Article

Cork as a Unique Object: Device, Method, and Evaluation

Valter Costa ^{1,2,*}, Armando Sousa ^{2,3} and Ana Reis ^{1,2}

¹ INEGI—Institute of Science and Innovation in Mechanical and Industrial Engineering, Porto 4200-465, Portugal; areis@inegi.up.pt

² FEUP—Faculty of Engineering of the University of Porto, Porto 4200-465, Portugal; asousa@fe.up.pt

³ INESC TEC—INESC Technology and Science (formerly INESC Porto), Porto 4200-465, Portugal

* Correspondence: ee09115@gmail.com; Tel.: +351 229578710

† Current address: Campus da FEUP, Rua Dr. Roberto Frias, 400, Porto 4200-465, Portugal.

‡ These authors contributed equally to this work.

Received: 11 October 2018; Accepted: 31 October 2018; Published: 3 November 2018

Abstract: Unique Objects (UNOs) are relevant for real-world applications such as anti-counterfeiting systems. In this work, cork is demonstrated as a UNO, part of the Physical Unclonability and Disorder (PUD) system. An adequate measurement kit (illumination device) and recognition method are also devised and evaluated. Natural hills and valleys of the cork are enhanced using the illumination device and the overall robustness of the recognition application inherent to UNOs is presented. The lighting device is based on grazing light and the recognition task is based on a local feature detector and descriptor called ORB - Oriented FAST (Features from Accelerated Segment Test) and Rotated BRIEF (Binary Robust Independent Elementary Features). The performance evaluation utilizes a private cork database (1500 photos of 500 cork stoppers) and three public iris databases. In the tests carried out on the illumination device, the results clearly show the success of capturing stable/repeatable features needed for the recognition task in the cork database. This achievement is also reflected in the perfect recognition score achieved in the cork database, in the intra-distance measure μ_{intra} , which gives the notion of average noise between measures, and in the inter-distance μ_{inter} which provides hints about the randomness/uniqueness of a cork. Regarding the recognition application, its effectiveness is further tested using the iris databases. Regardless of the fact that the recognition algorithm was not designed for the iris recognition problem, the results show that the proposed approach is capable of competing with the techniques found in the literature specially designed for iris recognition. Furthermore, the evaluation shows that the three requirements that constitute a UNO (Disorder, Operability, and Unclonability) are fulfilled, thus supporting the main assertion of this work: that cork is a UNO.

Keywords: RIOTA; wine anti-counterfeiting; object fingerprinting; UNO; unique object; CASIA-IrisV1 Database; IIT Delhi Iris Database; MMU1 Iris Database

1. Introduction

In the context of anti-counterfeiting systems, a new concept named Recognition of Individual Objects using Tagless Approaches (RIOTA), along with an approach to prevent wine counterfeiting have been introduced [1]. In that work, the anti-counterfeiting scheme is achieved in a two phase process: the enrollment phase, and the verification phase. In the enrollment phase, during the bottling process, every wine bottle is registered in a database by capturing a photo of the top surface of the cork stopper. In the verification phase a common user, using a camera (e.g., smartphone camera) takes a photo of the same region of interest (the enrolled region), which is uploaded to a server, where a computer vision application capable of discerning if the query image has a match in the database is applied. Finally, the relevant information is sent back to the user, notifying him if the bottle

had previously been registered or not, indicating if the wine bottle is genuine or not. The high precision and recall rates presented come from the success of capturing repeatable features from the top surface of the cork stoppers, necessary for the computer vision recognition system. To capture these repeatable features across different camera sensors, a patented technology [2] was devised. This technology comprises an illumination device and the computer vision method.

In this work, the illumination device is presented, tested, and discussed. It includes an illuminator ring arranged for illuminating tangentially with grazing light towards the centre of said ring, and an optical lens allowing focus at a short distance. The effectiveness of the illumination device in capturing high-contrast stable photos with repeatable cork features is also demonstrated. Moreover, the computer vision recognition system is extensively tested on its generalization capabilities. Four different databases were utilized: the improved private cork database, comprising 1500 photos from 500 cork stoppers; and, in order to compare with other researcher's works, three public iris databases were employed, namely the CASIA-IrisV1 database (CASIA-IrisV1, <http://biometrics.idealtest.org/>), the MMU1 iris database [3] and the IIT Delhi iris database [4]. The results clearly show the success of capturing and extracting repeatable cork surface features using the proposed illumination device across three different smartphone rear cameras. Regarding the computer vision recognition system that suits the RIOTA method, a significant improvement of the results from Reference [1] is shown. RIOTA's implementation achieved a perfect score in False Acceptance Rate, False Rejection Rate, accuracy and Equal Error Rate (EER) on the private database. In respect to the publicly available iris databases, the recognition results demonstrate that the RIOTA method is able to compete with the state of art methods specially designed for iris recognition. Finally, this work advocates the cork as a Unique Object, part of the Physical Unclonability and Disorder system.

PUD security systems take advantage of the randomness and disorder of some physical features of a given object to uniquely identify it. Some advantages of these kind of systems are [5]:

- Avoiding storing secret digital keys on vulnerable hardware;
- Natural feature disorder is very hard to clone and falsify. As a consequence, it becomes very expensive to replicate these kind of features;
- The existence of this randomness can be a valuable asset, allowing the use of some cryptographic protocols.

PUD systems are divided in two major types: Unique Objects (UNOs) and Physical Unclonable Functions (PUFs). Unique Objects are defined as physical systems displaying a set of unique and hard to clone features (i.e., a human "fingerprint"), which can be measured using external equipment. Ideally, this equipment would have to be cost-effective and enable fast calculation of the unique features. This "fingerprint" has to be robust enough to be unfeasible to clone. For a system to be considered a UNO, it must have the following properties [5]:

- **Disorder**—The generated fingerprint should only be based on the unique disorder of the object in study;
- **Operability**—It is imperative that the fingerprint is calculated in a timely manner, can be detected with different measurements, and is robust to ageing and environmental conditions. Simultaneously, it should be economically viable to manufacture several instances of the measurement equipment;
- **Unclonable**—It should be overly expensive or impossible for any entity to reproduce an object with the same features of the extracted fingerprint of the physical object.

Summarily, a UNO should be unique and unclonable, and the measuring equipment should be mass produced.

From this work, two main contributions are highlighted:

- Proposing cork as a UNO, part of the Physical Unclonability and Disorder systems approach;

- Proposing a low cost hand-held illumination device for wine anti-counterfeiting applications;

According to a report published in 2016 by the European Union Intellectual Property Office, roughly 21% of the value of Geographical Indication (GI) infringing products in the European Union in 2014 were in spirits and wines [6]. Additionally, from the same report, the “consumer loss, defined as the price premium unjustly paid by consumers in the belief that they are buying a genuine GI product, is estimated at up to €2.3 billion.” Within this scenario, another contribution can be identified in a social context: proposing a device and method to prevent wine counterfeiting.

The remainder of this document is organized as follows: Section 2 presents a literature review focusing on image-based approaches for individual object recognition, targetting anti-counterfeiting systems; the illumination device and RIOTA’s implementation are detailed in Section 3; the evaluation of the performance including the databases used, evaluation metrics, testing procedures, results and discussion are shown in Section 4; in Section 5 the conclusions for this work are drawn; finally, in Section 6 a description of the related patent for this work is presented.

2. Related Works

The use of anti-counterfeiting systems based on unique features is increasing, with some research having been made regarding this topic. This section explores the current strategies used in those systems.

According to Medasani [7], “Fingerprinting an object is the ability to identify an individual object based on unique features such that if the object is seen by the system in other unfamiliar environments, or views, it can still be recognized”; in other words, it is the individual object identification in different scenes based on unique features.

