017) in 2017 Brazil witnessed an economic loss of approximately 145 billion BRL due to counterfeiting. In the last three years, the total amount of lost revenue reached the mark of 395 billion BRL in the corporate and public sectors combined. The US Customs and Border Protection Office of Trade (CBP, 2018) reports that in 2018 the most seized products within the United States were clothing/accessories, shoes, watches/jewelry, bags, and electronic equipment, and this caused a loss of about 1,4 billion USD.

The considerable economic impact associated with counterfeiting and the need to guarantee authenticity has driven research for new methods and techniques that combat fraud. The goal is to provide the customer with information related to the product, such as origin, company information, serial number, among other things to provide credibility regarding product authenticity. The most commonly applied techniques are barcodes, holographic stamps, QR Codes, RFID tags, and visual cryptography. The most widespread system today is the barcode due to its simplicity and ease of implementation. Simões (2015) proposes to use the barcode system in supermarkets. Holographic stamps can be used for product traceability and authenticity (BJELKHAGEN, 2017). Another widely used alternative is QR Codes (Quick Response Code) which allows companies to register different types of product information according to the supplier's and the customer's needs (PENG *et al.*, 2014). RFID (Radio Frequency Identification) tags are a radio frequency identification system that allows you to track the product in real-time, but its implementation has a higher cost than the previous ones due to the infrastructure requirements, including antennas, readers, software and a communication system. This option has an additional drawback since it is subject to electromagnetic interference. Nonetheless, RFID tags have been applied in different sectors, including the industrial food sector (KARAGIANNAKI; PRATAMARI, 2011).

Visual cryptography has some interesting applications in the authentication of commercial transactions NAOR; SHAMIR, 1995). Feijó (2016) combines visual encryption with a watermark technique to authenticate copywriting digital static images. Visual cryptography also has applications regarding security and has been used in online banking transactions (CHANDRASEKHARA; JAGADISHA, 2013; RAJGURU; DHOMSE, 2018; SRIKANTH *et al.*, 2014).

This technique is interesting and feasible in authenticating products and services since the information is recorded in a mask and since the verification process does not require prior knowledge or expertise in advanced processing skills. Besides, it has low-cost production and implementation, being that its production requires reduced computational processing and can be printed on inexpensive photolithography. However, the technique demands precise alignment between the encoded masks to allow visual verification and the confirmation of authenticity. This problem has been addressed in (LIU; WU; LIN, 2008) and (MACHIZAUD; CHAVEL; FOURNEL, 2011).

Fraud attempts regarding counterfeiting of products are common in the audio equipment market (PROSOUND, 2019). The visual encryption technique can provide a viable alternative to combat fraud within this sector. This paper proposes a visual encryption authentication system for an effect pedal (JANONES, 2018). The application of visual cryptography for audio products and equipment has not yet been reported in the literature. The proposed system will address the specificities considering the user's needs.

The system aims to provide authenticity to the product (effect pedal) which will be sold with a built-in encoded mask. A second mask will also be sent to the customer by the product manufacturer. Customers can attest product authenticity by overlaying these two masks, and verifying if the correct data image appears One of the greatest challenges faced in the application of the proposed method is concerning the perfect alignment of the two masks. This is a fundamental condition for the functionality of the authentication process. This problem was addressed by increasing the size of the pixels and designing a device (a joint system using an acrylic plate) to facilitate the alignment between masks.

This paper will firstly present the security aspects regarding product fraud and then describe the visual cryptography technique, encompassing its applications, advantages, and vulnerabilities. It will also detail the proposed authentication system, its implementation, testing, and evaluation. The conclusion section describes the feasibility of the proposed system regarding product authentication according to the assessment tests applied and the analysis of its cryptographic efficiency.

Security in product sales

According to Primi (2019), there are five fraud modalities. These being counterfeiting, adulteration, duplication, simulation, and violation. Counterfeiting is when there is an exact reproduction of the product, including all security elements, and it's intended to try to deceive those who are experts in the field. Adulteration is when parts of the document or product are modified or tampered with. Duplication is replication through digital means. Simulation is an approximate reproduction of a product that is meant to deceive non-experts. Finally, Violation is the opening of the packaging or wrapper leading to product replacement, subtraction, or damaging.

