UNIVERSIDADE D
COIMBRA

António José de Carvalho Madaleno

Autenticidade de Objetos de Metais Preciosos com Marcações a Laser usando Deep Learning

VOLUME 1

Dissertação realizada no âmbito do Mestrado Integrado em Engenharia Eletrotécnica e de Computadores, ramo de Computadores, sob a orientação do Sr. Professor Doutor Nuno Miguel da Silva Gonçalves, apresentado ao Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Fevereiro de 2022

UNIVERSIDADE D
COIMBRA

António José de Carvalho Madaleno

Autenticidade de Objetos de Metais Preciosos com Marcações a Laser usando Deep Learning

Dissertação realizada no âmbito do Mestrado Integrado em Engenharia Eletrotécnica e de Computadores, ramo de Computadores, sob a orientação do Sr. Professor Doutor Nuno Miguel Mendonça da Silva Gonçalves, apresentado ao Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Ciências e Tecnologias da Universidade de Coimbra

Júri:
Sr. Professor Doutor Jorge Manuel Moreira de Campos Pereira Batista
Sr. Professor Doutor Fernando Manuel dos Santos Perdigão
Sr. Professor Doutor Nuno Miguel Mendonça da Silva Gonçalves

Coimbra, 2022

Este projeto foi desenvolvido em colaboração com:

Universidade de Coimbra

UNIVERSIDADE D
COIMBRA

Instituto de Sistemas e Robótica

INSTITUTE OF SYSTEMS AND ROBOTICS
UNIVERSITY OF COIMBRA

Imprensa Nacional-Casa da Moeda

INCM

VIS Team

vis team
isr-uc

Agradecimentos

Primeiramente, um obrigado especial e sincero ao meu orientador, professor Nuno Gonçalves, pelo seu dedicado acompanhamento nesta etapa tão importante, aconselhando-me sempre da melhor maneira possível com um enorme apoio e exigência que foi essencial para a conclusão da dissertação. Também, um enorme agradecimento aos membros da VIS Team, que mostraram a total disponibilidade para despenderem do seu tempo de trabalho para ajudar, quando necessário. Em especial, numa fase inicial, um agradecimento ao Andoni Santos e, numa segunda fase, ao Iurii Medvedev por toda disponibilidade mostrada para me auxiliar na conceção da parte prática e experimental deste trabalho. Um enorme agradecimento à comunidade do DEEC, colegas, professores e funcionários que de alguma maneira se cruzaram com o meu percurso e que contribuíram para que esta caminhada finalizasse da maneira desejada.

Aos meus companheiros nas lutas associativistas, um obrigado por todas as vivências e aprendizagens que me foram proporcionadas, que me desenvolveram tanto a nível pessoal, como a nível profissional. Um agradecimento especial aos colegas e amigos das Direções Gerais da Associação Académica de Coimbra 2018 e 2019. À Secção de Andebol da Associação Académica de Coimbra, um amor antigo de mais de uma década enquanto atleta. O desporto é e sempre será uma escola de vida e, neste caso, foi um dos principais pilares para o desenvolvimento do meu caráter lutador e resiliente, onde aprendi que, muitas vezes, é necessário sacrificar-nos pelos outros para poder vencer na vida. A todos os meus amigos e companheiros de inúmeras batalhas, um enorme obrigado. Foi, é e sempre será um prazer incalculável representar a Académica Andebol.

Ao meu grupo de amigos, minha segunda família construída ao longo do meu percurso universitário, um obrigado é pouco, sei que serão amizades para a vida. Sem dúvida, a maior razão para estes anos terem valido a pena. À minha namorada, por todo o suporte, motivação e confiança que me transmitiu, nesta fase final, para alcançar todos os meus objetivos. Sem esquecer todos os meus amigos de longa data que permaneceram presentes mesmo com diferentes percursos de vida.

Ao mais importante, à minha família, pela oportunidade que me deram de poder estudar e seguir os meus sonhos, nunca me faltando nada, muito menos apoio, motivação e compreensão, tanto nos bons como nos maus momentos. Sou eternamente grato. Dedico todo este meu percurso ao meu tio, António Pinto dos Santos, um segundo pai, que não acompanhou esta caminhada de perto, mas esteja onde estiver, sei que está orgulhoso.