The most common application, found in the literature, of extracting fingerprints from objects is a paper authenticity check in relevant documents. Buchanan et al. [8] have found that the unique surface imperfections from paper, plastic cards, and product packaging contain an unique code formed by microscopic imperfections. These intrinsic characteristics can act as important features for the recognition system. The structure of some surfaces were examined using diffuse scattering of a collimated laser. To correlate the measurements obtained from the generated pattern of the laser speckle, cross-correlation was employed. Sharma et al. [9] devised PaperSpeckle, which takes advantage of the natural randomness present on paper to generate a fingerprint based on the texture speckle pattern. To capture the patterns, a mobile phone with a microscope attached to its camera, and a laptop/desktop connected to an USB microscope were used. For the extraction of the fingerprint from the speckle pattern, Gabor transform was employed.

Beyond forgery detection/authenticity checks on paper, other applications of object fingerprinting include anti-counterfeiting systems for consumer safety, product traceability, among others. In 2014, Takahashi and Ishiyama [10] proposed the Fingerprint Imaging by Binary Angular Reflection (FIBAR) method, which is an imaging method used to capture repeatable “fingerprints” from the surface of metal bolts. Since smooth metal surface does not provide enough features for individual object identification, the authors take advantage of a pear-skin finish to create a rough texture useful for identification purposes. The acquisition system is composed of a white diffuser made from translucent plastics, a black ring absorber and a macro lens. This setup prevents ambient light from falling on the metal surface, directly enabling repeatable image features to be captured from a common camera. To identify each bolt individually, the authors use Oriented FAST and Rotated BRIEF (ORB) [11] combined with a brute-force matcher with a cross-check. Moreover, the authors state that their approach can be applied to tiny mass-produced metal parts with the same finishing. The impact of this research may prevent metal bolt counterfeiting and/or help metal bolt traceability. This work was extended to an industrial setup in Reference [12].

In another work, “A micro identifier dot on things” (mIDoT) was proposed as an alternative to barcodes, tags, or marking for industrial parts traceability in Reference [13]. The dots were made using glitter or metallic-coloured ink, which is a mixture of basic ink with micro shiny particles that

form random irregularities on the surface of the ink. The method used a modified version of FIBAR to capture micro surface irregularities as image features, enabling the possibility of individual object recognition. One thousand one hundred and seventy-two manually made ink dots on regular paper were uniquely identified achieving a perfect score on equal error rate. This work was extended [14] to an automatic dotting unit capable of dotting and capturing for numerous parts. The system comprises four different parts: (i) automatic dotting; (ii) image capturing; (iii) parts feeder unit; and (iv) image matching unit (PC). This system was tested in a database of 11,423 chip capacitors achieving an equal error rate of 0%.

Wigger et al. [15] proposed an individual object recognition system based on the surface patterns of Printed Circuit Boards (PCBs) for traceability purposes. The authors take advantage of the fiducial markers, commonly used to align the PCBs, to define the region of interest and capture the images. To find a match in their database, a template matching technique is employed. The results show that the proposed approach can accurately perform individual object recognition.

All of these applications share some important assumptions: the object's intrinsic visual features are unique between objects of the same class, and as a result of its nature (e.g., manufacturing process, features from natural objects) it would be almost impossible to clone/replicate. Therefore, it will most likely allow safe individual object recognition. Either by stimulating the object and reading its response (e.g., paper authenticity check) or simply by reading its visual features (e.g., FIBAR [10], RIOTA [1]), the assumptions remain valid. As aforementioned, these kinds of applications are part of a larger concept named Physical Unclonability and Disorder and are divided in two types: UNOs and PUFs.

There are several examples of UNO applications, like bank cards, passports or access cards, paper fibbers in banknotes, among others. The UNO application can be achieved in two ways [5]: the classic way, where a UNO is applied to the product to be protected, or certain features of the object are measured. With this measurement serving as the fingerprint, it is compared with another previously stored in a database. The alternative method is an extension of the previous one, with the addition of more information, such as a barcode. Therefore, the validation/authentication of a product involves two steps: (i) Read the additional information of the product and check its digital signature by using the public key stored on the device; (ii) get the fingerprint of the product and check if all digital signature and additional information is correct. Common attacks to UNOs are cloning or re-fabrication. A perfect reproduction from the original is not needed to bypass the measurement system. Indeed, the second structure just has to provide the same measured response as the original one. Theoretically, the replica could have a different size, lengthscale, or appearance. In addition, the clone could be a smart reactive device that artificially presents the same response.

An Alternative to UNOs are Physical Unclonable Functions. These functions were introduced in 2001 by R. Pappu [16] and originally were called "Physical One-Way Functions". By definition, a PUF is a physical system S questioned by a challenge C that generates a unique response called R . An applied challenge and its measured response is usually referred as Challenge-Response Pair (CRP) [17]. The generated response depends on the applied function and the disorder of the physical object. The unclonable demand on a PUF should be impossible for someone with access to the physical system to replicate the physical object or the software. In a typical application scenario, a PUF has two distinct phases: (i) enrollment phase—a number of CRPs are collected from one PUF and stored in a database; and (ii) verification phase—a challenge from the database is applied to the PUF and the response produced is compared with the corresponding response from the database.

A typical PUF possesses five important characteristics [18]:

- **Unique**—The output of a PUF is unpredictable as a result of the unique micro-structural variations.
- **Unclonable**—Because of its inherent physical properties, cloning a PUF should be unfeasible or extremely difficult. Two PUFs cannot produce the same response via cloning.

- **Unpredictable**—Given a set of known challenges $C = (c_1, c_2, \dots, c_n)$ producing the responses $R = (r_1, r_2, \dots, r_n)$, it should not be possible to predict the correct response r_{n+1} of the challenge c_{n+1} .
- **One-way**—It must not be possible to calculate the challenge c_i that triggers a PUF to generate r_i .
- **Tamper evident**—Any attempt to recover the structural aspect of a PUF should alter the original structure and therefore the initial challenge-response pair.

Both the fingerprints of a UNO and the challenge-response of a PUF have the purpose of identifying an object. In order to guarantee the uniqueness and robustness of a PUF or a UNO, two metrics are commonly used in the literature. The first is called inter-distance and expresses the distance between two responses of different PUFs [17]. The second is intra-distance and evaluates the distance between two responses of the same PUF. These distances are often summarized using histograms, showing their occurrence observed over a number of CRPs. It is common that the resulting histograms could be approximated by a Gaussian distribution, and are summarized by providing their averages μ_{intra} , μ_{inter} and their standard deviations σ_{intra} and σ_{inter} [17]. The above mentioned means give a very important notion to the evaluation of the PUFs/UNOs. μ_{intra} indicates the average noise on the responses, i.e., it measures the average reproducibility of a measured response related to an earlier realization of the same response. μ_{inter} indicates the notion of uniqueness, i.e., it measures the average distinguishable responses given by the PUFs/UNOs. Depending on the nature of the PUF response, the distance measure can vary. One distance measure commonly used in PUFs is the Hamming distance, as used in Optical PUFs [19].

Since the appearance of the PUFs in 2001, several object types were proposed as candidates to PUF systems, such as Optical PUFs [19,20], Image-based PUFs [21,22], Coating PUFs [23,24], Silicon PUFs [25], SRAM (Static Random Access Memory) PUFs [26–29], Paper PUFs [8,30], Arbiter PUFs [31], Reconfigurable PUFs [32], Ring Oscillator Pufs [33,34], RFID (Radio-Frequency Identification) PUFs [35], among others. This work focuses on image-based PUFs because as the authors are interested in its scope.