As mentioned in the introduction, the most used techniques used to combat fraud are Barcodes (SIMÕES, 2015), QR Codes (PENG *et al.*, 2018), RFID tags (KARAGIANNAKI; PRATAMARI, 2011), Visual Encryption (CHANDRASEKHARA; JAGADISHA, 2013; FEIJÓ, 2016; RAJGURU; DHOMSE, 2018; SRIKANTH *et al.*, 2014),

Initially proposed by Naor and Shamir (1995) the visual encryption technique has in recent years been used to authenticate visual patterns. This technique has the advantage of not requiring computational processing in the authentication process. Instead, the verification process is performed visually. However, since it is performed manually, the technique has some drawbacks such as alignment issues, rotation, and focal distortion problems. The technique has mainly been used in digital systems, as proposed in (CHANDRASEKHARA; JAGADISHA, 2013; FEIJÓ, 2016; RAJGURU; DHOMSE, 2018; SRIKANTH *et al.*, 2014). In these proposals, the overlay of the encoded masks is performed through a computational procedure that eliminates any of those foreseen issues.

This paper proposes an alternative system for product authentication that applies the visual encryption technique (NAOR; SHAMIR, 1995). The system consists of designing two encoded masks, which when overlaid form an image with the product data. The technique uses digital processing to generate the masks in software, but the image recovery process is carried out physically. The process requires the manual alignment between both masks so the product information is retrieved and verified visually, without the need for any computational processing.

This system was proposed to meet the security needs of an audio company that manufactures and markets effect pedals used in musical instruments. Such a system has never been previously proposed in the literature and is not applied in the authentication of audio equipment. The visual encryption technique of Naor and Shamir (1995), used in the proposed system will be presented and discussed in the following section.

Visual cryptography technique

Visual cryptography proposed by Naor and Shamir (1995) uses a mapping technique to read and transform a set of black and white pixels of an original image into n modified versions (called masks), one for each transparency.

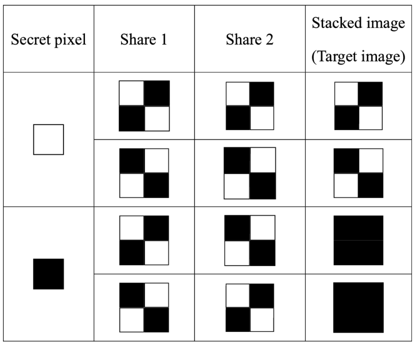
Figure 1 shows the mask generation process. Each mask contains a set of m black and white sub-pixels, arranged in such a way that the human vision system averages their contributions. The resulting configuration can be described by an nxm Boolean matrix $S = [s_{ij}]$ where

$$s_{ij} = 1 \text{ if sub-pixel } j \text{ in transparency } i \text{ is black}$$

and

$$s_{ij} = 0 \text{ if sub-pixel } j \text{ in transparency } i \text{ is white.}$$

Figure 1 – Process of generating sub-pixels and overlaid masks

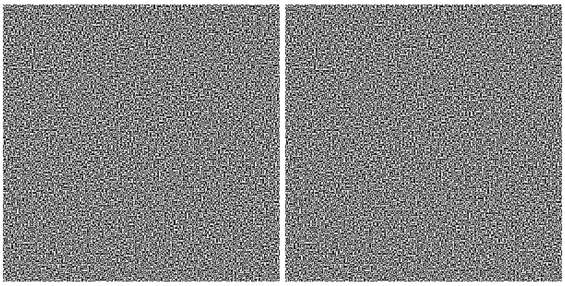


Source: Yan, Xiang and Hua (2020).

Masks i_1, i_2,...,i_r, do not reveal any information when viewed individually, but when overlaid with proper sub-pixel alignment, the combined masks form a grayscale image. The resulting gray tone is proportional to the amount of black and white pixels in each set of sub-pixels. This processing is carried out visually by the human eye.