António Madaleno

Abstract

This master dissertation was created as part of a project developed between the Institute of Systems and Robotics (ISR) of the University of Coimbra and the Portuguese Mint and Official Printing Office, called UniqueMark. This project has created a system that identifies precious metal artefacts with small unique markings that cannot be cloned and are irreproducible. The identification of the laser markings is accomplished by building a system that authenticates these precious objects with only the use of a smartphone to capture the images. Two distinct markings have been developed: markings made with a punching method by scattering diamond particles on the object and markings that are deterministic laser-marked drawings on the artefact, based on a mathematical function. In this dissertation, only the laser markings will be considered to verify the effectiveness of this mark in a pattern verification system. It is essential to highlight that this is the first study carried out using the laser markings of the UniqueMark project. The novelty of the laser markings led to the development of a first image bank, which includes several conditions in the acquisition of images, from images obtained with a microscope to images captured with different models of smartphones, as well as images with variations in the type of metal used and with variations in brightness. Artificial neural networks are the approach used to create classification models. The deeper layers of the neural networks are the layers that act as extractors of sets of features from the images. The image classification process is carried out using a 1-to-1 verification system. This dissertation aims to verify the behaviour of a neural network-based classification system when images of the markings undergo variations, both at the time of training and in the testing process. These variations are present in the datasets created, and the manipulation of the image acquisition constraints is performed based on these same variations present in the image banks built.

Thus, this work is intended to find particularities that can hinder or improve the performance of the classifier models and verify in which conditions where there is a probability of the image verification system having gaps in its classification process. It is also taken into consideration the influence of images conditions variations in the training process of the classification models.

Keywords: Assay Markings; Physical Unclonable Functions; Authentication Systems; Deep Learning; Anti-counterfeiting.

Resumo

Esta dissertação é realizada no âmbito de um projeto que resultou de uma parceria entre a Universidade de Coimbra e a Imprensa Nacional-Casa da Moeda, designado por *UniqueMark*. Este visa a criação de um sistema que identifica artefactos de metais preciosos com pequenas marcações únicas, não clonáveis e irreproduzíveis e a sua identificação é realizada com a construção de um sistema que, com apenas a utilização de um telemóvel para a captura das imagens, autentifica estes objetos preciosos. Foram desenvolvidos dois tipos de marcações distintas: marcações realizadas com um método de punção através da dispersão de partículas de diamante no objeto e marcações que são desenhos determinísticos marcados a *laser* no artefacto, com base numa função matemática. Nesta dissertação apenas serão consideradas as marcas a *laser*, com o objetivo de verificar a eficácia da utilização deste tipo marcações num sistema de verificação de padrões, sendo importante realçar o facto de ser o primeiro estudo realizado utilizando as marcações a *laser* do projeto *UniqueMark*. A novidade das marcações a *laser* levou ao desenvolvimento de um primeiro banco de imagens, que inclui diversas condicionantes na aquisição das imagens, desde imagens obtidas com microscópio a imagens capturadas com diferentes modelos de telemóvel, bem como imagens com variações do tipo de metal utilizado e com variações de luminosidade. A utilização de redes neuronais artificiais é a abordagem utilizada para a criação dos modelos de classificação, em que as camadas mais profundas das redes neuronais funcionam como extratores de conjuntos de características das imagens. O processo de classificação das imagens é realizada utilizando um sistema de verificação 1 para 1. O foco desta dissertação visa verificar o comportamento de um sistema de classificação baseado em redes neuronais quando as imagens das marcações sofrem variações, tanto no momento de treino como no processo de teste. Esta variações referidas estão presentes nos conjuntos de imagens criados e a manipulação das condicionantes de aquisição de imagens é realizada com base nessas mesmas variações presentes nos bancos de imagens construídos.

Assim sendo, com este trabalho é pretendido encontrar particularidades que possam prejudicar ou melhorar a performance dos modelos classificadores e verificar quais as condições onde existe a probabilidade de o sistema de verificação de imagens possuir lacunas no seu processo de classificação, tendo atenção, também, à influência das variações de condições das imagens no processo de treino dos modelos de classificação.

Palavras-Chave: Marcações de Contrastaria; Funções Físicas Não-Clonáveis; Sistemas de Autenticação; Aprendizagem Profunda; Anti-contrafação.

