Perceptual Hashing for Authentication using Physically Unclonable Functions

João Barbosa Tareco
Instituto Superior Técnico
joao.tareco@tecnico.ulisboa.pt

***Abstract*—The development of authentication methods is an increasingly important topic, which is also the focus of a wide discussion in the public sphere. Optical PUFs are a type of cryptographic device that leverages the inherent randomness of certain objects (tokens) for authentication purposes, by probing them with a coherent light, generating unique speckle patterns. However, a problem arises due to intra-variability, where speckle patterns obtained from the same token can vary depending on the acquisition environment and system alignment. This work shows how a PUF system utilizing tracing paper tokens can be employed for authentication purposes, despite the intra-variability between acquired speckle pattern images. Two datasets were acquired with the purpose of simulating intra-variability (turning the system ON and OFF and changing the camera positioning). Non-reflective black tape around the RoI was also used to automate the cropping process. In the pre-processing stage, warping was performed, as well as pixel intensity normalization, followed by Gabor Filtering. Two feature extraction methods were tested for hash generation using: (i) Discrete Cosine Transform and (ii) Principal Component Analysis. Two classification approaches were tested: (i) a Hamming Distance based classification and (ii) machine learning classifiers. For a data independent method, the DCT combined with HD-based classification achieved the best results. For a data dependent method, the PCA with machine learning classifiers performed the best overall. Gabor filtering provided an authentication performance boost, but the kernels used may need to be calibrated between datasets.**

***Index Terms*—Discrete Cosine Transform; Principal Component Analysis; Support Vector Machines; k-Nearest Neighbour; Random Forest; Machine Learning; Hash Generation; Authentication; Gabor Filtering; Intra-Variability;**

I. Introduction

The development of authentication methods is an increasingly important topic, which is also the focus of a wide discussion in the public sphere. From maintaining security in communications to preventing counterfeiting of documents, authentication has a necessary role in our society and everyday life.

Physically Unclonable Functions (PUFs) [1] are a type of cryptographic device that leverages the inherent randomness of certain objects as an authentication token, which can be used as a fundamental layer in the design of security systems. They are the physical equivalent of one-way mathematical transformations that, upon external excitation, can generate irreversible responses. PUFs are characterized by challenge-response pairs, in which a certain input to the system generates an uniquely related output. This thesis focuses on Optical PUFs. These consist of an inhomogeneous material that contains inherent imperfections and random structures that, when challenged with a coherent light source, creates an unique speckle image response. This speckle pattern, obtained from the scattering of light through the object, can be used for authentication purposes. Image based PUFs are especially useful for anti-counterfeiting purposes. Not only can an object be used to generate a cryptographic key, but this key can also be used to authenticate the object itself.

A. Objectives

A sheet of paper, for instance used as the support of an important document, can be used as an optical diffuser, or token, since the microscopic structures of the paper diffuse light in random directions. This token can be used to generate an unique speckle pattern when challenged with a coherent light. This would be an example of a PUF system used for authentication purposes, where the sheet of paper acts as the authentication token. As illustrated in figure 1, the document can be authenticated by generating a hash key from the perceptual analysis of the speckle image, obtained by the PUF system, and matching it to the hash key value stored in a database. However, a problem arises due to the variability in challenge/response pairs. In fact, a same challenge can generate different responses depending on the time instant the image was recorded at. The same light probing the document paper token, previously described, can generate slightly different speckle patterns.

The main objective of this thesis is to deal with the variations between different acquisitions from the same token by developing a perceptual hash algorithm that is robust against intra-variability. In a first step, the speckle pattern images obtained will be processed by being cropped and scaled as well as corrected in illumination variations. This will yield images with standard geometry that can be compared to a reference. After this, perceptual hash algorithms can be applied to the normalised images, to produce responses that are not affected by intra-variability. So, in a given PUF, different acquisitions of the same challenge taken at different temporal instants will yield the same responses. This will allow accurate authentication of PUF tokens.

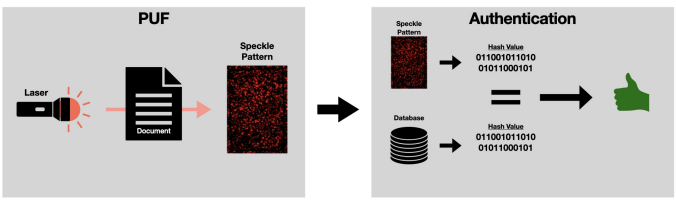

Fig. 1. Example of using PUFs for document authentication.

B. Document Outline

This extended abstract is composed of six sections, whose contents are summarized here:

- **Introduction**: In this section, the motivation and objectives for this dissertation are presented.
- **Review of Authentication Techniques using Optical Physical Unclonable Functions**: In this section, the state of the art for optical PUF devices and perceptual hashing is presented.
- **The PUF System Used**: In this section, the physical PUF system used is described. The characteristics of the acquired datasets are also explained.
- **Proposed Approach for Authenticating a PUF**: In this section, the proposed approach for authenticating the PUF tokens, despite intra-variability, is explained.
- **Experimental Results**: In this section, the experimental results obtained from the proposed algorithms are presented and discussed. The parameter tuning done for each algorithm is also described.
- **Conclusion and Future Work**: This section presents the conclusions of this work, as well as possible approaches for future work.

II. Review of Authentication Techniques using Optical Physical Unclonable Functions

Optical PUF's were first proposed by Pappu et al. [1]. In their implementation the light source can move in a 3D space pointing to a stationary scattering medium. The challenge is the position of the laser beam and the response is the speckle pattern recorded. The scattering medium considered was composed of a large number of randomly positioned silica spheres embedded in hardened epoxy. Since then, many iterations of this fundamental concept have been proposed.

A cost effective and relevant example of a PUF implementation is the called PaperSpeckle [2], which consists of a portable paper fingerprinting system that can identify and authenticate paper. The main use for this is to prevent document forgery and counterfeiting, which is a very relevant problem around the world. In PaperSpeckle the paper works as the scattering medium, having random and hard to replicate structures that create unique speckle images. PaperSpeckle showed that it is possible to extract repeatable speckle patterns from microscopic regions of paper, with just paper, pen and a microscope. These speckle patterns can then be turned into unique fingerprints associated with the document.