The present work applies the visual cryptography technique to a company TP logo (CICARELI, 2020). Figure 2(a)-(b) shows the created masks, Mask 1 and Mask 2, respectively, and Figure 3 shows the overlaid resulting image. The markings on the edges in Figure 2 were made to help assist alignment.

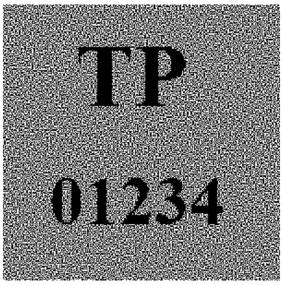
Figure 2 – The created masks, 300x300 pixels



(a) Mask 1 (b) Mask 2

Source: The authors.

Figure 3 – Overlaid resulting image, Mask 1 and Mask 2, 300x300 pixels



Source: The authors.

The technique implementation illustrated in Figures 2-3 uses the model described in Figure 1. Each pixel is transformed into four white and black sub-pixels ($m = 4$) arranged in 2x2 matrices ($n = 2$) in each mask. Although it's possible to create masks using only two subpixels per pixel, this changes the aspect ratio of the image and the result will be distorted. Thus, it is recommended that the masks have twice the size of the original image in each dimension. Therefore, each pixel will generate a set of four sub-pixels. Matrices M_1 and M_2 have four columns and are defined as follow:

$M_1 =$ matrices obtained by exchanging the columns of

$$(1\ 1\ 0\ 0\ 1\ 1\ 0\ 0); \tag{1}$$

$M_2 =$ all matrices obtained by exchanging the columns of

$$(1\ 1\ 0\ 0\ 0\ 0\ 1\ 1). \tag{2}$$

Each mask is formed by a random choice of black and white sub-pixels. Each pixel of the original image is subdivided into four white or black sub-pixels in their specific masks. The overlay of Masks 1 and Mask 2, when encoded in a black pixel, is a matrix with 4 black sub-pixels that will be detected as a black pixel by human vision. The encoding of the white pixel is formed by a matrix in which the amount of white sub-pixels is greater than black sub-pixels, resulting in shades of gray. The size of the masks and the final image formed by their overlay is twice as large as that of the original image. Also, it should be noted that the final image is presented visually in shades of gray.

According to Feijó (2016) the two-mask model has a high degree of reliability. If an interceptor has access to one of the masks they will not be able to decode the information.

The greatest difficulty in applying the visual encryption technique when implemented physically is the adequate alignment of the masks. This alignment depends on the chosen image resolution and definition. The alignment between the masks is performed manually. There is no need for computational processing and the information retrieval is carried out visually. The higher the resolution and definition of the recovered image, the smaller the required pixel size and, consequently, the greater the difficulty of manual alignment. Tests carried out above 150x150 pixels have shown infeasible for manual alignment. Finding an optimum point between resolution (size of sub-pixel blocks) and alignment capacity is a requirement, but the design should also consider the specific needs of each application. In this paper, the visual encryption technique will be applied for product authentication of effect pedals. The company's specific needs have been taken into consideration. The proposed system design will be presented in the next section.

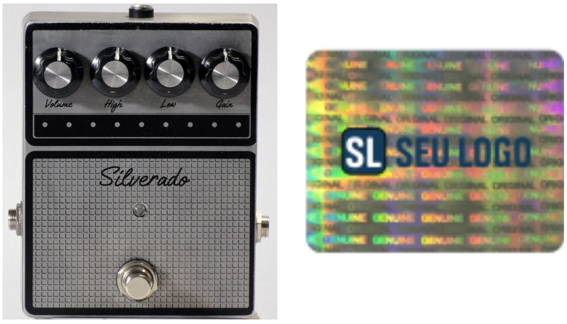
Proposed authentication system

This authentication system may be used for product authentication in general. However, this work applies it to the Silverado Effect Pedal, Figure 4(a). Although holographic seals are currently used by several companies as shown in Figure 4(b), visual encryption has shown to be more advantageous according to the demands of the company in question (cost restrictions and the need for easy customization). Holographic seals are manufactured on a large scale and are not a cost-effective option when there is a need for customization (an exclusive seal for each specific product). Due to the need for customization, visual encryption was the chosen technique.