Lista de Figuras

Lista de Tabelas

Lista de Acrónimos

UC Universidade de Coimbra

ISR Instituto de Sistemas e Robótica

INCM Imprensa Nacional-Casa da Moeda

SIFT *Scale-Invariant Feature Transform*

ORB *Oriented FAST and Rotated BRIEF*

SURF *Speeded-Up Robust Features*

FAST *Features From Accelerated Segment Test*

BRIEF *Binary Robust Independent Elementary Features*

SVM *Support Vector Machine*

KNN *K-Nearest Neighbours*

CNN *Convolutional Neural Networks*

GAN *Generative Adversarial Networks*

PUF *Physical Unclonable Functions*

CRP *Challenge-Response Pair*

FIBAR *Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts*

RANSAC *Random Sample Consensus*

TP *True Positive*

TN *True Negative*

FP *False Positive*

FN *False Negative*

ROC *Receiver Operating Characteristics*

TPR *True Positive Rate*

FPR *False Positive Rate*

AUC *Area Under the Curve*

FMR *False Match Rate*

FNMR *False Non-Match Rate*

EER *Equal Error Rate*

DET *Detection Error Tradeoff*

SGD *Stochastic Gradient Descent*

Conteúdo

Capítulo 1

Introdução

1.1 Contextualização

Historicamente, as jóias e metais preciosos sempre mobilizaram uma enorme atenção por parte da Humanidade, devido ao seu elevado valor, tanto a nível de poder pessoal, como em reserva de valor. A sua elevada valorização levou a que a criminalidade aumentasse, nomeadamente na produção e fabrico ilegal destes metais preciosos, que exponencia o poder do seu mercado paralelo. Este problema, denominado de contrafação, tem um impacto económico muito negativo. Devido a estes dados, durante centenas de anos desenvolveram-se diversos métodos de comprovação de autenticidade dos materiais, que variam consoante a lei de cada país. No caso de Portugal, a Unidade de Contrastaria Portuguesa, que faz parte da Imprensa Nacional-Casa da Moeda (INCM), emerge com a função de garantir a segurança no setor da ourivesaria e iniciou a sua atividade de certificação de metais preciosos há mais de 100 anos. Antes de qualquer objeto chegar às superfícies comerciais, este sofre dois processos distintos de certificação: o primeiro refere-se à sua marca oficial, relativo ao material desse objeto (como por exemplo, prata ou ouro); a segunda marcação identifica o local onde o objeto foi produzido [33]. Com o desenvolvimento tecnológico, a capacidade de falsificação aumentou e a utilização das marcações convencionais deixou de ser uma solução viável. A solução viável pode centrar-se na introdução de um identificador único e impossível de clonar no material.

Esta temática, aplicada a muitos domínios científicos, tornou-se recorrente no seio da comunidade científica, existindo um desenvolvimento de sistemas de segurança eficazes, nomeadamente, para autenticar produtos e reconhecer marcações nos produtos, com o intuito de combater a problemática da contrafação.

No âmbito da garantia da segurança de artefactos preciosos, o Instituto de Sistemas e Robótica (ISR) da Universidade de Coimbra (UC) em parceria com a Imprensa Nacional-Casa da Moeda (INCM) desenvolveu um projeto denominado por *UniqueMark* [33], que visa a construção de um sistema capaz de introduzir marcações únicas, não clonáveis e irreprodutíveis nos materiais e que estas possam ser detetadas e reconhecidas a partir da utilização de um telemóvel. As marcações

podem ser inseridas no material de duas maneiras distintas: 1) mecanismo punção no material, na qual é gerada uma dispersão aleatória de partículas de pó de diamante; 2) marcação a *laser* do material, que é determinística, ou seja, não é aleatória, e é desenhada com base numa função matemática, fazendo com que o seu padrão seja único. Na área da investigação científica, este problema é denominado por reconhecimento de padrões aleatórios, inseridos nas vastas áreas de Visão por Computador e Inteligência Artificial, na qual pode ser abordado utilizando métodos convencionais de *Machine Learning* ou métodos mais modernos, como os de *Deep Learning* [21].