A. Overview of Perceptual Hashing Methods

There are several methods of perceptual hashing that have been proposed over the last decades, each with different approaches, and exploring distinct concepts. A recent publication by Du et al. [3] describes the results of a survey where they compare and categorise existing perceptual hashing methods. They propose that perceptual hashing can be grouped into five main categories:

- **Invariant feature transform methods** - Methods in this category explore a representation of the input image in a transformed domain. They generally have the advantage of being robust against certain types of distortion and noise attacks. Wavelet and Quaternion based hash functions fall under this category, as well as the Discrete Cosine Transform (DCT);
- **Local feature methods** - Methods in this category leverage local features that are invariant under content preserving attacks. Feature-point based hash functions fall under this category, including examples such as SIFT, SURF and ORB;
- **Dimension reduction methods** - Methods in this category make use of dimension reduction techniques. SVD based hash functions fall under this category, with Principal Component Analysis (PCA) being an example;
- **Statistic feature methods** - Methods in this category take advantage of image statistics for the calculation of the hash value. RPIVD and histogram based hash functions fall under this category;
- **Learning methods** - Methods in this category take advantage of efficient learning algorithms that can be implemented to generate hash values based on parameters learned from the training of data;

B. Gabor Transform for Speckle Pattern Analysis

Speckle patterns, in general, have very few predominant features. To improve their perceptual analysis, the Gabor transform can be useful. Theoretically, Gabor filtering is closely related to the primary visual cortex [4], in terms of perceiving texture and detecting edges. In the realm of optical PUFs, the Gabor transform is often used in speckle pattern authentication systems.

A Gabor filter is a linear filter. In the spatial domain, it is derived from the modulation between a Gaussian kernel and a sinusoidal plane wave. Because of this, the parameters of a 2-D Gabor function include wavelength λ, orientation θ, phase offset ϕ, as well as aspect ratio $\gamma < 1$, and bandwidth b . The gabor kernel can be defined as:

$$g(x, y; \lambda, \theta, \phi, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)\cos\left(2\pi\frac{x'}{\lambda} + \phi\right) \quad (1)$$

where

$$x' = x\cos\theta + y\sin\theta,$$

$$y' = -x\sin\theta + y\cos\theta.$$

Due to the inherent orientation of a Gabor kernel, certain features of the unfiltered image that are aligned with that orientation will become more prevalent in the filtered image.

In the first optical PUF implementation, proposed by Pappu et al. [1], Gabor filtering is utilized for the generation of hash values. In short, speckle patterns are down-sampled by applying Gabor filters, thresholding at zero and scaled down. This method can be represented as a multi-resolution pyramid, in which a level of the pyramid refers to one iteration of filtering and sub-sampling of the image. In this algorithm only diagonal orientations are used on the Gabor kernels. This is mainly due to the fact that the values of the Gabor transform along the diagonals are much less sensitive to small changes in the horizontal or vertical positioning of the token. The work carried out by Pappu et al. not only introduced optical PUFs, but established the Gabor transform as a capable tool for the analysis of these types of images. In the implementation of PaperSpeckle [2], the Gabor transform is also used. In both

papers [2] ,[1] only the imaginary part of the Gabor wavelet is used to extract bits. By doing this, any illumination defects, contrast variations or poor focus that are present in the speckle image are eliminated. This improves the robustness of the system.

C. Classification Algorithms

In the context of PUF authentication, hash generation is only a means to an end, which is classification. After an hash is generated from a particular image, it needs to be classified. To accomplish this, classifying algorithms are employed.

A normalized hamming distance (HD) classification approach is widely used in this space, with a few notable mentions being [5], [1], [6]. The normalized hamming distance can be interpreted as the number of different bits between two binary hashes of the same size. Because it is normalized, when its value is zero, it means that both hashes are the same. On the contrary, if the hamming distance is 1, both hashes are 100% different. Utilizing a hamming distance threshold for classification means that, in short, if the hamming distance between two hashes is below a certain threshold, they are considered to be from the same image. A benefit of this classification approach is that it allows for the use of error correction codes, which could be employed to improve the authentication performance of the entire PUF system. It is also data independent, meaning it does not need a training set to be able to classify new occurrences in a testing dataset.

Classification is also the driving force of machine learning. In the topics of authentication systems, such as face recognition applications, machine learning plays an important role, and is served as the fundamental technique in many existing literatures. Machine learning utilizes previously obtained data, which is denominated as the training set, to make accurate predictions in new data, which is denominated as the test set [7]. In short, machine learning, for classification purposes, has two main categories: Unsupervised learning and supervised learning. Unsupervised learning uses an unlabeled dataset (i.e. the feature vectors from the dataset don't contain a label, like a specific PUF token) to train a certain model and then classifies new data based on it. PCA is an unsupervised learning technique, on which a vector space is built so that new data can be projected upon it. This projected data tends to cluster when it is similar, therefore allowing it's classification. The results from unsupervised learning could be further used for supervised learning. Supervised learning utilizes labeled datasets to train a model and make predictions on it.

On table I, an overview of some important machine learning classifiers is presented. All four algorithms employ different classification mechanisms and are from different categories [7].

TABLE I
OVERVIEW AND CATEGORIZATION OF SOME WIDELY USED MACHINE LEARNING CLASSIFIERS.

Method	Category
Support vector machine (SVM)	Linear Model
K-nearest neighbors	Non-parametric model
Decision tree	Non-metric model
Random forest	Mixed method

Support vector machines (SVM) is one of the most successful classification algorithms developed to date, being widely used and often providing results that are better than competing methods [8]. SVM tries to make a decision boundary so that the separation between two classes the widest it can be. To accomplish this, the distance between the decision threshold and the closest points from each class (support vectors) are calculated. The hyperplane for which the margin is maximized is returned as the optimal hyperplane.

K-nearest neighbors is likely the simplest supervised learning algorithm to understand. Given a new unlabeled data point x_a, simply find the k nearest neighbouring points. The label of x_a is determined by the majority of the labels of the k nearest neighbours.

The decision tree is a hierarchical construct that looks for optimal ways to split the data in order to provide a robust classification and regression. These decision trees generally lack robustness to different samples of the data. Thus, random forest works by constructing various decision trees at training time. New data is then classified by the class given as output by the majority of the trees.

III. The PUF System Used

The physical PUF system utilized was developed in [9], having been employed to acquire the datasets used in this work. This system is described in figure 2.