Image-based PUFs for anti-counterfeiting applications were introduced in Reference [36]. These kind of PUFs are based on random visual features of physical objects. The process relies on the capture of 2D or 3D images, where the outline of the object is observed. The image-based PUF is physically unclonable, but not necessarily “mathematically unclonable” [21]. It should be very hard and expensive to build a mathematical model that provides the correct answer to the same challenge-response generated by a PUF. As these vision based systems do not have this feature, it is possible to create a mathematical clone (fake image - i.e., print attack) that presents the same result as the one provided by a PUF. As a workaround, it is assumed that this process has to pass a first check to validate the study image. Contrary to other PUFs, the input of an image-based PUF is usually a fixed challenge (e.g., light used to capture the photos) and, as mentioned before, it is possible to create a mathematical clone that presents the same response. The response of an image-based PUF is a real value image so it is necessary that the image processing system is integrated in the extraction process [21].

Recently, Valehi et al. presented an authentication mechanism using images of metallic dendrites as an image-based PUF [37]. The recognition framework includes image denoising, skeletonizing, pruning, and feature point extraction. The authentication problem is converted to a graph matching problem, because the obtained skeletons are mapped to tree-based weighted graphs.

An image-based PUF using imagery from injection moulded plastic for anti-counterfeiting purposes was introduced by Wigger et al. [38]. A database of 200 samples from two different injection moulded materials (100 + 100) was used to demonstrate the effectiveness of using the surface patterns for individual object recognition. The results show that the proposed method accomplished a perfect score, with the system being able to correctly recognize each sample from the database.

To prevent counterfeiting in metal parts manufacturing, Dachowicz et al. [39] presented a methodology which relies on inherent randomness present in the microstructure of metal parts

resulting from the manufacturing process. The developed protocol uses micrographs as inputs to generate a bit strings and Hamming distance to measure the similarity.

3. Proposed Approach

This section presents the proposed approach to support the proposal of this work: cork being considered as a Unique Object. The illumination device (comprising an illumination ring and lens) is described, along with the RIOTA's recognition application.

3.1. Illumination Device

The need for capturing repeatable features necessary for individual cork stopper recognition, across different acquisition sensors, culminated in the design of an illuminator device, Figure 1. It comprises an illumination ring arranged for illuminating tangentially with grazing light from the periphery towards the centre of a surface of a cork stopper, and a macro lens to enhance the surface hills and valleys.

Figure 1. Developed illumination setup: (a) snapshot of the 3D CAD model; (b) picture of the 3D Printed model—side view; (c) picture of the 3D Printed model without lens—top view; (d) Picture of the 3D Printed model with lens—top view; (e) photo captured using a smartphone; (f) photo captured using a USB camera.

The lens also allows the camera to focus at a smaller distance while the illuminator ring creates a uniform light, suppressing shadows and enhancing the details naturally present on each cork. Two examples of photos captured using this setup are shown in Figure 2.

The enhanced details are valued information needed for the RIOTA's recognition task. The next section presents the algorithm used in this work that suits the RIOTA method.

Figure 2. Two photos taken using the illumination setup: (a) image of the top surface of an agglomerated cork stopper; (b) image of the top surface of a natural cork stopper.

3.2. RIOTA

The concept of RIOTA was introduced in a previous work [1]. The idea behind RIOTA is for it to be a generalized application capable of recognizing and distinguishing individual objects among others of the same class. This concept comprises four important characteristics: (i) a non-invasive property; (ii) a tagless approach; (iii) zero added info; and (iv) zero added finishing. The developed algorithm uses a local feature detector and extractor entitled Oriented Fast and Rotated BRIEF [11] combined with a brute force matcher and RANSAC (Random Sample Consensus) [40] for outliers removal. The procedure for finding a correspondence in the cork database is shown in Algorithm 1.

Algorithm 1 RIOTA's Implementation

```

1: procedure FINDMATCH(queryImage, imagesDatabase, decisionThreshold)
2:   queryKeypoints  $\leftarrow$  detectKeypoints(queryImage)                                 $\triangleright$  ORB Detection
3:   queryDescriptors  $\leftarrow$  extractDescriptors(queryKeypoints)                     $\triangleright$  ORB Extraction
4:   for img in imagesDatabase do
5:     matches1  $\leftarrow$  knnMatch(queryDescriptors, img.Descriptors)
6:     matches2  $\leftarrow$  knnMatch(img.Descriptors, queryDescriptors)
7:     matches1  $\leftarrow$  ratioTest(matches1)
8:     matches2  $\leftarrow$  ratioTest(matches2)
9:     symmetricMatches  $\leftarrow$  symmetryTest(matches1, matches2)
10:    numberOfMatches  $\leftarrow$  ransacTest(queryKeypoints, img.Keypoints, symmetricMatches)
11:    if numberOfMatches > decisionThreshold then
12:      return True                                                                 $\triangleright$  Found a match in the database
    return False                                                                 $\triangleright$  No match found in the database

```

The algorithm takes as arguments the query image, the database of images, and the threshold needed to decide if the query image has an homologous counterpart in database or not. The ORB keypoint detection task of the algorithm was tuned to detect up to 1500 keypoints. Then, ORB extracts binary descriptors of the keypoints. For each image in the database, the matching process of the resultant binary descriptors use a brute force approach. The *knnMatch* tries to match the *k* with the best nearest neighbors for each binary descriptor (in this work *k* was tuned to 2). Next, the ratio test proposed in Reference [41] is applied. At this point, two different sets of matches exist. These sets are merged using a symmetry test. This test only retains the common matched descriptors in the two sets. For the symmetric matches, the homography is calculated using RANSAC [40] which serve as outlier removal (the re-projection error was tuned to 5, which considering the resolution of the images in the Cork Database is adequate to reject false matched descriptors). Finally, if the resultant number of matches is greater than a predefined threshold, the query image has a match in the database and the procedure returns the true value. Otherwise, the value false is returned.

4. Experimental Evaluation—RIOTA's Implementation and Cork as a UNO

This section describes the methodology and methods used to test and validate the unique object recognition proposal. First, it characterizes the databases used. Next, it details the metrics used to evaluate the proposed system. Later, it presents the results achieved and compares them with the state of the art methods on the public databases. Finally, a discussion about the achieved results is presented.

4.1. Databases Description

4.1.1. CASIA-IrisV1 Database

The CASIA-IrisV1 database (IIT Delhi Iris Database version 1.0, http://web.iitd.ac.in/~biometrics/Database_Iris.htm) comprises 756 greyscale iris images from 108 eyes. The images were captured in two different sessions, and for each eye, seven images were captured: three images in the first session and four images in the second. All images have a resolution of 320×280 and are available in BMP (Bitmap) format. For this database no evaluation metrics and/or testing protocol were specified by the provider.

4.1.2. MMU1 Database

The MMU1 iris database [3] was made available by the Multimedia University in Malaysia and comprises 450 greyscale iris images from 100 subjects. As before, no evaluation metrics and/or testing protocol was provided by the developer.

4.1.3. IIT Delhi Iris Database

The IIT Delhi iris database (IIT Delhi Iris Database version 1.0, http://web.iitd.ac.in/~biometrics/Database_Iris.htm) includes 1120 greyscale iris photos from 224 users (176 males and 48 females). The age of the subjects used in this database ranges from 14 to 55 years. The photos were captured in an indoor environment, and are available in BMP format with a resolution of 320×240 . No evaluation metrics/testing protocol is suggested by the provider of this database.

4.1.4. Cork Database

The cork database comprises of 1500 photos from 500 cork stoppers. Two types of cork stoppers were used: natural cork stoppers and agglomerated cork stoppers. For the natural cork type 200 stoppers were collected, and for the agglomerated type 300 stoppers were used. For each cork, three images were captured. To acquire the images, three different cameras were used: rear camera of Sony Xperia Z3 Compact, rear camera of Asus Zenfone 5 A500CG, and USB PlayStation Eye. The diameter of cork stopper used ranges from 19 mm–23.5 mm. The resolution in pixels (height $\times$ width) of captured images ranges from (244×244) to (526×526) pixels, and two identical illumination devices (each device with its own illuminator ring and lens), as illustrated in Figure 1 were used. For the image acquisition task, these two identical devices were used equally (half of the photos were captured using illumination device 1 and the other half using illumination device 2).

