Uniquemark: A Computer Vision System for Hallmarks Authentication

Ricardo Barata[1]
rbarata@isr.uc.pt
Leandro Cruz[1]
lmvcruz@isr.uc.pt
Bruno Patrão[1]
bpatrao@isr.uc.pt
Nuno Gonçalves[12]
nunogon@deec.uc.pt

[1] Institute of Systems and Robotics,
University of Coimbra
Coimbra, Portugal

[2] Portuguese Mint and
Official Printing Office
Lisboa, Portugal

Abstract

We are presenting Uniquemark[1], a vision system for authentication based on random marks, particularly hallmarks. Hallmarks are worldwide used to authenticate and attest the legal fineness of precious metal artefacts. Usually, these artefacts are marked with a punch, which embeds on the surface of the metal an illustration (Fig. fig:arq b) and c). In addition to the illustration, we propose the deposition of randomly scattered micro-diamonds ($\approx 50\mu m$)on the metal surface in order to create a unique random pattern. Diamond particles patterns are randomly produced, and the probability of two equal patterns coexist is null. By detecting patterns on a precious metal piece, we can authenticate it. Our authentication method is based on a multiclass classifier model that uses mark descriptor composed by several geometric features of the particles. The proposed authentication system has met better results in both real examples and simulations.

1 Introduction

In this work, we use marks made from scattered particles over a metallic support surface to create random patterns. The main assumption of our authentication proposal is: the probability of the particles spreading process to generate two identical marks is zero. Most pattern recognition systems describe data through image-based features [1, 3]. The most important contribution of this work is the usage of geometric features to depict a unique random scattering of particles, shaping an authentication system. Such mark creation is meant to be integrated to a large-scale production environment like Assay Offices. Marks are randomly produced by scattering diamond particles over the metal surface before the official hallmark application. This procedure of mark production turns its counterfeit nearly impossible.

2 Methodology

Authentication is performed in two steps: registration and identification. The first involves mark description and subsequent training of the classifier. The second also involves the description of a given mark, followed by the search for the most similar mark previously registered and the verification whether it is a true match. Both processes start by acquiring images of marks (Section 2.1). Afterwards, it is performed the mark detection (Section 2.1): (i) region of interest detection and (ii) its rectification and crop. Over the region of interest, the segmentation is applied to identify the particles, then it is defined a respective key point for each of them (Section 2.2). The mark description (Section 2.3) consists of the creation of a vector that characterizes key points scattering. In Section 2.4, it is presented our mark registration method and the identification approach.

2.1 Mark Detection

Once acquired the hallmark image, we crop the respective image tight to the mark edges (Fig. 1 b)). It follows that such step requires the mark to be detected. In this way, mark detection is performed by a U-Net Convolutional Neural Network (CNN) [4] which defines whether a pixel belongs to the mark or not. The network is trained with a set of 132 coloured images and its handcrafted label masks by means of Stochastic Gradient Descent with Momentum method to update the weights, over 150 epochs. Although the images are acquired using a high-resolution device, they are downsampled to 256×256.

2.2 Particle Detection

Particle detection process determines a key point for each particle in the mark. It consists of a binary classification process, carried out by employing a U-net neural network [4], that defines whether each pixel of the rectified image belongs to a particle or not (Fig. 1 c). As a result, the network output experiences a series of erosion operations until the segmentation mask becames noise and big particle agglomerates free. For each connected component on the mask, we associate a key point to its centre of mass.

2.3 Description

The descriptor indicates a global representation of a geometric feature distribution of the scattered key points. Likewise, it is scale and rotation invariant. It therefore follows that the mark description is based on a histogram of distances between each pair of key points (Fig. 1 c)).

It should be borne in mind that our descriptor is a histogram that contains 142 bins. In this way, we assume that the key points are in a normalized square whose length of each side is 100. Hence, we assess the distance between all key point pairs and approximate the value to the closest integer (the bin index).

It is also important to highlight that this is a global descriptor whose dimension (142×1 vector) does not depend on the input size (amount of key points) so that we can compare different size marks. For instance, if during the detection step some particles are not identified, we are still able to compare this description with the registered one.

2.4 Registration and identification

The registration step (Fig. 1 f)) give rise to the creation of the authentication model using the representation provided by the descriptor, introduced in previous section. The authentication is treated here as a multiclass classification problem [2]. For this reason, each mark is acquired from different poses and lighting conditions, what generates a set of samples that define a class.

With respect to the identification process, it is performed by means of a Nearest Neighbour method. Besides, to speed up the search process, we use a kd-tree [5] for the nearest neighbour search. Additionally, in this process (Fig. 1 (e)) the feature vector of the mark under test is provided to the kd-tree which returns the closest mark registered in the database. Thus, if the distance between the mark descriptor under test and the registered mark is lower than a certain threshold, hallmark authenticity is confirmed.

3 Results and Discussion

3.1 Simulations

Simulations on synthetic data and tests on real databases were applied to assess our authentication process performance. It was conducted tests which targeted several pattern databases, each of them showing different features.

Table 1 exhibit three different simulation batches performed to validate the identification process (Section 3.1). We decided to apply accuracy as the metric to compare results. We also performed tests in real marks to validate the authentication system as a whole (Section 3.2).