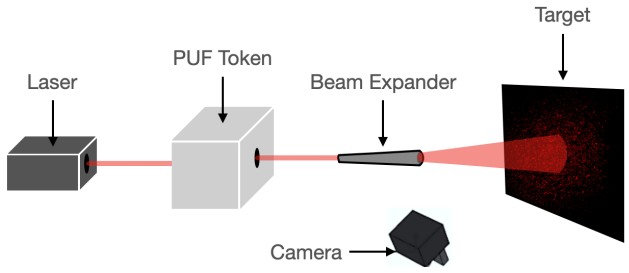

Fig. 2. Illustration of the physical PUF system used to generate and acquire speckle pattern images.

The light source of this optical PUF system is a coherent He-Ne Laser (ref. HNLS008R by Thorlabs). The beam passes through the PUF, which consists of a nonwoven polyester paper fabric that is characterized by being water resistant, capable of withstanding high mechanical strain and with a density of 250 g/cm^2. This type of tracing paper was chosen because it is a translucent object, meaning that the light emitted by the laser will be transmitted and result in a clear speckle pattern. The paper is placed in a sample holder which consists of a compact structure covered with black tape to prevent any external interference from light sources other than the laser. The light that passes through the PUF is directed into a beam expander, that serves the purpose of increasing its diameter. The beam expander used is the GBE20-A - 20X Achromatic Galilean Beam Expander (by Thorlabs). The speckle pattern is then projected onto a sheet of paper with a black rectangle printed on it, acting as a target. The purpose of this black rectangle is to have have a focus area of the speckle pattern which will later be perceptually analysed. If the

entire obtained image were to be analysed, some control over certain conditions of the system would be lost (like camera focus a lighting conditions). To acquire the images, the Camera Module V2 connected to a Raspberry PI is used.

A. Image Acquisition

To test the authentication algorithms implemented, a dataset that purposefully introduces intra-variability between acquisitions is necessary. To understand what varies the most between acquisitions taken at different times, it is important to define how the system is operated. Initially, the laser is switched off. After a PUF token is inserted the camera should be positioned in as close of a position as possible as previous acquisitions of the same token. The paper token, which is placed under the sample holder, should also be positioned with maximal aligning to prevent fluctuations in the speckle pattern.

The three main sources of intra-variability in the system identified were:

- Switching ON and OFF the entire system, creating a change in the phase of the optical signal.
- Changes in the orientation of the camera between 5º and 15º degrees in relation to the target.
- Changes in alignment of the PUF token in the mask.

However, in [9] it is stressed that token alignment is a key factor in the implementation of optical PUF devices. In fact, even a small difference in the positioning of the PUF token in the mask can generate an entirely different speckle pattern. This is because the structures of the paper function as a chaotic system. Because of this, only the two first sources of intra-variability were employed in the acquisition of the dataset.

Two different datasets were obtained. In the first obtained dataset, four different tokens were utilized. For each PUF token, certain rules were followed during the acquisition process:

- Switching OFF and ON the system between all acquisitions.
- Obtaining 50 acquisitions with a static camera.
- Obtaining 50 acquisitions while varying the camera orientation between 5º and 15º degrees in relation to the target.

The difference between camera positioning/orientation is exemplified in Figure 3.

After testing was done with the described dataset A, some limitations needed to be addressed. Particularly, an effort was made to aid the cropping of the black rectangle. To do this, a new dataset B was obtained. A black non-reflective tape was used on the outside of the black rectangle. This means that the camera only captures the content on its inside. The same acquisition rules employed in the first dataset were also used. This translates into a dataset with 400 images.

With both datasets combined, 800 speckle pattern images are available for testing. An overview of the described datasets is presented in table II

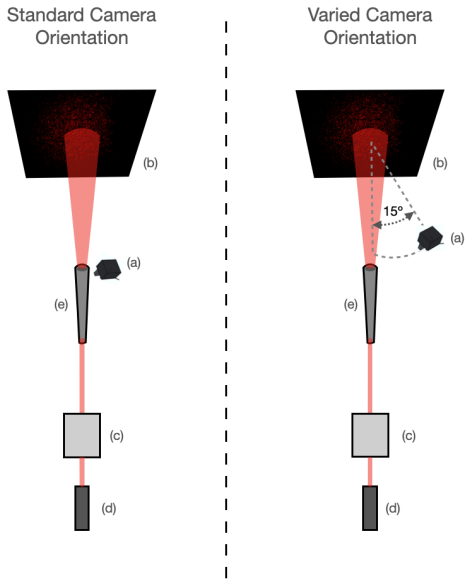

Fig. 3. Exemplification of the variance introduced by changing the positioning/orientation of the camera; (a) Camera; (b) Target; (c) PUF Token; (e) Beam Expander;

TABLE II
OVERVIEW OF THE OBTAINED DATASETS.

Dataset	PUF Token	Conditions	Notes
A	1AA	Standard camera orientation	Standard target
	1AB	Different camera orientations	
	1BA	Standard camera orientation	
	1BB	Different camera orientations	
B	2AA	Standard camera orientation	Target with black tape to reflect only the contents of the rectangle
	2AB	Different camera orientations	
	2BA	Standard camera orientation	
	2BB	Different camera orientations	

IV. Proposed Approach for Authenticating a PUF

Each proposed approach can be divided into 5 distinct modules, which are represented in figure 4.

It is important to note that an authentication system has two distinct operational settings: a registration phase and an authentication phase. The registration phase encapsulates the procedure of registering a new item (a new PUF token) in the system. In this case, it consists of perceptually analysing a speckle pattern image and generating an hash value. This value is then stored. The authentication phase consists of the same process of analysing a new speckle pattern image and generating an hash value for it. However, once this is done, the hash value is compared to all other previously registered hashes and consequently classified as a certain PUF token.

In this thesis, a DCT based approach (an invariant feature transform based method, which is data independent) is compared to a PCA based approach (a dimension reduction based method). These feature extraction techniques were chosen for comparison because one is data independent (DCT) and the other is data dependent (PCA). Each of these feature extraction methods is then paired and tested alongside different classifying strategies: a simple hamming distance threshold classification or a machine learning classifier (like Support Vector Machines). This modular process of testing how the different feature extraction and classification methods work together, in this context, gives us four distinct approaches, which are represented in table III.