4.2. Evaluation Metrics

In the literature, various metrics are often used to evaluate recognition systems. These include: False Acceptance Rate (FAR), False Rejection Rate (FRR), accuracy (Acc), and Equal Error Rate (EER). These metrics depend on the number of correct and misclassified subjects. In this context, a True Positive (TP) is a sample being correctly recognized, True Negative (TN) is a sample being correctly rejected, False Positive (FP) is a sample being incorrectly recognized, and False Negative (FN) is a sample being incorrectly rejected.

$$FAR(\%) = \frac{FP}{FP + TN} \times 100 \quad (1)$$

$$FRR(\%) = \frac{FN}{TP + FN} \times 100 \quad (2)$$

$$Acc(\%) = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (3)$$

The EER is obtained at the threshold that provides the same FAR and FRR.

4.3. Testing Procedures

4.3.1. Illumination Setup

Two different tests were used to evaluate the illumination setup. The first one measured the influence of using the grazing light to illuminate the surface of the cork stopper. The procedure followed in the first test (from now on named illumination setup—lighting test) is described as follows:

1. Randomly select 20 cork stoppers from the database (10 cork stoppers from each type of cork: agglomerated and natural);
2. Capture four images using the same smartphone camera per cork: two images using with the light turned on, and two images with the light turned off;
3. Match the images with and without light using RIOTA's implementation;
4. Store the matching results for further analysis.

The second test, (hereafter called illumination setup—repeatable features test) measures the success of capturing repeatable features using different camera sensors. For this test, only 10% of the “best” detected keypoints, from the original version of RIOTA's implementation, were used to match two images of cork stoppers. Moreover, RIOTA's implementation was tuned for this test (details about the adjustments are further explained). The test procedure used is exhibited as follows:

1. Randomly select 10 cork stoppers from the database (5 cork stoppers from each type of cork: agglomerated and natural);
2. Capture six images per cork using different cameras: rear camera of Sony Z3 Compact, USB camera Logitech C930, rear camera of Samsung Galaxy Note8, USB camera PlayStation Eye and Asus Zenfone 5 A500CG;
3. Match the images using the tuned version of RIOTA's implementation;
4. Store the matching results for further analysis.

The selection of the “best” keypoints was achieved by sorting the keypoints in descending order, according to its response, and using the first 10% best keypoints. The keypoints response was calculated using Harris corner measure [42]. The adjustments of the RIOTA's implementation include the tuning of the RANSAC re-projection error, which was tuned to 1 pixel to ensure that the keypoints matched between two images correctly.

4.3.2. RIOTA's Implementation

To test the proposed approach, several databases were employed. The procedure followed was the comparison of all images in a database against the same database. For a database populated with N samples, this method relies on a number of comparisons of N^2 . Since this approach includes repeated comparisons, these were discarded. Therefore, for a database populated with N samples, the number of comparisons decreases to $N \times (N - 1) / 2$, which reduces the time needed to evaluate a database. Additionally, the time spent to perform a one-to-one match was measured in both private and public databases.

4.3.3. UNO Evaluation

As mentioned in Section 2, the common evaluation methods for UNOs and PUFs are the inter- and intra-distance measures. Both distances are often represented using histograms for a given

image test set and/or CRP database. Additionally, it is normal to summarize the histograms by their average and standard deviation ($\mu_{intra}, \sigma_{intra}$) and ($\mu_{inter}, \sigma_{inter}$). As highlighted by Maes and Verbauwhede in Reference [17], since these measures are frequently used in the literature, it makes, in a generic way, an objective comparison between previous work proposals. However, an important note must be pointed out. Several works use the Hamming distance as distance measure for evaluation purposes. For these systems, which use bit strings as responses, it is usual to state that the smaller the μ_{intra} , the more reliable the UNO and/or PUF. At the same time, μ_{inter} measures the average distinguishability of two different systems based on their responses, i.e., giving them the notion of uniqueness of UNOs and/or PUFs based on the responses. On bit string responses, the best distinguishability is achieved when 50% of the bits differ. In short, it is expected to minimize both μ_{intra} and $|\mu_{inter} - 50\%|$ for systems using bit strings as responses.

In this work, the score is not represented by the Hamming distance but by the number of matched descriptors in two images. The higher the score, the higher the similarity and most likely is for the two sets of descriptors under test to belong to the same object. Therefore, a low value of μ_{inter} and a high value of μ_{intra} is desirable.

4.4. Results

The illumination device was tested in two different ways. First, the necessity of using the illuminator ring was tested. As aforementioned, the photos were captured with the illuminator ring turned on and off. The results of the number of matched descriptors are shown in Figure 3.

Figure 3. Bar chart of the light test performed on the illumination setup. Each individual bar corresponds to the matching result obtained using Recognition of Individual Objects using Tagless Approaches (RIOTA) implementation.

The second test was devised with the aim of studying the influence of the illuminator device on capturing stable and repeatable features across different camera sensors. The results are presented in the bar chart of Figure 4.

The discussion of tests and results shown on Figures 3 and 4 are presented in Section 4.4.1. Beyond the tests performed on the illuminator device, RIOTA's implementation was tested against different databases. Three different approaches were used to evaluate RIOTA's implementation on

the cork database: (i) accuracy, EER, FAR, and FRR are exhibited on Table 1; (ii) the equal error rate plot, often used to evaluate a biometric recognition system, is shown in Figure 5; (iii) in Figure 6 the inter- and intra-distances, commonly used to evaluate UNOs and/or PUFs, are represented by their histograms, whereby the occurrences are replaced by its normalized value such that the maximum frequency equals 1.0, and the number of matched descriptors is normalized to a score (%) ranging from [0, 100], such that the maximum number of matched descriptors equals to the score of 100%. The value of statistical mean and standard deviations of the inter- and intra-normalized distance scores are calculated as $(\mu_{intra}, \sigma_{intra}) = (25.64, 28.55)$ and $(\mu_{inter}, \sigma_{inter}) = (2.00, 14.00)$.

Figure 4. Bar chart of the repeatable test performed. Each individual bar corresponds to the matching result obtained using the tuned version of RIOTA's implementation.

Table 1. Results from cork stopper database.

Methods	Acc (%)	EER (%)	FAR (%)	FRR (%)
Proposed approach: RIOTA's implementation	100.0	0.00	0.00	0.00

Figure 5. Error rate for the cork database.

Figure 6. Inter- and intra-distance results on the cork database. The raw number of occurrences for the inter-distance histogram is 1,122,750, and for the intra-distance histogram is 1500. Therefore, for display purposes, each histogram was individually normalized.

To infer how well the RIOTA's implementation behaves in a different domain, three public iris databases were used. The results are presented using the EER measure and compared with state of the art methods. Table 2 presents the results obtained using the CASIA-IrisV1 database, on Table 3 the results achieved on the IITD iris database are shown, and in Table 4 the EER are displayed for the MMUv1 iris database.

Additionally, the time needed for each task of the RIOTA's implementation was measured for each database and the results are exhibited on Table 5.

Table 2. Results from the CASIA-IrisV1 database.