1.2 Motivação

O impacto social, económico e governamental da contrafação de metais preciosos é grande e, segundo dados de 2017 na União Europeia da *Europol* [25], a contrafação na indústria de jóias e relógios representa perdas anuais de 1.9 mil milhões de euros, o que corresponde a 13.5% das receitas deste setor. Também tem implicações na empregabilidade, tendo custado o emprego a 15 mil pessoas e, acrescidamente, representa perdas de receitas de 600 milhões de euros dos governos europeus, para além das áreas industriais que dependem do setor da joalharia.

Assim, o desenvolvimento do projeto *UniqueMark* pode ajudar nesta temática e, com a criação das suas marcações únicas e irreprodutíveis, o seu desenvolvimento pode significar um avanço tecnológico e social na área em questão.

1.3 Objetivo

Dos dois tipos de marcações existentes no projeto *UniqueMark*, apenas as marcações realizadas a *laser* serão consideradas, com o intuito de perceber se estas apresentam total viabilidade para a sua potencial industrialização.

O facto de este tipo de marcações serem recentes, criou a necessidade de construir bancos de imagens, com as suas devidas caraterísticas evidenciadas, ou seja, será tido em conta o modo de aquisição de imagem, bem como as suas condicionantes de captura e as suas propriedades. A construção de um modelo de *Deep Learning* com recurso à utilização de redes neuronais é o mecanismo que será implementado para, posteriormente, ser o método responsável pelo processo de classificação das imagens pretendidas em cada teste. Todo este processo classificador é realizado com base no método de verificação 1 para 1.

Foi procurado um modelo de *Deep Learning* com bons resultados e o foco deste projeto não é otimizar esse mesmo modelo, mas estudar as diversas variantes de dados representadas nos bancos de imagens, sendo essas variantes os objetos de avaliação. Serão consideradas as variações do tipo de metal precioso, as tecnologias de aquisição de imagens e, também, as diversas condições, tanto a nível físico como a nível de luminosidade. Aos fatores enumerados, será acrescentado o comportamento do sistema de reconhecimento, no momento da introdução dessas mesmas variações, de modo a detetar possíveis lacunas e condicionantes onde as variações possam apresentar mais entraves, para além da apresentação de possíveis soluções para estes problemas.

1.4 Contribuições Científicas

Este trabalho tem as seguintes contribuições científicas e técnicas:

- Desenvolvimento de um modelo de *Deep Learning* com a capacidade de classificar corretamente as marcações realizadas a *laser*;
- Análise do efeito da utilização de marcações com desenhos determinísticos em diferentes objetos, que simulam falsificações, no modelo classificador;
- Comparação de resultados entre diferentes tipos de telemóveis com caraterísticas diversas nas câmaras fotográficas;
- Comparação de resultados entre diversos tipos de metais;
- Verificação do efeito da utilização de marcações em superfícies inclinadas no modelo classificador;
- Análise de resultados quando são apresentadas variações nas condições de aquisição das imagens e na sua luminosidade;
- Análise do efeito nos resultados da introdução de imagens no treino da rede neuronal com as caraterísticas específicas de cada teste realizado;
- Submissão de um artigo cientifico para a *International Conference in Image Processing (ICIP)*, que se encontra nos anexos desta dissertação.

1.5 Organização da Dissertação

Esta dissertação está dividida em 5 grandes capítulos. O primeiro (capítulo 1), e atual, é o capítulo introdutório, na qual o tema é enquadrado no contexto atual e são apresentado os objetivos do projeto a desenvolver. O capítulo 2 é relativo ao Estado da Arte do tema a desenvolver neste projeto. São apresentados os fundamentos de Visão por Computador e de reconhecimento de padrões e, posteriormente, é realizado um paralelismo das diversas particularidades presentes neste trabalho com outros estudos realizados nesta área. O capítulo seguinte, o capítulo 3, aborda as metodologias utilizadas para a realização do projeto, desde a criação das bases de dados, ao modelo classificador utilizado e aos protocolos de teste implementados. Os trabalhos experimentais e os seus resultados serão mostrados no capítulo seguinte (capítulo 4), bem como será realizada a discussão desses mesmos resultados. O capítulo 5 apresenta as conclusões obtidas sobre a dissertação realizada e, também, propostas a desenvolver como trabalho futuro.