Figure 5 illustrates the proposed authentication system process.

Figure 6 shows the test image (75x75 pixels), chosen considering the application requirements. This image will be the image retrieved and viewed in the authentication process.

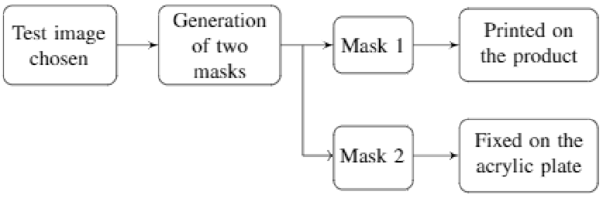
Figure 4 – Athentication system



(a) Silverado effect pedal (b) Holographic seal example

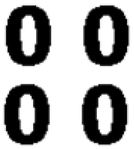
Source: (a) CICARELI (2020) and (b) Dotter Brasil (2020).

Figure 5 – Proposed authentication system



Source: The authors.

Figure 6 – Chosen test image, 75x75 pixel



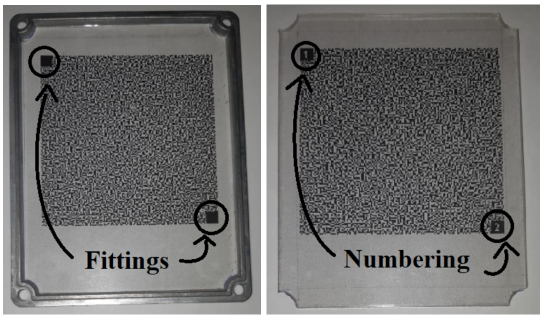
Source: The authors.

The masks were designed applying the algorithm in Matlab software. The resulting masks, Mask 1 and Mask 2, are 150x150 pixels.

Both masks will be sent to customers that acquire the Silverado effect pedal. Mask 1, Figure 7(a), will be printed on the inside of the product's metal housing and Mask 2, Figure 7(b), will be attached to an acrylic plate and sent in an envelope, with the following information: For further details, please contact the company. This authentication system increases the product cost by approximately 2%.

After buying the product the customer will be asked to register the product's warranty at the store. This registration will contain the product's invoice serial number along with the buyer's personal information (phone number, address, and email). An automatic message will be sent to the customer via email (or instant message) with instructions on how to verify the product's authenticity. The steps and guidelines are illustrated in Figure 8.

Figure 7 – Mask in the product housing

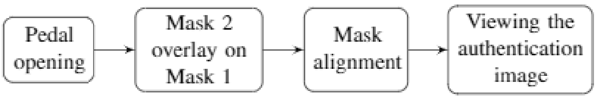


(a) Mask 1 in Silverado effect pedal (b) Mask 2 in acrylic plate

Source: The authors.

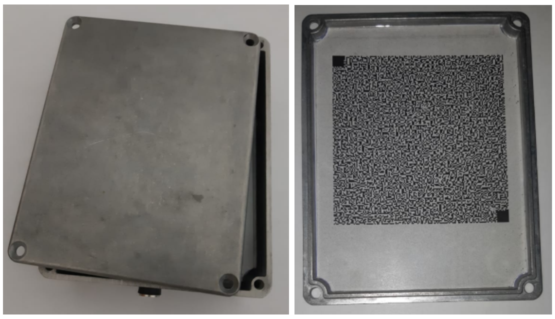
The customer should open the pedal housing as shown in Figure 9(a). There they will find Mask 1, see Figure 9(b). Mask 2 (fixed to acrylic plate) and Mask 1 must be overlaid, as shown in Figure 10(a). The correct alignment between Masks 1 and 2 will show the authentication image, see Figure 10(b).

Figure 8 – Authentication process instructions



Source: The authors.