Methods	Acc (%)	EER (%)	FAR (%)	FRR (%)
Discrete Fourier Transform (DFT)+ Hadamard Transform (HT) [43]	-	1.2	-	-
Gabor [44]	-	9.81	-	-
Decision Tree Construction based on Rough Set Theory under Characteristic Relation (DTCCRSCR) [45]	98.649	-	-	-
Scale-Invariant Features Transform (SIFT) [46]	-	2.1	-	-
Logarithmic Gabor filters [47]	-	-	3.25	3.03
Robust Principal Component Analysis (PCA) [48]	-	0.02	-	-
Support Vector Machine (SVM) [49]	-	2.63	-	-
Proposed approach: RIOTA's (Recognition of Individual Objects using Tagless Approaches) implementation	98.14	1.89	-	-

Table 3. Results from the IITD database [4].

Methods	Acc (%)	EER (%)	FAR (%)	FRR (%)
Texture code matrix [50]	99.96	0.00	-	-
Triplet Half-Band Filter Bank (THFB) + k-out-of-n [51]	99.84	-	0.16	0.15
Fuzzy Binary Decision Tree (FBDT) [52]	-	-	0.0250	8.1081
Localized Radon Transform (LRT) [53]	-	0.53	-	-
Log-Gabor + Haar wavelet [4]	-	2.59	-	-
Discrete Fourier Transform (DFT)+ Hadamard Transform (HT) [43]	-	3.3	-	-
Proposed approach: RIOTA's (Recognition of Individual Objects using Tagless Approaches) implementation	99.76	0.311	-	-

Table 4. Results from the MMU1 database [3].

Methods	Acc (%)	EER (%)	FAR (%)	FRR (%)
Texture code matrix [50]	100	0.00	-	-
Triplet Half-Band Filter Bank (THFB) + k-out-of-n [51]	98.06	-	1.99	1.88
Proposed approach: RIOTA's (Recognition of Individual Objects using Tagless Approaches) implementation	97.59	2.45	-	-

Table 5. Mean time results of RIOTA's implementation on the private and public databases—1 vs. 1 comparison. (CPU: Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz; OS: Xubuntu 16.04LTS)

Databases	Detection Time (ms)	Extraction Time (ms)	Matching Time (ms)	Total Time (ms)
Cork database	7.88	5.99	56.1	70.0
CASIA-IrisV1 database	2.60	3.64	32.3	35.3
IITD database	4.17	4.38	37.5	46.5
MMU1 database	2.34	3.40	12.5	18.2

4.4.1. Discussion

This section details the discussion about the results reported in the previous one.

The first test, referred to as the illumination setup—lighting test, tries to evaluate the influence of the light on capturing valuable information for the recognition task. The results are presented in the bar chart in Figure 3. From this bar chart, it is possible to observe that the number of matched descriptors is always higher with the light turned on. This is an expected behavior, since the illumination was designed to enhance the quality of the information present on the surface of cork stopper. The illumination ring arranged for illuminating tangentially with grazing light from the periphery towards the centre of the cork stopper suppresses inconvenient shadows and creates high-contrast images which leads to a “suitable environment” and potentiates the usage of local feature detectors and extractors like ORB for the recognition task. In this context, for the authors, a “suitable environment” is the circumstance in which the illumination creates areas where the valleys remain dark and the surface gets lighter which are promising areas for the Harris corner detector, often used in the local feature detectors.

The second test seeks to evaluate how stable and repeatable the detected keypoints are in the images captured using the illumination device across seven different camera sensors. As before, the results are displayed as a bar chart shown in Figure 4. For this test, only 10% best detected keypoints were used to match the images, and RIOTA's implementation was tuned to ensure that the pairs of matched keypoints from one image to another were correctly matched. Let us assume a value of $decisionThreshold = 13$ (i.e., the threshold used to decide if two images represent the same object or not) which is the minimal threshold that ensures a perfect score ($EER = 0.0\%$, see Figure 5). In this scenario, all of the images taken by all the cameras used can still be correctly recognized. These results tend to indicate that the features are repeatable using different camera sensors, and this is achieved through the usage of the illumination device.

The third test comprises the evaluation of the RIOTA's implementation over the cork database. The results are summarized in Figures 5 and 6, Table 1. The perfect score shown in Table 1 indicates that recognition Algorithm 1 is adequate for this application. Moreover, by analysing the evolution of both FAR and FRR along different values of the decision threshold, as seen in Figure 5, it can be verified that a decision threshold in the interval results in a $EER = 0.0\%$. This fact suggests that it is possible to choose a threshold up to a certain degree of confidence that does not compromise both FAR and FRR. These kind of measurements, including accuracy, EER, FAR and FRR, are often used to evaluate biometric recognition systems. As previously described, in the context of PUD systems, two measures are usually utilized: inter-distance and intra-distance. Commonly, these distances are represented using histograms and described by its statistical mean and standard deviation ($\mu_{intra}, \sigma_{intra}$) and

$(\mu_{inter}, \sigma_{inter})$. Figure 6 shows the normalized histograms for both distances in the cork database. As it can be seen, there is no overlap in the histograms, which is coherent with the error rate plot, and the low value of inter-distance achieved reinforces the idea of randomness and uniqueness of the cork. Moreover, since intra-distance provides the notion of evaluation noise, and there are no false negatives, this reinforces the idea of the success of capturing repeatable and stable features using the illumination device. The noise present in the acquired images from different camera sensors is not enough to compromise the recognition task. This also suggests some camera invariance which is a good indicator of this system.

To evaluate the generalization capability of RIOTA's implementation, the fourth test was carried out using different iris databases found to be state of the art. Regardless of the fact that the recognition Algorithm 1 was not designed for the iris recognition problem, the results shown in Tables 2–4 are capable of competing with the techniques found in the literature, which were specially designed for iris recognition. An important note to be highlighted is: the input image for the RIOTA's implementation is a full size image and not the segmented iris as it should be. This decision was made to boost the development and testing process, considering that iris segmentation is out of the scope of this work. However, the results would most likely improve if the segmented image was used instead of the full size image. By visually inspecting all databases, it was observed that the photos with higher quality (i.e., higher definition, focused photos, etc.) belong to the IITD iris database, and there are some low quality photos (i.e., blurred/unfocused images) in the CASIA-IrisV1 database and MMU1 iris database. That might be the reason why the best recognition results are reported for the IITD database (Table 3). This fact is coherent to the method used (ORB) taking into account the specificities of the recognition algorithm. The keypoint detection is based on the Harris corner detection, and for blurred images, this detector is not very capable of detecting the stable keypoints necessary for the extraction and matching task. Therefore, the recognition results drops on both the CASIA-IrisV1 and MMU1 iris databases. From these results, it is possible to infer that RIOTA's implementation possesses a certain degree of generalization, with an identified limitation (the blurrier the image is, the more likely it is that the recognition system fails).

For any type of recognition systems (e.g., biometrics, anti-counterfeiting systems) the time spent on the searching/matching process is crucial. The time needed to validate the identity of a person or perform a product authenticity check can compromise the applicability in a real-world scenario. For that reason, the time needed to match two images was measured and is shown in Table 5. This time includes the detection, extraction in two images, matching descriptors, and outlier removal with RANSAC. Let us assume a scenario where the database is populated by 1,000,000 images and the total time of 70 ms is a representative time for this recognition system. In this scenario, the total time needed to perform 1,000,000 comparisons is ~19.4 h. Naturally, this result raises real-world applicability issues for this system. In order to enhance the time performance, a preliminary work on a Content Based Image Retrieval (CBIR) for this system was already proposed [54]. In that work, the matching process takes 10 ms to perform 100 comparisons. In the aforementioned scenario, the time needed to perform 1,000,000 comparisons is 100 s, which is more acceptable. Despite the tremendous improvement on the time performance, once again, this improvement may not suffice in a real-world system. Other time improvements may include parallelization of the software application and/or reducing the image to hash codes [22,55,56]. Comparing with other state-of-the-art works, Takahashi et al. [12] measured a time of 0.827 s to perform 1 vs. 1 comparison, while Wigger et al. [15] reported a time to perform 1 vs. 1 comparison (The authors state that: “in the present case of 115 PCB parts, the identification process for one part takes 1.11 s”, so we are assuming that is the time needed to perform 115 comparisons (the identification process does not stop after finding a correct correspondence). In that case, the extraction time takes 680 ms and the time for 1 vs. 1 comparison is calculated as $1000 \times 0.42 / 150 = 3.7$ ms.) of 3.7 ms. From the performed analysis, it is clear that time is one of the limitations of the proposed approach and the trade-off between time and accuracy

may also be considered. As such, a careful optimization to comply to real-world requirements should be conducted.