Simulations on synthetic databases include patterns with different key points and artificial noise quantities. Doing so, allows simulating flaws

[1] Patent Application: INPI 20181000043541

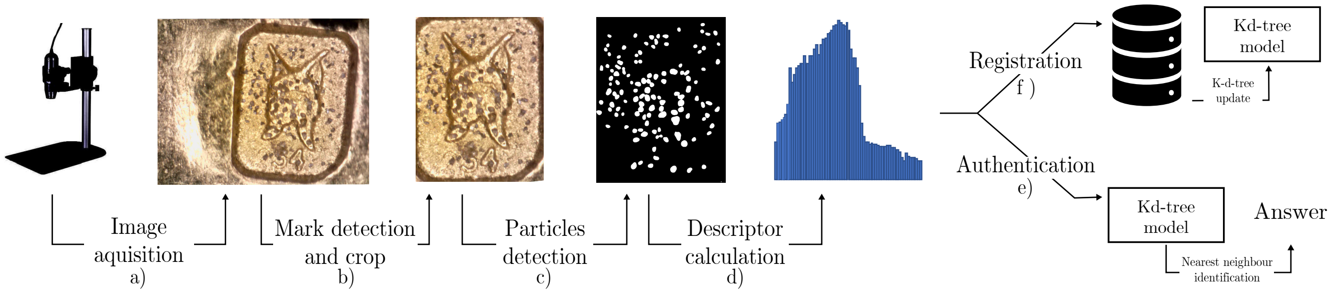

Figure 1: Brief registration and authentication system scheme.

occurred during the particle detection and aging that creates small alterations on marks. Each synthetic pattern was created by randomly scattering a predetermined number of key points on a 100 × 100 grid cells. Secondly, we added noisy transformations, i.e., the removal, addition and translation of key points to a neighbour cell. The number of removed, added or even translated key points was defined as a percentage of their initial quantity.

For each pattern, we created 14 variations containing different noisy transformations. Among these, 11 were used to train the Kd-tree, and the other three ones were used to validate its performance.

The first simulation was performed for the propose of noise effect assessment (1st batch in Table 1). Consequently, we generated four databases containing 10.000 patterns (and we used a total of 30.000 samples for testing). We also applied different amounts of noise to the databases that had patterns composed by 100 particles. The second simulation (2nd batch) analysed the effect of the number of particles. Finally, the third simulation (3rd batch) evaluated the scalability of our classification model. In this case, each database contained 100.000 patterns.

Table 1: Simulation results.

Number of patterns	Number of key points	Addition, removal and translation noise (%)	Model accuracy (%)
10.000	100	5	100.00
10.000	100	10	99.42
10.000	100	15	95.59
10.000	100	20	84.58
10.000	10	15	99.99
10.000	20	15	98.98
10.000	30	15	99.69
10.000	40	15	98.55
10.000	50	15	98.85
100.000	100	5	100.00
100.000	100	10	99.02
100.000	100	15	92.69
100.000	100	20	74.83

Regarding Table 1, it goes without saying that since the noise increases, accuracy drops. At this point, it should be emphasized that even though the introduced noise is 15%, our model is still able to successfully identify 28.677 of the 30.000 test samples (95.59%).

Furthermore, on the second simulation batch, we kept the amount of noise at 15%, and results call for a reduction of key points number on patterns does not affect method performance.

Regarding the simulations that tested the model capacity to scale towards larger databases, there was no difference between the 10.000 and 100.000 tests when applying 5% of noise (addition/removal and translations). For high levels of noise (10%, 15% and 20%) the accuracy drops 0.40pp, 2.95pp and 9.75pp (percent points), from 10.000 to 100.000 patterns database.

3.2 Real Data Tests

Image acquisition device depends on the purpose. The marks were captured using a medium magnification microscope (Fig. 1 a), and a smartphone with a macro lens.

We collected images from gold and silver samples which were individually tested. From the gold sample it was registered 17 hallmarks, and from the silver sample, 33 hallmarks. From each mark were taken 9 acquisition, 6 used to build the kd-tree, and the remaining 3 were used to testing purposes. The same testing methodology was carried out for the smartphone acquisitions.

The results obtained are presented in the Table 2. As it was expected, the accuracy for the samples acquired with the microscope was higher than the one in the samples acquired with the smartphone. The superior magnification allows a better segmentation of the diamond particles which affect the results downstream. The accuracy is also higher for the marks on gold due to the metal physical features and particle detection is better archived.

Table 2: Results of the real tests

	Gold sample	Silver sample
Microscope	100%	91%
Smartphone	88%	77%

4 Conclusion

In this paper, we presented a vision system for authentication based on random patterns that may be massively produced, Uniquemark[1]. These patterns can be used to identify products, people, etc., since their randomness makes them unique. In this case, we focused on the authentication of precious metal artefacts through official hallmarks.

We have conducted tests on real data and we have taken interesting results. We also have realized that the most delicate step on our system is the detection/segmentation of particles because it highly relies on the type of mark. To sum up, we have performed simulations on synthetic data that does not depend on detection/segmentation, and we obtained high levels of accuracy, that also proves that scalability of the system in the sense of quantity of marks.

References

[1] H. Ali, M. J. E. Salami, and Wahyudi. Iris recognition system by using support vector machines. In *2008 International Conference on Computer and Communication Engineering*, May 2008.

[2] Maya R. Gupta, Samy Bengio, and Jason Weston. Training highly multiclass classifiers. *Journal of Machine Learning Research*, 2014.

[3] Maria De Marsico, Alfredo Petrosino, and Stefano Ricciardi. Iris recognition through machine learning techniques: A survey. *Pattern Recognition Letters*, 2016.

[4] O. Ronneberger, P.Fischer, and T. Brox. U-net: Convolutional networks for biomedical image segmentation. In *Medical Image Computing and Computer-Assisted Intervention (MICCAI)*, 2015.

[5] Robert F. Sproull. Refinements to nearest-neighbor searching ink-dimensional trees. *Algorithmica*, 1991.

[1] Patent Application: INPI 20181000043541