Capítulo 2

Estado da Arte

2.1 Métodos de Deteção de Caraterísticas de Imagens

Ao longo dos anos, uma grande fração dos estudos realizados na área da visão computacional centrou-se na capacidade de detetar e extrair informação que caraterize as imagens com base nas suas propriedades. Nos métodos convencionais de Visão por Computador a utilização de caraterísticas das imagens para as representar tornou-se numa prática bastante comum.

A extração de informação de imagens pode incluir métodos mais simples, baseadas em pontos (*pixel-based*) [88], ou métodos mais elaborados baseado em caraterísticas das imagens (*feature-based*) [1], como por exemplo, *SIFT* [52], *ORB* [70], *SURF* [9], entre outros. Estes métodos baseados em caraterísticas procuram estabelecer similaridades entre imagens diferentes, e, assim, devem possuir caraterísticas essenciais, como a invariância ao ruído, à escala, à translação ou às rotações. As técnicas referidas anteriormente são, por norma, boas opções para problemas de verificação e reconhecimento de padrões, que se enquadra no tema desta dissertação [1].

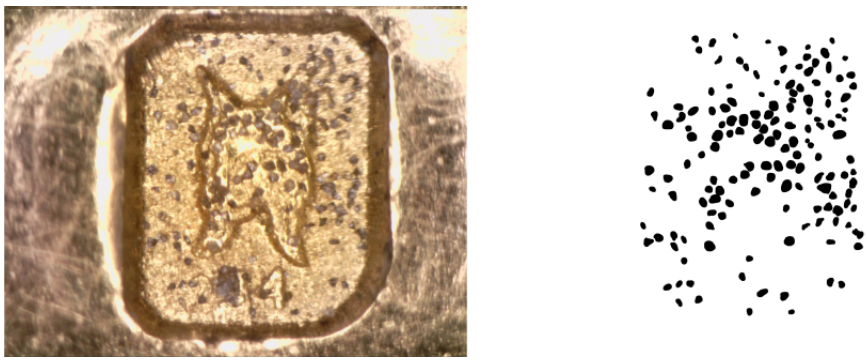

Figura 2.1: Exemplo de imagem na qual são representados os pontos-chave extraídos (retirado de [33]).

A forma de operar dos métodos referidos no parágrafo anterior centra-se pela deteção dos pontos de interesse nas imagens, em que para cada um desses pontos é calculado um descritor geométrico, matematicamente representado por um vetor, que apresenta a capacidade de distinguir

os pontos de interesse detetados entre si [82]. No que diz respeito ao método *SIFT*, os vetores descritores calculados mostram ser invariantes a diferentes tipos de transformações de imagens, tais como, translação, escala, rotação, variações de iluminação, entre outras [52]. Analogamente, foi desenvolvido o método *SURF* [9] que ao nível da performance de extração de caraterísticas nas imagens é muito semelhante ao *SIFT*, no entanto o *SURF* destaca-se pela redução da complexidade computacional e no seu tempo de execução [46]. Aumentando o leque de possibilidades, o *ORB* [70] foi criado com o intuito de ser uma alternativa viável aos métodos convencionais, como o *SIFT*, sendo que este apresenta um nível de eficácia semelhante aos anteriores, com a vantagem de alcançar tempos de execução bastante reduzidos o que fornece a capacidade de este ser utilizado em sistemas de tempo-real. O *ORB* combina o detetor de pontos-chave *FAST* [69] com o método *BRIEF* [11], utilizado para calcular os vetores descritores.

2.2 Metodologias de *Machine Learning* para classificação de imagens

A classificação de imagens é uma área que nos últimos anos foi alvo de um grande desenvolvimento e, em consequência disso, surgiram diversos algoritmos com capacidade de distinguir e classificar imagens, sendo que esta tecnologia é útil em inúmeras áreas. Os métodos convencionais usados para este tipo de classificação são uma parte do campo da inteligência artificial denominada por *Machine Learning*. Os métodos convencionais de *Machine Learning* consistem na construção de um modelo de classificação com base na utilização de caraterísticas de imagens, descritas por vetores descritores, sendo que essas caraterísticas podem ser detetadas com os métodos de Visão por Computador abordados na secção anterior. A maior limitação destes métodos convencionais é a incapacidade de extrair e utilizar diferentes tipos de caraterísticas de imagens, não diferenciando essas mesmas caraterísticas no momento do treino dos dados. Estas metodologias operam com base em modelos matemáticos que fornecem a capacidade de criar paralelismos entre as diversas caraterísticas extraídas de diferentes imagens [50].