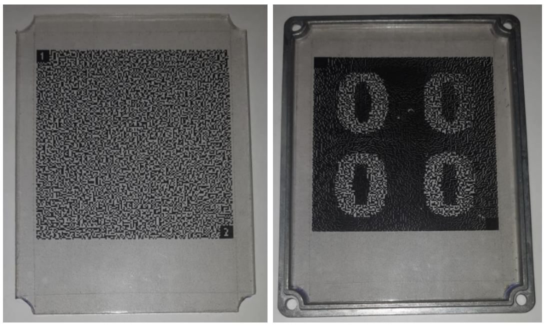
Figure 9 – Opening and internal view



(a) Pedal metal housing (b) Mask 1

Source: The authors.

Figure 10 – Alignment process



(a) Mask 2 in the acrylic plate (b) Result of Mask 1 and and Mask 2 overlay

Source: The authors.

The outcome of the proposed authentication process can be one of the following cases:

- The code is retrieved successfully, confirming product authenticity;

- The correct code was not retrieved. In this case, the product is fake;

- The buyer sends an email questioning what the acrylic plate is for. This means the customer did not register the warranty and that the shopkeeper did not notify the customer about the authentication verification. In this case, the situation should be further investigated by the product manufacturer;

- Two warranty registrations have the same serial number. This implies that one of them is fake. An investigation process can be performed by tracing the origin of the serial number;

- The buyer received the email but did not find one or neither of the masks. In this case, the product manufacturer will be able to solve the issue by tracing the invoice serial number.

In direct purchases from the product manufacturer, there is no risk of fraud. Therefore, the authentication instructions are delivered at the moment of purchase.

Some aspects regarding the implementation of this system are worth mentioning. The dimension choice of the test image, Figure 6, and the size of the masks were determined based on the clarity and definition requirements of the resulting overlaid image. The pixel dimension, the number of pixels, and the mask alignment are basic elements that contribute to an optimal visualization of the encoded image. The analysis performed in this work indicates that the test image size should range between 75 to 150 pixels in width and length. This parameter must be taken under consideration since the masks and the recove-red image will have double the test image original size.

The next step was to study how to perform the mask overlay. The system relies on the printing of images on transparencies with high resolution. This made it impossible to send the images to the client via email since it is unlikely they will have access to high-level printers and acetate or photolith paper. The inversion of black and white pixels contributed to a better visualization in low light environments, and, therefore, was adopted in the design.

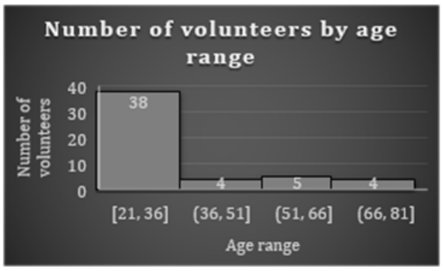
The overlaying process of the masks showed a high degree of difficulty for their precise alignment. The air in between prints generated a parallax effect which only allowed the visualization of the authentication data at a certain angle of sight. The selected approach to solve this problem was to fix one of the masks on an acrylic plate, which is adjusted to the size of the pedal's metallic housing. The use of a rigid acrylic plate minimizes the air between the devices (masks or transparencies) and decreases the parallax effect (ŽIŽEK, 2006). The performance analysis of the system was based on tests with users and will be presented as follows.

Performance analysis

The proposed system was optimized in such a way as to meet the needs of the manufacturer and user. The proposed system was developed to meet the demands of a company that focuses on handmade products that need customization. The company aims to deliver high-quality products and also has a great concern with the quality of its customer service. Visual encryption was the chosen technique considering all of these company needs and specificities.

An important step after system development is in regards to user behavior. An analysis was carried out with 50 volunteers, who performed the procedure described in Figure 8. Figure 11 shows the interviewees' age range. The performance of this procedure assessed the following parameters: difficulty in mask alignment, visual observation of authentication code, and the quality of the instructions given by manufacturers based on the user's understanding of the authentication procedure. The survey results show that all respondents, regardless of age or gender, were satisfied with the system and were able to view the authentication code. In addition, users were also asked to give suggestions on improvements to increase the viability of the proposed system.