4.4.2. Cork as Unique Object

As defined in Section 2, for an object be considered as a UNO, it must satisfy the following requirements: disorder, operability, and Unclonability.

The disorder requirement is simple to achieve, since the information used for recognition purposes are binary descriptors extracted from the detected keypoints on the image of the cork stopper. Therefore, the "fingerprint" is only based on the unique disorder of the surface of cork stoppers.

The operability requirement includes several prerequisites: (i) the time needed to calculate the object's fingerprint; (ii) the repeatability of measurements; (iii) the robustness to aging and environmental conditions; and (iv) the measurement equipment should be economically viable. Regarding point (i), this approach only takes an average time of 6.9 ms to detect and extract the "fingerprint" from one image of a cork stopper. This time is spent just one time per image on two occasions: when registering the image in the database (enrollment phase), and when querying the database (verification phase). Although the matching time needs further improvements as discussed previously in Section 4.4.1, the detection/extraction time is adequate for this application. The repeatability of measurements, point (ii), by using different camera sensors, was demonstrated in the tests performed (repeatability features test, and cork database test) and proven by the achieved results. The non-overlapping in Figure 6, the score displayed in Figure 4, and the intra-distance (μ_{intra}) that expresses the notion of average noise on the measurements demonstrate that cork stoppers can be measured repeatedly (using an image as representation of the measure). Relative to point (iii), in Reference [57], the authors have performed aging tests exposing cork to extreme environmental conditions following the standard ASTM (American Society for Testing and Materials) G154-12a [58]. The authors state that cork does not suffer large changes when exposed to extreme environmental changes even in the face atmospheric factors such as light and humidity. Although the focus of this study is the mechanical properties (e.g., elasticity, damping, etc.) and not the variation of the visual appearance of cork, this can be used as a good indicator that the visual aspect of the cork possesses a certain degree of robustness to aging and environmental conditions. Besides, in this application, the cork stoppers are not exposed to these hard environmental conditions. Moreover, the wine experts from a large bottling company in Portugal have guaranteed that beyond some possible color changes in the cork the physical structure does not change over the years. Therefore, it is expected that the illumination device minimizes these color changes allowing the method to successfully recognize a cork stopper. However, full cork stopper aging tests according to standard ASTM G154-16 [58] may be necessary to correctly support the aforementioned sentence. Lastly, point (iv), the measurement device should be economically viable. Since no special components are used in the illumination device (the setup comprises two 3D printed parts, six Consumer Of the Shelf (COTS) white LEDs, and a smartphone COTS macro lens) it is not expected that the production cost of this device will make it impossible to use. "The rule of thumb" of anti-counterfeiting systems states that an anti-counterfeiting device should not be more expensive than the product its protecting. Despite not having calculated a real cost for the illumination device, it is not expected that the cost of mass-producing this device would exceed the cost of expensive/premium wine bottles and/or spirits or even the cost of regular wine/spirits bottles that use cork stoppers. Moreover, the same illumination device can be used to validate several wine bottles.

Finally, the unclonable requirement was demonstrated in two different ways. The first one is the non-overlapping shown in Figure 6 and the inter-distance (μ_{inter}) that expresses the notion of randomness/uniqueness that leads to the object's unclonability. The second is the physical features displayed by the natural and agglomerated cork stoppers. As a result of the natural extraction of the cork stoppers from *Quercus suber* L., it is highly unlikely that two natural cork stoppers possess identical physical visual features. Regarding the agglomerated cork stoppers, because of their completely

random manufacturing process it is also highly unlikely, even for the manufacturer, to produce an agglomerate cork displaying the same physical features in the same geometric disposal. Therefore, the unclonability is, up to a certain limit, ensured by the extraction/manufacturing process of the cork stoppers.

As a final remark, the aforementioned discussion supports the hypothesis of cork being considered a Unique Object.

5. Conclusions

In this work, cork was proposed as a UNO, part of the PUD system, along with its measurement kit (illumination device), and its recognition method. The effectiveness of capturing relevant information using the devised setup along with the proposed RIOTA's implementation was demonstrated in several tests: light test, repeatable features test, and databases test. In the tests carried out on the illumination device, the results clearly show the success of capturing stable/repeatable features needed for the recognition task. This achievement is also reflected in the perfect score achieved in the cork database, in the intra-distance measure μ_{intra} , which gives the notion of average noise between measures, and with inter-distance μ_{inter} , which provides hints about the randomness/uniqueness of the cork. Moreover, these results show that the three requirements that formulate a UNO—Disorder, Operability, and Unclonability—are fulfilled, regardless of the fact that cork stopper aging tests must be conducted to better support the operability requirement, as discussed in Section 4.4.1.

The cork, measurement device and recognition method that suit the UNO definition [5] and the RIOTA's concept [1] has the following advantages over other anti-counterfeiting implementations: (i) it's non-invasive; (ii) it does not require any kind of marking and/or tagging; (iii) it does not use any kind of helper data (e.g., bar codes, serial numbers, etc.) to support or simplify the recognition task; (iv) it does not use any kind of superficial treatment to enhance the surface details (just use the object "as is"); (v) the information used for the recognition task only depends on the surface of the cork, making it hard to clone or falsify. In addition, this approach does not require a completely novel computer vision algorithm nor a huge dataset, which are usually necessary in machine learning-based approaches, since a state of the art local feature detector and extractor achieve a good performance. However, some limitations can also be identified from the application point of view: (i) the time needed to perform 1 vs. 1 match can make the application in a real-world scenario unachievable for a huge cork database if no other technique to reduce the search space and/or improve time performance is used; (ii) the quality of the images may alter the success of the RIOTA's implementation (as previously discussed, the blurrier the images are, the more likely it is that the recognition fails); (iii) the indispensability of using the illumination device to capture the images has, perhaps, a low degree of user friendless. The user is asked to put the illumination device in the bottle, turn the light on, and take the photo to validate a wine bottle.

As previously pointed out, the necessity of reducing the search space and/or improving the time is mandatory. Therefore, future work should aim at addressing this question.

6. Patent

Related with this work is the patent entitled: "Device and Method for Identifying a Cork Stopper, and Respective Kit" [2]. This patent includes a method for identifying a cork stopper comprising: capturing an image of a surface of the cork stopper which is being illuminated tangentially to said surface; comparing the captured image to a database of previously stored images of cork stoppers; indicating whether the captured image matches one of the previously stored images of cork stoppers. A device for identifying a cork stopper comprising an electronic data processor arranged to carry out said method is also disclosed. A kit comprises said device and an illuminator arranged for illuminating tangentially (grazing light) the surface of the cork stopper. The kit and the method can be used to easily identify cork stopper and bottle together, thus making counterfeiting much harder.

Author Contributions: Data curation, V.C.; Methodology, V.C. and A.S.; Project administration, A.R.; Resources, A.R.; Software, V.C.; Supervision, A.S. and A.R.; Writing—original draft, V.C.; Writing—review & editing, A.S.

Funding: This research received no external funding.