Existem variados métodos convencionais de *Machine Learning* desenvolvidos com diversos fins e aplicações. Para a resolução de problemas de reconhecimento de padrões ou classificação de imagens a utilização de métodos como a *Support Vector Machine (SVM)* [15] ou o *K-Nearest Neighbors (KNN)* [10] é comum [74]. Ambos os métodos operam com a utilização de vetores descritores para distinguir os dados no momento da classificação e são considerados dos mecanismos mais básicos da área do *Machine Learning* [49]. A metodologia *SVM* é capaz de obter uma ótima classificação em ambientes lineares, dividindo o espaço de dados em duas classes consoante a localização dos pontos no espaço. Finalizada essa divisão, o *SVM* encontra o ponto mais próximo no hiperplano e determina a sua solução ideal dentro das restrições [8]. Por sua vez, o método *KNN* inicia com o armazenamento dos descritores das imagens de treino e a sua respetiva indexação, posteriormente, a classificação é procedida determinando os k descritores mais próximos [49], e este cálculo, geralmente, é definido através da distância euclidiana entre os objetos de treino e os objetos de teste [32]. O *SVM* apresenta vantagens no que diz respeito à eficácia na classificação, por sua vez o *KNN* é inferior no que diz respeito a essa mesma eficácia, mas apresenta simplicidade e facilidade de implementação e apresenta baixa taxa de erro no momento do treino [84].

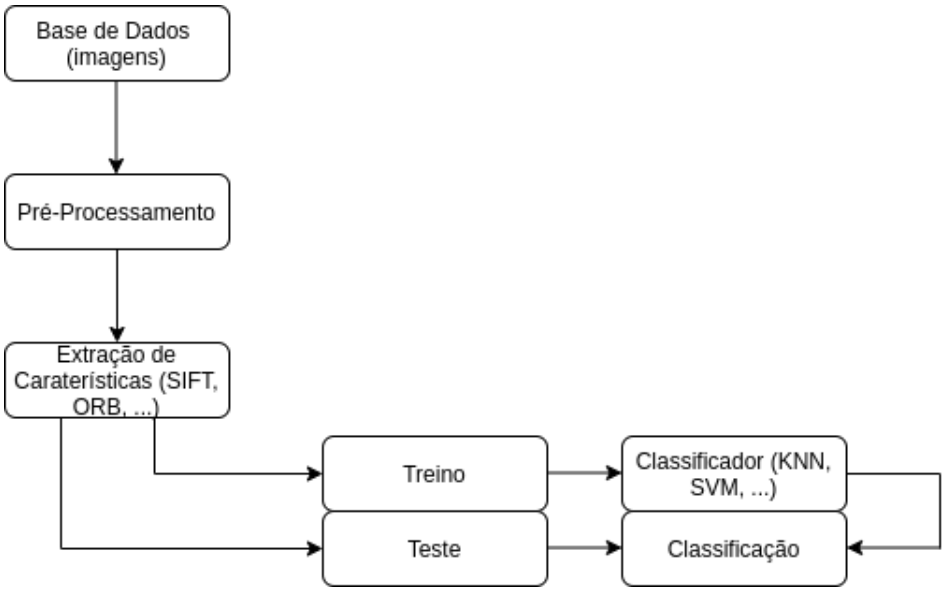

Figura 2.2: Diagrama de fluxo referente ao reconhecimento de imagens utilizando métodos convencionais de *Machine Learning*, aliados a métodos de Visão por Computador para a extração de caraterísticas de imagens (retirado e adaptado de [37]).