Figure 11 – Number of volunteers by age range



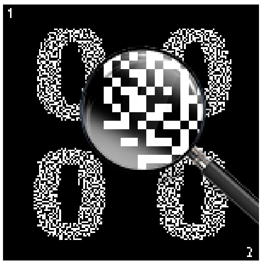
Source: The authors.

One of the suggestions was to give the option of receiving the authentication instructions via WhatsApp, since some users may not access their email often. This recommendation is easily implemented by the manufacturer. A second suggestion was to improve the authentication code image visualization. An additional mask design was performed increasing the number of black pixels, without unbalancing the number of white pixels. The result was increased sharpness to the image.

Next, the system's robustness regarding the safety criteria was examined. An important step when analyzing the efficiency of visual encryption is to verify the existence of repeated patterns throughout each mask.

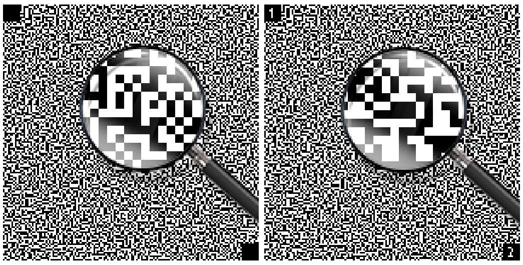
Figures 12 and 13 highlight the pixel display for one selected region. The comparison between the samples in Figure 13(a)-(b), samples in Mask 1 and Mask 2, respectively, does not allow us to recognize any pattern from the original image, see Figure 12.

Figure 12 – Sample region in the overlaid image



Source: The authors.

Figure 13 – Sample region in Mask 1 and Mask 2



(a) Sample in Mask 1 (b) Sample in Mask 2

Source: The authors.

Another important criterion is the spatial distribution of the black and white pixels in each mask. A balance in pixel distribution avoids identifying traces of the authentication code in each mask. Tables 1 and 2 show that both masks have an adequate pixel balance between black and white pixels.

These analyses indicate that the proposed system can be a viable alternative for product authentication.

Table 1 – Black and white pixel ratio in Mask 1

Mask 1	Re (PPI)	150x150 pixels
black pixels	11,349	50,44%
white pixels	11,151	49,66%
Total pixels	22,500	

Source: The authors.

Table 2 – Black and white pixel ratio in Mask 2

Mask 2	Re (PPI)	150x150 pixels
black pixels	11,360	50,49%
white pixels	11,140	49,51%
Total pixels	22,500	

Source: The authors.

Conclusion

Security in product sales is of paramount importance to prevent fraud and protect both the company and the consumers from major financial losses.

This paper proposed an authentication system that applies visual encryption (NAOR; SHAMIR, 1995), considering the needs of TP company, and their product, the Silverado Effect Pedal. The system consists of two masks that when overlaid with proper alignment results in an image containing an authentication code. This verification process occurs visually, without the need for any computational processing.

To function properly, this system requires correct positioning and alignment between the masks since this interferes with the visualization of the authentication code. The alignment issue was addressed in the *Proposed authentication system* section and this system was approved by all 50 users, according to a conducted survey.

The proposed system has an acceptable degree of security when applied to product authentication, as described in the *Performance analysis* section.

This paper demonstrates that the application of visual cryptography in a product the authentication system is viable for physical implementation and offers security efficiency.

Acknowledgments

We would like to thank the Federal University of São Carlos - UFSCar for their support in the development of this research.

References

ABCF - ASSOCIAÇÃO BRASILEIRA DE COMBATE À FALSIFICAÇÃO. Pirataria causou 145 bilhões de prejuízos a economia em 2017 São Paulo: *ABCF*, 2017. Available in: https://abcf.org.br/abcf-news/. Access in: 16 set. 2019.

BJELKHAGEN, H. I. *Holography & philately*: postage stamps with holograms. [Holywell]: Hansholo Consulting Ltd, 2017.