A. Pre-Processing

The pre-processing module is always present in the proposed solutions, as it contributes decisively to improve their

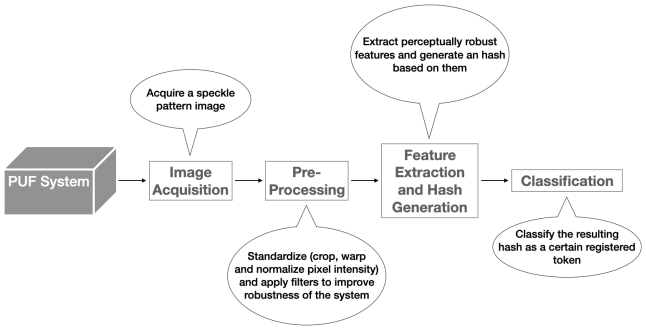

Fig. 4. Diagram and description of each module in a perceptual hashing based authentication algorithm.

TABLE III
AUTHENTICATION APPROACHES IMPLEMENTED AND TESTED.

Approach	Feature Extraction Method	Classification Method
Approach 1	DCT	Hamming Distance Classification
Approach 2	DCT	Machine Learning Classifier
Approach 3	PCA	Hamming Distance Classification
Approach 4	PCA	Machine Learning Classifier

robustness. This module has four steps:

- Conversion to grayscale.
- Perspective warping and cropping of the speckle pattern images.
- Image standardization, which includes image resizing and normalizing the intensity of all pixels.
- Gabor filtering.

In a first step, the raw input image is first converted to grayscale [10]. After this, the images are warped and cropped.

If the entire obtained image were to be analysed, some control over certain conditions of the system's implementation would be lost. Cropping and warping the obtained images, so that they only consist of the contents inside the black rectangle all from the same perspective as each other, is an important step towards improving the system's authentication performance.

The process of cropping and warping the images can be structured in the following logic:

- Detecting the black rectangle (possibly utilizing the Hough Transform, ORB, pixel intensity)
- Cropping only the contents of the black rectangle
- Warping (taking similar points between a distorted image and a default image and finding the homography)

For the first dataset, where black non-reflective tape is not used, cropping is done manually by selection of the area between the pixel coordinates that more or less coincide with the black rectangle. The manual cropping process takes a considerable amount of time, making it impractical in the scope of an authentication algorithm. However, in dataset B, with the non-reflective black tape around the rectangle, it can easily be discriminated from the rest of the image, allowing for an automatic cropping process. To accomplish this, the image is converted to binary using a thresholding operation. This improves the accuracy of contour discrimination. Contours can be described simply as a curve joining all the continuous points, along a boundary, having the same intensity. Afterwards, a straight bounding rectangle that encompasses the largest contour can be computed (this is done with OpenCV's *boundingRect()* function).

In terms of warping, ORB is utilized to detect feature points and find the homography between a distorted image and an image acquired with standard camera positioning.

The image is then resized to 64x64 pixels, which is important for subsequent image matching operations. After this, the intensity of each pixel of the image is normalized following a correction ratio. This makes each image have all pixels in a range of intensities from 0 to 255. Finally, Gabor filtering is applied. The final implementation utilizes a single Gabor kernel with a 45º degree diagonal orientation. As it was shown in [1], diagonally orientated Gabor kernels emphasize diagonal features in the speckle pattern, reducing the effect of unwanted horizontal or vertical movement in the token image. The pre-processing stage is presented in figure 5 as a block diagram.

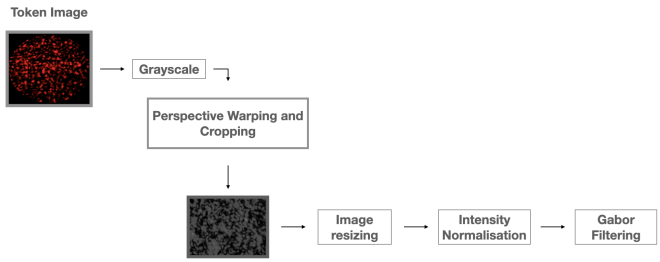

Fig. 5. Pre-processing diagram all implementations.

B. Feature Extraction and Hash Generation

In approaches 1 and 2 of table III, the DCT is applied. To obtain a one-dimensional array, a zig-zag type scan is utilized, as the DCT tends to compact most of the energy in the first coefficients of the matrix. The DC coefficient is discarded as it does not translate any discriminating information from the images. This results in a vector of coefficients, which will be the hash value of the image. Because the initial coefficients hold the majority of the image's energy, the final hash does not need to contain all coefficients given by the DCT. More coefficients in the final hash will translate more of the image's data. However, the hashes will take up more space in memory and hash matching algorithms, i.e. the classifiers will take longer to compute the results. From the research done in [9], for this type of PUF token, a 64 bit hash provides sufficient discrimination between different paper tokens. Hash sizes of 64 bits are also common in cryptographic studies [11], [12]. Because of this, the DCT based algorithms generate hashes with 64 bits.

Finally, the resulting array is quantized into the final hash, so that the sequence can be normalized into a binary form. The conditions for the quantization are

$$h_i = \begin{cases} 0, & \text{if } C_i < m \\ 1, & \text{if } C_i \geq m \end{cases} \tag{2}$$

where h_i is the hash value, C_i is the coefficient of the array and m is the mean of all the coefficients. So any

coefficients that are above the median value are declared to 1, and any below as 0. Quantization is necessary for hamming distance calculation. There are several quantization schemes, some more complex than others. The applied mean based quantization is taken from [10], which showed good results in conjunction with the DCT.

In approaches 3 and 4, the PCA is applied. As it was said in previous sections, PCA is a data dependent method of feature extraction. This means that it needs a training set to extract predominant patterns from. After the token images are pre-processed, they are reshaped into a vector with one dimension. This vector is then appended to a larger matrix that contains all other vectors from reshaped images of tokens already registered in the system. This matrix serves as a vector space for other token images to be projected upon [13], returning weighted coefficients, that allow for their classification. The resulting hash is then quantized in the same way as in the DCT based approaches.

C. Classification

There are two different means of classification utilized in this dissertation. One is a normalized hamming distance threshold based classification and the other consists of machine learning classifiers.

The hamming distance obtained from two images of the same PUF token is denominated intra-HD, while the one obtained from two images of different PUF tokens is denominated inter-HD. In these types of classification problems, the HDs are represented in a histogram and can be described by a Gaussian probability density function. The mean (μ) and variance (σ^2) values of this Gaussian distribution function can be utilized to evaluate the robustness of the system. More distant mean values of the intra-HDs and inter-HDs translate in a better classification capacity. Lower variance also makes a correct classification more likely.