Acknowledgments: The authors gratefully acknowledge the funding of Project NORTE-01-0145-FEDER-000022 (SciTech (Science and Technology for Competitive and Sustainable Industries)), co-financed by Programa Operacional Regional do Norte (NORTE2020), through Fundo Europeu de Desenvolvimento Regional (FEDER). Portions of the research in this paper use the CASIA-IrisV1 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA). Portions of the work tested on the IITD Iris Database version 1.0. This work is partially financed by the ERDF—European Regional Development Fund through the Operational Programme for Competitiveness and Internationalisation—COMPETE 2020 Programme «POCI-01-0145-FEDER-006961» and by National Funds through the FCT—Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) within project «UID/EEA/50014/2013».

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

RIOTA	Recognition of Individual Objects using Tagless Approaches
ORB	Oriented Fast and Rotated BRIEF
PUD	Psysical Unclonability and Disorder
PUF	Psysical Unclonable Function
UNO	Unique Object
FAR	False Acceptance Rate
FRR	False Rejection Rate

References

- Costa, V.; Sousa, A.; Reis, A. Preventing Wine Counterfeiting by Individual Cork Stopper Recognition Using Image Processing Technologies. *J. Imag.* **2018**, *4*, 54. [CrossRef]
- Joaquim Ramos Costa, V.; Jorge Miranda De Sousa, A.; Rosanete Lourenço Reis, A.; Gerard Celina Robert Loyens, D. Device And Method For Identifying A Cork Stopper, And Respective Kit. WO 2018/078600 A1. 2018. Available online: <https://patents.google.com/patent/WO2018078600A1/en> (accessed on 31 October 2018).
- Lee, P.S.; Ewe, H.T. Individual Recognition Based on Human Iris Using Fractal Dimension Approach. In *Biometric Authentication*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 467–474.
- Kumar, A.; Passi, A. Comparison and combination of iris matchers for reliable personal authentication. *Pattern Recog.* **2010**, *43*, 1016–1026. [CrossRef]
- Rührmair, U.; Devadas, S.; Koushanfar, F. Security Based on Physical Unclonability and Disorder. In *Introduction to Hardware Security and Trust*; Springer: New York, NY, USA, 2012; pp. 65–102.
- European Observatory on Infringements of Intellectual Property Rights. In *Infringement of Protected Geographical Indications for Wine, Spirits, Agricultural Products and Foodstuffs in the European Union*; Technical Report; European Observatory on Infringements of Intellectual Property Rights; EUIPO: Alicante, Spain, 2016.
- Medasani, S.; Srinivasa, N.; Owechko, Y. Active learning system for object fingerprinting. In Proceedings of the 2004 IEEE International Joint Conference on Neural Networks (IEEE Cat. No.04CH37541), Budapest, Hungary, 25–29 July 2004; Volume 1, pp. 345–350.
- Buchanan, J.D.R.; Cowburn, R.P.; Jausovec, A.V.; Petit, D.; Seem, P.; Xiong, G.; Atkinson, D.; Fenton, K.; Allwood, D.A.; Bryan, M.T. Forgery: 'fingerprinting' documents and packaging. *Nature* **2005**, *436*, 475. [CrossRef] [PubMed]
- Sharma, A.; Subramanian, L.; Brewer, E.A. PaperSpeckle: Microscopic fingerprinting of paper. In Proceedings of the 18th ACM Conference on Computer And Communications Security—CCS '11, New York, NY, USA, 17–21 October 2011; p. 99.
- Takahashi, T.; Ishiyama, R. FIBAR: Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts. In Proceedings of the 2014 Fifth International Conference on Emerging Security Technologies, Lisbon, Portugal, 16–20 November 2014; pp. 46–51.

11. Rublee, E.; Rabaud, V.; Konolige, K.; Bradski, G. ORB: An efficient alternative to SIFT or SURF. In Proceedings of the 2011 International Conference on Computer Vision, Barcelona, Spain, 6–13 November 2011; pp. 2564–2571.
12. Takahashi, T.; Kudo, Y.; Ishiyama, R. Mass-produced parts traceability system based on automated scanning of “Fingerprint of Things”. In Proceedings of the 2017 Fifteenth IAPR International Conference on Machine Vision Applications (MVA), Nagoya, Japan, 8–12 May 2017; pp. 202–206.
13. Ishiyama, R.; Kudo, Y.; Takahashi, T. mIDoT: Micro identifier dot on things—A tiny, efficient alternative to barcodes, tags, or marking for industrial parts traceability. In Proceedings of the 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan, 14–17 March 2016; pp. 781–786.
14. Kudo, Y.; Zwaan, H.; Takahashi, T.; Ishiyama, R.; Jonker, P. Tip-on-a-chip: Automatic Dotting with Glitter Ink Pen for Individual Identification of Tiny Parts. In Proceedings of the 9th ACM Multimedia Systems Conference on—MMSys ’18, New York, NY, USA, 12–15 June 2018; pp. 502–505.
15. Wigger, B.; Meissner, T.; Winkler, M.; Foerste, A.; Jetter, V.; Buchholz, A.; Zimmermann, A. Label-/tag-free traceability of electronic PCB in SMD assembly based on individual inherent surface patterns. *Int. J. Adv. Manuf. Technol.* **2018**. [[CrossRef](#)]
16. Pappu, R. Physical One-Way Functions. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2001.
17. Maes, R.; Verbauwhede, I. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In *Towards Hardware-Intrinsic Security*; Sadeghi, A.R., Naccache, D., Eds.; Number 71369 in Information Security and Cryptography; Springer: Berlin/Heidelberg, Germany, 2010; pp. 3–37.
18. Dolev, S.; Krzywiecki, L.; Panwar, N.; Segal, M. Optical PUF for Non Forwardable Vehicle Authentication. In Proceedings of the 2015 IEEE 14th International Symposium on Network Computing and Applications, Cambridge, MA, USA, 28–30 September 2015; pp. 204–207.
19. Pappu, R. Physical One-Way Functions. *Science* **2002**, *297*, 2026–2030. [[CrossRef](#)] [[PubMed](#)]
20. Rührmair, U.; Hilgers, C.; Urban, S.; Weiershäuser, A.; Dinter, E.; Forster, B.; Jirauschek, C. Optical PUFs Reloaded. 2013. Available online: http://www.crypto.rub.de/imperia/md/crypto/kiltz/ulrich_paper_48.pdf (accessed on 31 October 2018).
21. Shariati, S.; Koeune, F.; Standaert, F.X. Security Analysis of Image-Based PUFs for Anti-counterfeiting. In *Communications and Multimedia Security*; De Decker, B., Chadwick, D.W., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 26–38.
22. Shariati, S.; Standaert, F.X.; Jacques, L.; Macq, B. Analysis and experimental evaluation of image-based PUFs. *J. Cryptogr. Eng.* **2012**, *2*, 189–206. [[CrossRef](#)]
23. Tuyls, P.; Schrijen, G.J.; Škorić, B.; van Geloven, J.; Verhaegh, N.; Wolters, R. Read-Proof Hardware from Protective Coatings. *Proc. Cryptogr. Hardw. Embed. Syst.* **2006**, 369–383. [[CrossRef](#)]
24. Škorić, B.; Maubach, S.; Kevenaar, T.; Tuyls, P. Information-theoretic analysis of capacitive physical unclonable functions. *J. Appl. Phys.* **2006**, *100*. [[CrossRef](#)]
25. Gassend, B.; Clarke, D.; van Dijk, M.; Devadas, S. Silicon Physical Random Functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security, New York, NY, USA, 17–20 May 2002; pp. 148–160.
26. Guajardo, J.; Kumar, S.S.; Schrijen, G.J.; Tuyls, P. FPGA Intrinsic PUFs and Their Use for IP Protection. *Lect. Notes Comput. Sci.* **2007**, *4727*, 63–80. [[CrossRef](#)]
27. Holcomb, D. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In Proceedings of the Conference on RFID Security, Graz, Austria, 11–13 July 2007; pp. 1–12.
28. Arjona, R.; Prada-Delgado, M.; Arcenegui, J.; Baturone, I. A PUF- and Biometric-Based Lightweight Hardware Solution to Increase Security at Sensor Nodes. *Sensors* **2018**, *18*, 2429. [[CrossRef](#)] [[PubMed](#)]
29. Gong, M.; Liu, H.; Min, R.; Liu, Z. Pitfall of the Strongest Cells in Static Random Access Memory Physical Unclonable Functions. *Sensors* **2018**, *18*, 1776. [[CrossRef](#)] [[PubMed](#)]
30. Bulens, P.; Standaert, F.X.; Quisquater, J.J. How to strongly link data and its medium: The paper case. *IET Inf. Secur.* **2010**, *4*, 125–136. [[CrossRef](#)]
31. Lee, J.; Lim, D.L.D.; Gassend, B.; Suh, G.; Dijk, M.V.; Devadas, S. A technique to build a secret key in integrated circuits for identification and authentication applications. In Proceedings of the 2004 Symposium on VLSI Circuits, Tokyo, Japan, 17–19 June 2004; pp. 176–179.