CBP - CUSTOMS AND BORDER PROTECTION OFFICE OF TRADE. *Intellectual property rights*: fiscal Year 2018 Seizure Statistics. United States: Homeland Security, 2018. Available in: <https://www.cbp.gov/sites/default/files/assets/documents/2019-Aug/IPR_Annual-Report-FY-2018.pdf.> Access in: 13 dec. 2019.

CICARELI, RODRIGO DOS SANTOS. *Um sistema de autenticação de produtos que emprega a criptografia visual*. Course Conclusion Paper (Graduation in electrical engineering) – Universidade Federal de São Carlos, 2020.

CHANDRASEKHARA, V.; JAGADISHA. Secure banking application using Visual Cryptography against fake website authenticity theft. *International Journal of Advanced Computer Engineering and Communication Technology*, Bhubaneswar, v. 2, n. 2, p. 1-5, 2013.

DOTTER BRASIL. *Selos holográficos*. Americana, 2020. Available in: https://dotter.com.br/selos-holograficos. Access in: 20 may 2020.

FEIJÓ, E. A. *Proteção dos direitos autorais de imagem estática usando criptografia visual e marca d'água.* São Paulo: Instituto de Matemática e Estatística da Universidade de São Paulo, 2016.

JANONES, U. O. *Um novo olhar sobre os pedais de efeito*. 2018. Course Conclusion Paper (Graduating in music) - Universidade Federal de Uberlandia, Uberlandia, 2018.

KARAGIANNAKI, A.; PRATAMARI, K. *Leveraging RFID-enabled traceability for the food industry*: a case study. Blackwell Publishing Ltd. 2011.

LIU, F.; WU, C. K.; LIN, X. J. *The alignment problem of visual cryptography schemes*. Switzerland: Springer, 2008.

MACHIZAUD, J.; CHAVEL, P.; FOURNEL, T. Fourier-based automatic alignment for improved visual cryptography schemes. *Optics Express*, Massachusetts, v. 19, n. 23, p. 22709 – 22722, 2011.

NAOR, M.; SHAMIR, A. Visual cryptography. *Advances in Cryptology* - EUROCRYPT'94, Switzerland, p. 1-12, 1995.

PENG, K.; SANABRIA, H.; WU, D.; ZHU, C. *6857*: computer and network security. Massachusetts: Massachusetts Institute of Technology, 2018.

PRIMI. *Selo holográfico*. São Paulo, 2019. Available in: https://www.primi.com.br/selo-holografico/. Access in: 16 set. 2019.

PROSOUND. Detido: equipamento de áudio profissional falsificado apreendido na China. *Prosoundnetwork*, EUA, 23 dec. 2019. Available in: https://www.prosoundnetwork.com/business/busted-counterfeit-pro-audio-gear-seized-in-china. Access in: 18 nov. 2019.

RAJGURU, P.; DHOMSE, J.; PY, P. Securing online transaction using visual cryptography. *Journal of Telecommunications System & Management*, Brussels, v. 7, n. 1, p. 1-3, 2018.

SIMÕES, E. D. *Desenvolvimento de sistema para leitura de código de barras com "feedback" para aquisição e segurança de produtos em supermercados*. 2015. Course Conclusion Paper (Graduating in automation control engineering) - Universidade Tecnológica Federal do Paraná, Curitiba, 2015.

SRIKANTH, B.; PADMAJA, G.; KHASIM, S.; LAKSHMI, P. V. S.; HARITHA, A. Secured bank authentication using image processing and visual cryptography. *International Journal of Computer Science and Information Technologies*, [*S. l.*], v. 5, n. 2, p. 2432-2437, 2014.

YAN, B., XIANG, Y., HUA, G. Basic visual cryptography algorithms. In: YAN, B., XIANG, Y., HUA, G. *Improving image quality in visual cryptography*. Berlin: Springer; Singapore: Springer Singapore, 2020. chap. 2.

ŽIŽEK, S. *The parallax view*. Cambridge: The MIT Press, 2006.

Received: May 26, 2020
Accepted: July 21, 2020