Utilizing a hamming distance threshold for classification means that, in short, if the hamming distance between two hashes is below a certain threshold, they are considered to be from the same PUF token. This threshold can be calculated with the mean values of the intra and inter Hamming distances, as well as their variances [14].

Four different machine learning classifiers were also selected to holistically understand what works best. Each of these supervised learning techniques can be organized in different categories [7]. These machine learning classifiers and their organization are presented in table IV.

TABLE IV
OVERVIEW AND CATEGORIZATION OF THE MACHINE LEARNING CLASSIFIERS TESTED IN THE IMPLEMENTED ALGORITHMS.

Method	Category
Support vector machine (SVM)	Linear Model
K-nearest neighbors	Non-parametric model
Decision tree	Non-metric model
Random forest	Mixed method

V. EXPERIMENTAL RESULTS

After implementing the previously described algorithms, it is essential to analyse how they perform with both obtained datasets. There are two datasets (dataset A and dataset B). Each dataset utilizes 4 different PUF tokens and contains 400 images (100 for each token under different conditions).

It is important to note that all methods (except the PCA and machine learning classifiers) utilized in these algorithms are from the OpenCV Python package. The PCA implementation and machine learning classifiers utilized belong to Scikit Learns's Python package

A. Evaluation Metrics

First, it is important to define the evaluation metrics utilized in this chapter. In general, the classification measures obtained in these types of problems are based on the concepts true positive (TP), false negative (FN), false positive (FP) and true negative (TN), which can be explained, for a binary problem, as:

- True positive means it was correctly predicted as positive.
- False negative means it was incorrectly predicted as negative.
- False positive means it was incorrectly predicted as positive.
- True negative means it was correctly predicted as negative.

The accuracy rate (Acc) is a widely used and practical evaluation metric. It evaluates the performance of the classifier by means of its percentage of correct predictions. The *Acc* is computed as in $\mathrm{Acc}_e q$.

$$Acc = \frac{TN + TP}{FN + FP + TN + TP} \tag{3}$$

The error rate (Ecc) is another useful metric, which translates the percentage of incorrect predictions done by the classifier. Both the *Acc* and *Ecc* are general measurements that can be extended to multiclass classification problems. The *Ecc* is given by $Ecc = 1 - Acc$.

B. Parameter Tuning

Several different tools are used in the implementations of the proposed solutions. Each of these methods and processes have parameters that need to be tailored to their application environment.

1) Speckle Pattern Image Sizes: First, the size to which images should be resized to should be discussed. In this analysis, image sizes will be chosen with the aim of keeping processing times low, while achieving satisfactory authentication results. Based on some past research [10], from which the DCT based proposed approaches are based on, resizing images to 32x32 pixels seems to work well. When it comes to the PCA based approaches, it has been shown by Yuen et al. [15] and also in [16] that a face image with a resolution of 16×16 is enough for authentication using PCA. Because of this, we consider the DCT based approaches as the bottleneck in image size selection. With this in consideration, for the tests to decide what image size to use, the DCT is utilized. Image sizes from 16x16 to 512x512 are examined.

The computing time taken to execute the DCT based algorithm and compare each hash, from a subset of dataset A, is plotted, for each image size, in Figure 6.

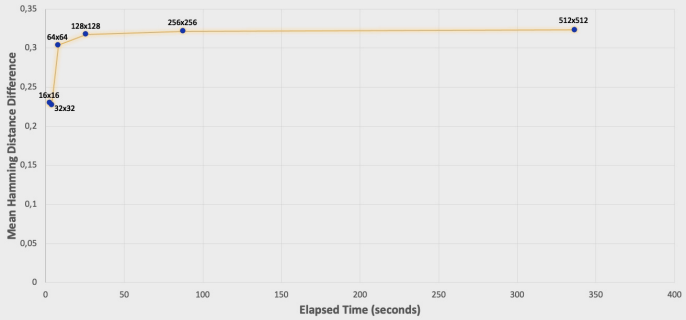

Fig. 6. Impact of resizing the speckle pattern images to different sizes in terms of computational time taken and hamming distance difference between the same tokens and different tokens.

Each dot is the average result for a specific image size. On the y axis we have the difference between the mean inter hamming distance and the mean intra hamming distance. On the x axis the time it took to process the entire subset of the dataset is displayed. The optimal image size will be the one closest to the "elbow" of the blue line, i.e. 64x64. Resizing images to 64x64 provides nearly as much authentication capability as bigger image sizes and is just a little slower than smaller image sizes.

2) Gabor Kernel Parameters: Once the image size is selected, the Gabor kernel utilized should be discussed. When generating Gabor kernels, three parameters have a larger impact, in the resulting filtered image, when compared to the others. These are the wavelength (or frequency), orientation and the scale of the kernel [17].

The orientation of the Gabor kernel will be kept at $\frac{\pi}{4}$ relative to the x axis. As explained in section II-B, this orientation reduces the impact of unwanted vertical and horizontal changes in camera positioning. The size of the kernel will also be set at 3x3, as it is one of the most common choices [18]. This means that the only variable left to be selected is the frequency of the kernel.

The Gabor filter which best applies to this specific type of speckle pattern image will be the one that maximizes the difference between the mean inter-hamming distance and the mean intra-hamming distance. The testing process done to select the image size is repeated here, with dataset A, for different frequency values. The results are presented in Figure 7.

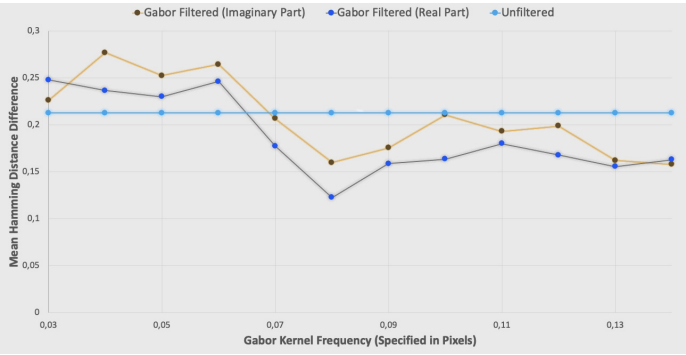

Fig. 7. Impact of Gabor filter frequency in authentication performance, comparing the mean hamming distance difference. It is possible to see the benefit of considering only the imaginary part of the Gabor kernels.