32. Kursawe, K.; Sadeghi, A.R.; Schellekens, D.; Skoric, B.; Tuyls, P. Reconfigurable physical unclonable functions—Enabling technology for tamper-resistant storage. In Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST, San Francisco, CA, USA, 29 October–5 November 2009; pp. 22–29.
33. Lu, Z.; Li, D.; Liu, H.; Gong, M.; Liu, Z. An Anti-Electromagnetic Attack PUF Based on a Configurable Ring Oscillator for Wireless Sensor Networks. *Sensors* **2017**, *17*, 2118. [[CrossRef](#)] [[PubMed](#)]
34. Cao, Y.; Zhao, X.; Ye, W.; Han, Q.; Pan, X. A Compact and Low Power RO PUF with High Resilience to the EM Side-Channel Attack and the SVM Modelling Attack of Wireless Sensor Networks. *Sensors* **2018**, *18*, 322. [[CrossRef](#)] [[PubMed](#)]
35. Xu, H.; Ding, J.; Li, P.; Zhu, F.; Wang, R. A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function. *Sensors* **2018**, *18*, 760. [[CrossRef](#)] [[PubMed](#)]
36. Shariati, S. Image-Based Physical Unclonable Functions for Anti-Counterfeiting. Ph.D. Thesis, Catholic University of Louvain, Louvain-la-Neuve, Belgium, 2013.
37. Valehi, A.; Razi, A.; Cambou, B.; Yu, W.; Kozicki, M. A graph matching algorithm for user authentication in data networks using image-based physical unclonable functions. In Proceedings of the 2017 Computing Conference, London, UK, 15–17 May 2017; pp. 863–870.
38. Wigger, B.; Meissner, T.; Förste, A.; Jetter, V.; Zimmermann, A. Using unique surface patterns of injection moulded plastic components as an image based Physical Unclonable Function for secure component identification. *Sci. Rep.* **2018**, *8*, 4738. [[CrossRef](#)] [[PubMed](#)]
39. Dachowicz, A.; Chaduvula, S.C.; Atallah, M.; Panchal, J.H. Microstructure-Based Counterfeit Detection in Metal Part Manufacturing. *JOM* **2017**, *69*, 2390–2396. [[CrossRef](#)]
40. Fischler, M.A.; Bolles, R.C. Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography. *Commun. ACM* **1981**, *24*, 381–395. [[CrossRef](#)]
41. Lowe, D.G. Distinctive Image Features from Scale-Invariant Keypoints. *Int. J. Comput. Vis.* **2004**, *60*, 91–110. [[CrossRef](#)]
42. Harris, C.; Stephens, M. A combined corner and edge detector. In Proceedings of the Fourth Alvey Vision Conference, Manchester, UK, 31 August–2 September 1988; pp. 147–151.
43. Punithavathi, P.; Geetha, S.; Sasikala, S. Generation of Cancelable Iris Template Using Bi-level Transformation. In Proceedings of the 6th International Conference on Bioinformatics and Biomedical Science—ICBBS '17, New York, New York, USA, 22–24 June 2017; pp. 94–100.
44. Awalkar, K.V.; Kanade, S.G.; Jadhav, D.V.; Ajmera, P.K. A multi-modal and multi-algorithmic biometric system combining iris and face. In Proceedings of the 2015 International Conference on Information Processing (ICIP), Quebec City, QC, Canada, 27–30 September 2015; pp. 496–501.
45. Mohamed, E.; Ahmed, F.; Rehan, S.E.; Mohamed, A.A. Rough set analysis and cloud model algorithm to automated knowledge acquisition for classification Iris to chieve high security. In Proceedings of the 2011 11th International Conference on Hybrid Intelligent Systems (HIS), Malacca, Malaysia, 5–8 December 2011; pp. 55–60.
46. Belcher, C.; Du, Y. Region-based SIFT approach to iris recognition. *Opt. Lasers Eng.* **2009**, *47*, 139–147. [[CrossRef](#)]
47. Marciniak, T.; Dąbrowski, A.; Chmielewska, A.; Krzykowska, A. Analysis of Particular Iris Recognition Stages. In *Multimedia Communications, Services and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 198–206.
48. Taur, J. Iris recognition based on relative variation analysis with feature selection. *Opt. Eng.* **2008**, *47*, 097202. [[CrossRef](#)]
49. Wang, Y.; Han, J. Iris Recognition Using Support Vector Machines. In *Advances in Neural Networks—ISNN*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 622–628.
50. Umer, S.; Dhara, B.C.; Chanda, B. Texture code matrix-based multi-instance iris recognition. *Pattern Anal. Appl.* **2016**, *19*, 283–295. [[CrossRef](#)]
51. Rahulkar, A.D.; Holambe, R.S. Half-Iris Feature Extraction and Recognition Using a New Class of Biorthogonal Triplet Half-Band Filter Bank and Flexible k-out-of-n: A Postclassifier. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 230–240. [[CrossRef](#)]

52. Kumar, A.; Hanmandlu, M.; Das, A.; Gupta, H.M. Biometric based personal authentication using fuzzy binary decision tree. In Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 396–401.
53. Zhou, Y.; Kumar, A. Personal Identification from Iris Images Using Localized Radon Transform. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 2840–2843.
54. Costa, V.; Sousa, A.; Reis, A. CBIR for a wine anti-counterfeiting system using imagery from cork stoppers. In Proceedings of the Iberian Conference on Information Systems and Technologies, CISTI, Cáceres, Spain, 13–16 June 2018; pp. 1–6, Volume 2018.
55. Shariati, S.; Jacques, L.; Standaert, F.X.; Macq, B.; Salhi, M.A.; Antoine, P. Randomly driven fuzzy key extraction of unclonable images. In Proceedings of the 2010 IEEE International Conference on Image Processing, Hong Kong, China, 26–29 September 2010; pp. 4329–4332.
56. Shariati, S.; Standaert, F.X.; Jacques, L.; Macq, B.; Salhi, M.A.; Antoine, P. Random Profiles of Laser Marks. In Proceedings of the 31st WIC Symposium on Information Theory in the Benelux, Rotterdam, The Netherlands, 11–12 May 2010; pp. 27–34.
57. Costa, M.; Sanchez, E.; Sanchez, C. Caracterização de espumas plásticas e cortiça para aplicação em um sistema de segurança acoplado ao para-choque frontal veicular. *Rev. Ciência Tecnol.* **2017**, *20*, 36.
58. G154-16. *Standard Practice for Operating Fluorescent Ultraviolet (UV) Lamp Apparatus for Exposure of Nonmetallic Materials*; Technical Report; ASTM: West Conshohocken, PA, USA, 2016.

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).