From the obtained results, the Gabor kernel selected for use in the pre-processing stage of the algorithms has the parameters summarized in table V.

TABLE V
MAIN CHARACTERISTICS OF THE GABOR KERNEL USED IN THE PRE-PROCESSING STAGE OF THE IMPLEMENTED ALGORITHMS.

Gabor Kernel	
Characteristic	Value
Size	3x3
Orientation	$\frac{\pi}{4}$
Frequency	0.04

C. Performance Results with Hamming Distance Based Classification

In this section, the authentication results obtained with each proposed approach and a hamming distance based classification are presented and discussed.

1) Testing with Dataset A: The hamming distances obtained by comparing the hashes generated with the DCT/PCA based algorithm can be plotted using an histogram. The resulting metrics are utilized for performance evaluation. To better evaluate the impact of Gabor filtering, the algorithms were tested both with and without it (the pre-processing pipeline was kept the same, except for Gabor filtering removal). An example of one of the obtained histograms is presented in figure 8.

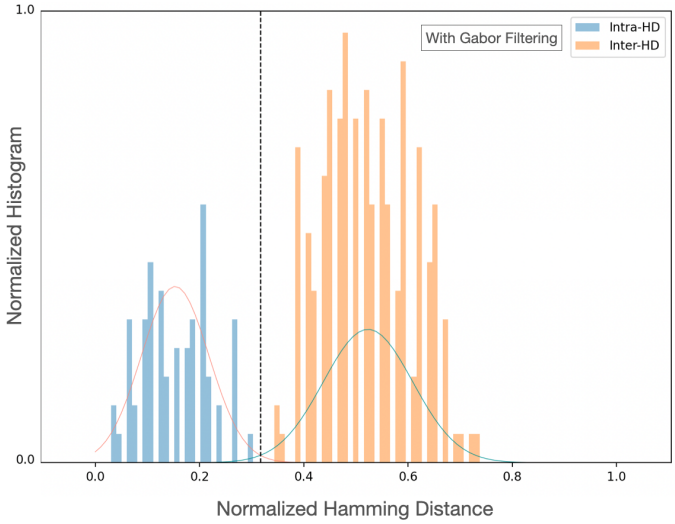

Fig. 8. Histogram obtained from the DCT based approach with Gabor filtering. The adapted normal distribution curves are also plotted. The optimal decision threshold was also computed and plotted as a vertical dotted line in the histogram.

The specific metrics of each normal distribution obtained from all tested algorithms are presented in table VI. It is to note that all algorithms generate a 64 bit hash. In the PCA based algorithms, 20 images from each token are utilized for training (10 images with standard camera orientation and 10 images with varied camera orientations). The remainder of the dataset is utilized for testing. It is important to note that, with the algorithm that utilizes Gabor filtering, 10 of these 20 images are the resulting real part and the other 10 are the resulting imaginary part derived from the Gabor kernel.

TABLE VI
METRICS OBTAINED FROM THE HAMMING DISTANCE HISTOGRAMS IMPLEMENTED ALGORITHMS ON DATASET A.

Algorithm	$\mu_{inter-HD} - \mu_{intra-HD}$	$\mu_{intra-HD}$	$\mu_{inter-HD}$	$\sigma_{intra-HD}$	$\sigma_{inter-HD}$
DCT With Gabor Filtering	0.317	0.153	0.523	0.064	0.085
DCT Without Gabor Filtering	0.285	0.138	0.455	0.066	0.081
PCA With Gabor Filtering	0.324	0.156	0.480	0.059	0.071
PCA Without Gabor Filtering	0.182	0.345	0.527	0.177	0.138

TABLE VII
METRICS OBTAINED FROM THE HAMMING DISTANCE HISTOGRAMS OF THE DCT BASED APPROACH ON DATASET B.

Algorithm	$\mu_{inter-HD} - \mu_{intra-HD}$	$\mu_{intra-HD}$	$\mu_{inter-HD}$	$\sigma_{intra-HD}$	$\sigma_{inter-HD}$
DCT With Gabor Filtering	0.340	0.152	0.492	0.056	0.052
DCT Without Gabor Filtering	0.372	0.093	0.465	0.042	0.041
PCA With Gabor Filtering	0.161	0.375	0.536	0.103	0.080
PCA Without Gabor Filtering	0.191	0.347	0.538	0.157	0.143

When new images are projected on the PCA matrix, only the imaginary part of the Gabor filtering is utilized. This combination provided superior classification performance. This is likely due to an increase of the eigenspace generated, allowing more faithful descriptions of new speckle pattern images.

Lower variance (σ) values are beneficial, as well as a higher difference between the mean of the inter-HDs and intra-HDs ($\mu_{inter-HD}$ and $\mu_{intra-HD}$).

In this setting, both DCT based algorithms correctly classified all speckle pattern images, with Gabor filtering providing a slight edge in performance.

The PCA based algorithm that did not utilize Gabor filtering performed significantly worse, having an *Acc* score of 76,5% (the other algorithms showed a clear distinction between intra-HDs and inter-HDs, which translates into an *Acc* of 100%). It is important to point out that the quantization method utilized likely results in a large amount of data loss, as each hash coefficient is binarized only with relation to the mean of the entire hash.

2) Testing with Dataset B: The same testing process performed on dataset A was followed for the tests with dataset B, which should allow the proposed algorithms to achieve a slight increase in robustness, as the automatic image cropping procedure is expected to avoid some imprecision that may result when doing manual cropping. The obtained results are presented in table VII.

Although both DCT based algorithms performed at 100% *Acc*, Gabor filtering resulted in a slight decrease of performance. Since the Gabor kernel was tuned with dataset A, its performance might improve if tuned again for the conditions of dataset B. However, since the achieved accuracy was still 100%, it was considered that the previous setup can be used for both datasets.

From the results we can conclude the PCA based algorithm does not provide satisfactory results in this scenario. Also, when using Gabor filtering, a decrease in performance was also observed.

D. Performance Results with Machine Learning Classifiers

In this section, the authentication results obtained with each proposed approach and machine learning based classification are evaluated. The metrics discussed in the previous section are also utilized here for evaluation.

In the evaluation stage of the supervised machine learning methods, overfitting is an important concern to take into consideration [19]. A model that overfits the training data will fail to accurately fit the observed data on the test dataset. Since overfitting typically occurs when the amount of training data is limited, cross-validation is utilized [20].

All four machine learning classifiers considered, as well as the cross-validation functions, are implemented using the Scikit Learn Python package (*sklearn*). To test the developed algorithms, a 5-fold cross validation scheme is utilized.

1) Testing with Dataset A: The results obtained with the DCT and PCA based algorithms combined with the different classifiers utilizing dataset A are shown in Table VIII.

From the displayed results, it is possible to conclude that the proposed DCT algorithm including Gabor filtering, with any of the tested machine learning classifiers, achieves satisfactory classification/authentication performance. SVC with a polynomial kernel performed the worst. This might seem counter intuitive, but the explanation is probably that overfitting is occurring because the kernel has a higher complexity. When Gabor filtering is removed from the DCT based algorithm, there is a significant decrease in the authentication performance. This reinforces the efficacy of using the selected Gabor kernel in the optical PUF scenario.

The PCA based approach, combined with any of the machine learning classifiers, achieves a very good authentication performance. In this result set, the difference between an algorithm with Gabor filtering and another without it is not as apparent. For four of the classifiers (all except the SVC with a polinomial kernel) the accuracy results seem to have slightly decreased when including Gabor filtering. This could be explained by the fact that these results are all very high, and in many of the cases the slight decrease with Gabor filtering is not meaningful.

It is important to note, however, that these results are obtained with a somewhat restricted dataset of only 4 different tokens with 400 images. Were these algorithms tested with a larger dataset, the performance would likely decrease.

2) Testing with Dataset B: The results obtained with the DCT and PCA based algorithms combined with the different

TABLE VIII
AUTHENTICATION RESULTS WITH DATASET A AND MACHINE LEARNING CLASSIFIERS

		With Gabor Filtering		Without Gabor Filtering	
	Classifier	Acc	Standard Deviation	Acc	Standard Deviation
DCT	SVC (Linear Kernel)	0.98	0.01	0.39	0.03
	SVC (Polynomial Kernel)	0.86	0.06	0.28	0.04
	Decision Tree	0.96	0.03	0.49	0.03
	k-Nearest Neighbour	0.96	0.02	0.43	0.05
	Random Forest	0.98	0.02	0.49	0.04
PCA	SVC (Linear Kernel)	0.99	0.01	1.00	0.00
	SVC (Polynomial Kernel)	0.90	0.06	0.75	0.25
	Decision Tree	0.97	0.03	0.99	0.01
	k-Nearest Neighbour	0.96	0.03	0.98	0.02
	Random Forest	0.95	0.05	0.98	0.02

TABLE IX
AUTHENTICATION RESULTS WITH DATASET B AND MACHINE LEARNING CLASSIFIERS

		With Gabor Filtering		Without Gabor Filtering	
	Classifier	Acc	Standard Deviation	Acc	Standard Deviation
DCT	SVC (Linear Kernel)	0.99	0.01	0.89	0.03
	SVC (Polynomial Kernel)	0.68	0.03	0.32	0.04
	Decision Tree	0.95	0.02	0.90	0.03
	k-Nearest Neighbour	0.97	0.02	0.89	0.05
	Random Forest	0.97	0.02	0.88	0.02
PCA	SVC (Linear Kernel)	0.99	0.01	1.00	0.03
	SVC (Polynomial Kernel)	0.85	0.03	0.75	0.06
	Decision Tree	0.98	0.02	0.99	0.02
	k-Nearest Neighbour	0.97	0.02	0.98	0.05
	Random Forest	0.94	0.02	0.98	0.02

classifiers utilizing dataset B are shown in Table IX.

The displayed results support the efficacy of this algorithm when applied to the considered PUF system, as they are satisfactory for most of the combinations considered.

All the accuracy results obtained from the DCT based algorithms without Gabor filtering increased with dataset B in comparison to dataset A. This could be due to the fact that the cropping and warping process was optimized. The speckle patterns are better aligned with each other and that could lead to superior comparison results. In this scenario, however, not all accuracy results improved. In fact, the SVC with a polynomial kernel and Gabor filtering performed worse with dataset B than with dataset A. Here, the fact that overfitting is likely happening should be reiterated. With much less variability in the training data, the decision boundary is likely excessively adapted to the training data.

In dataset B, the PCA based algorithm performs equally well. All accuracy results are similarly high. There is a slight decrease in performance with the SVC when utilizing a polynomial kernel. This is likely due to overfitting being exacerbated, as discussed earlier. Again, these accuracy results would likely decrease if the dataset contained images from more tokens.

E. Discussion of the Results

Taking into consideration the obtained results for each approach, it can be argued that some of the algorithms work best in certain application scenarios, while others work best in other application scenarios. Considering the PUF system used, there are two main application scenarios to be considered:

- A system with an integrated camera and computer, where registration and authentication time are not the main concern. The main objective is to provide very accurate authentication results. This could happen in the context of, for example, authenticating important documents or utilizing a PUF to gain entry into a highly secure system.
- A system where the camera and computer are not inherently part of it. In this scenario, computational time of the implemented algorithm is considerably more important. This could happen in the context of, for example, acquiring a speckle pattern image, with a smartphone, to authenticate a piece of equipment that is tagged with a PUF.

The DCT based approach showed good authentication performance when paired with a normalized hamming distance based classification. A clear distinction between intra-HDs and inter-HDs was achieved. Because this approach is entirely data independent, only one speckle pattern image from a certain token is necessary to register it in the system. This makes it more versatile in terms of possible application environments. Regarding the considered application scenarios, scenario B or other similar scenarios would benefit more from this approach.

The PCA based algorithm paired with a normalized hamming distance based classification showed worse authentication performance. However, when combined with machine learning classifiers, the PCA based approach showed remarkably good performance. The previously considered DCT based approach is data independent, and conversely this approach is data dependent. This means that it requires a certain amount of speckle pattern images to register a new token in the system. In fact, during testing, 80% of the datasets was used for

training of the algorithm. This means 80 images per token for training (or registering a token), leaving the 20 remaining images for testing. Another point that should be discussed is that every time a new token is registered in the system, a new PCA matrix and a new classifier model need to be computed. Ideally, this is only necessary until a descriptive enough eigenspace from the PCA matrix is obtained, i.e.,when the information gathered from the registered tokens becomes sufficient to represent also previously unseen tokens. However, this can be a computationally intensive task, representing a drawback if having to be repeated every time a new token is registered in the system.

From these characteristics, which include higher authentication performance but an increased need for computational resources and data, it can be concluded that the PCA with machine learning classifiers approach would be best suited for scenario A, where registration and authentication time are not the main concern and the main objective is to provide very accurate authentication results.

VI. Conclusions and Future Work

A. Conclusions

In this work, it was demonstrated how a PUF system, utilizing low cost tracing paper tokens, can be utilized for authentication purposes, despite intra-variability between acquired speckle pattern images. Obtained speckle patterns from the same token can vary depending on acquisition environment and system alignment. Multiple algorithms were tested, following a modular approach, to assess what works best for this specific PUF system and it's application scenarios. This implementation consisted in: (i) Image acquisition; (ii) Pre-processing for normalization and filtering; (iii) Feature extraction and hash computation; (iv) Classification.

For an entirely data independent approach, the DCT with an hamming distance based classification showed the best results. It is to note that if the PCA based algorithm employed a more adequate quantization scheme, perhaps the results obtained would be matched. This data independent approach has the main benefit of not needing a large amount of data to register a certain token in the system. The PCA with machine learning classifiers showed the best authentication performance out of all the tested algorithms. This is a data dependent approach. The only downside to this approach is that multiple images of a certain PUF token are required to register it in the system and that each time a new token is registered, the PCA matrix needs to be re-generated.

B. Future Work

During this work, only the DCT and PCA were employed for feature extraction. It is recognized that many more algorithms are capable of performing image-based hash extraction. It would be beneficial to implement and test other algorithms to improve the robustness of the PUF system and more accurately assess what works best.

Although an hamming distance based classification approach was considered, Error Correction Code algorithms were not employed. They are widely used for this type of problems, as well as in the cryptographic and communication areas in general, to enhance the performance of authentication algorithms by decreasing the error obtained from intra-variability. This would make them a compelling tool to test an implement along side the algorithms proposed in this dissertation.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, 2002, ISSN: 00368075. DOI: 10.1126/science.1074376.

[2] A. Sharma, L. Subramanian, and E. Brewer, "PaperSpeckle: Microscopic fingerprinting of paper," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2011. DOI: 10.1145/2046707.2046721.

[3] L. Du, A. T. Ho, and R. Cong, "Perceptual hashing for image authentication: A survey," *Signal Processing: Image Communication*, vol. 81, 2020, ISSN: 09235965. DOI: 10.1016/j.image.2019.115713.

[4] J. P. Jones and L. A. Palmer, "An evaluation of the two-dimensional Gabor filter model of simple receptive fields in cat striate cortex," *Journal of Neurophysiology*, vol. 58, no. 6, 1987, ISSN: 00223077. DOI: 10.1152/jn.1987.58.6.1233.

[5] C. Mesaritakis, M. Akriotou, A. Kapsalis, *et al.*, "Physical Unclonable Function based on a Multi-Mode Optical Waveguide," *Scientific Reports*, vol. 8, no. 1, 2018, ISSN: 20452322. DOI: 10.1038/s41598-018-28008-6.

[6] U. Rührmair, C. Hilgers, and S. Urban, "Optical PUFs Reloaded," *IACR Cryptology*, 2013.

[7] C. Wei-Lun, "Machine learning tutorial," *Aec-Apc*, 2011, ISSN: 1471-2105.

[8] S. L. Brunton and J. N. Kutz, *Data-Driven Science and Engineering*. 2019. DOI: 10.1017/9781108380690.

[9] Tiago Filipe Santos Silvério, "Photonic Implementation of Physically Unclonable Functions," Ph.D. dissertation, Universidade de Aveiro, 2021.

[10] B. Coşkun and B. Sankur, "Video İşaretlerinin Algisal Dayanikli Kiyimi," in *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, SIU 2004*, 2004.

[11] R. Fitas, B. Rocha, V. Costa, and A. Sousa, "Design and comparison of image hashing methods: A case study on cork stopper unique identification," *Journal of Imaging*, vol. 7, no. 3, 2021, ISSN: 2313433X. DOI: 10.3390/jimaging7030048.

[12] C. Zauner, "Implementation and benchmarking of perceptual image hash functions," *Master's thesis, Upper Austria University of Applied ...*, 2010.

[13] G. M. Zafaruddin and H. S. Fadewar, "Face recognition using eigenfaces," in *Advances in Intelligent Systems and Computing*, vol. 810, 2018. DOI: 10.1007/978-981-13-1513-8{_}87.

[14] J. F. Ramalho, L. C. António, S. F. Correia, *et al.*, "Luminescent QR codes for smart labelling and sensing," *Optics and Laser Technology*, vol. 101, 2018, ISSN: 00303992. DOI: 10.1016/j.optlastec.2017.11.023.

[15] P. C. Yuen, D. Q. Dai, and G. C. Feng, "Wavelet-based PCA for human face recognition," *Proceedings of the IEEE Southwest Symposium on Image Analysis and Interpretation*, 1998. DOI: 10.1109/iai.1998.666889.

[16] M. B. Ramalho, P. L. Correia, and L. D. Soares, "Hand-based multimodal identification system with secure biometric template storage," *IET Computer Vision*, vol. 6, no. 3, 2012, ISSN: 17519632. DOI: 10.1049/iet-cvi.2011.0095.

[17] P. Moreno, A. Bernardino, and J. Santos-Victor, "Gabor parameter selection for local feature detection," in *Lecture Notes in Computer Science*, vol. 3522, 2005. DOI: 10.1007/11492429{_}2.

[18] S. Ozturk, U. Ozkaya, B. Akdemir, and L. Seyfi, "Convolution kernel size effect on convolutional neural network in histopathological image processing applications," in *2018 International Symposium on Fundamentals of Electrical Engineering, ISFEE 2018*, 2018. DOI: 10.1109/ISFEE.2018.8742484.

[19] X. Ying, "An Overview of Overfitting and its Solutions," in *Journal of Physics: Conference Series*, vol. 1168, 2019. DOI: 10.1088/1742-6596/1168/2/022022.

[20] D. Berrar, "Cross-validation," in *Encyclopedia of Bioinformatics and Computational Biology: ABC of Bioinformatics*, vol. 1-3, 2018. DOI: 10.1016/B978-0-12-809633-8.20349-X.