2.2.1 Redes Neuronais

Uma rede neuronal tem como principal base o funcionamento do cérebro humano e a conexão entre os neurónios e a forma como trocam informação [24]. Por definição, estas redes podem ser descritas por sistemas denominados por *perceptron* multicamadas que possuem diversas camadas ocultas, cujos pesos estão totalmente conectados e, normalmente, são inicializados através de técnicas de aprendizagem supervisionada e aprendizagem não supervisionada. A aprendizagem supervisionada tem o poder de caraterizar padrões, sendo que os dados de cada padrão encontram-se sempre disponíveis de forma direta ou indireta para auxiliar e supervisionar o treino. Por sua vez, a aprendizagem não supervisionada tem capacidade de classificar e reconhecer padrões sem qualquer informação sobre a correspondência de cada classe, com a captura, e posterior síntese, dos dados visíveis [21].

Uma das primeiras redes neuronais artificiais implementadas mais simples é denominada por *perceptron*, que representa um neurónio e esta pode ser descrita a partir da figura 2.3. Estes neurónios são denominados de neurónios artificiais e as suas combinações geram as redes neuronais artificiais [59].

A figura 2.3 apresenta três *inputs* (designados por x) sendo que poderia apresentar muitos mais. Neste mecanismo, foram introduzidos pesos a cada *input* que definem a sua importância para o *output*. O resultado deste *output* pode variar entre 0 e 1 e é determinado pelo somatório do produto entre o valor do *input* x_1 e o peso desse mesmo input. O cálculo deste somatório é comparado a um limiar (em inglês *threshold*), que caso seja menor que o cálculo referido na frase

anterior o *output* é zero e caso seja maior o *output* é 1 [59].

$$output = \begin{cases} 0, \ se \ \ \sum_j w_j x_j \leq threshold \\ 1, \ se \ \ \sum_j w_j x_j > threshold \end{cases} \tag{2.1}$$

Decompondo este sistema de equações, é possível escrever a expressão $\sum_j w_j x_j = x \cdot w$, em que w e x são, respetivamente, os pesos e os *inputs* da rede. Esta expressão é a soma do produto escalar entre os vetores w e x, sendo uma operação comutativa. Com a resolução e simplificação das inequações, é assumido um novo parâmetro, $bias = -threshold$ (representado graficamente na figura 2.3). Com a inclusão do *bias* é possível reescrever a expressão matemática anterior da seguinte forma [59].

$$output = \begin{cases} 0, \ se \ \ w \cdot x + bias \leq 0 \\ 1, \ se \ \ w \cdot x + bias > 0 \end{cases} \tag{2.2}$$

2.2.1.1 Funções de Ativação

De modo a simular o comportamento do sistema neuronal biológico e com base no sistema apresentado na figura anterior, é possível entender o paralelismo entre os sinais elétricos que os neurónios biológicos. Nos sistemas biológicos, os neurónios recebem sinais elétricos provenientes de outros neurónios com diferentes pesos e são estes os sinais elétricos que são simulados nas construções das redes neuronais [22].

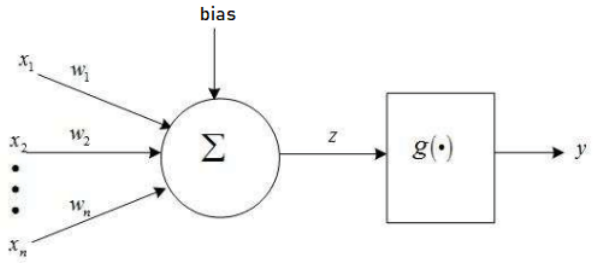

Figura 2.3: Representação de de um neurónio e dos seus *inputs*. (retirado e adaptado de [22]).

É possível verificar a utilização da função *g(.)*, que é denominada por função de ativação. Esta função apresenta o objetivo de simular o estado de resposta de um neurónio e obter o seu output *y*, obtendo a expressão $y = g(z)$. O processo de treino é dividido em duas partes: propagação direta e retropropagação. Nos algoritmos de retropropagação, as derivadas das funções de ativação devem ser calculadas em cada camada [22].

1. **Função *Sigmoid***: é dos tipos de funções de ativação mais conhecidas, em que o *output* da função é restrito ao intervalo [0,1]. Esta é uma função contínua, ou seja, é uma função derivável em toda a sua extensão. As funções *sigmoid* eram utilizadas com maior regularidade

em redes neuronais não muito profundas, isto é, com uma ou duas camadas e podem ser descritas pela seguinte expressão:

$$g(x) = \frac{1}{1 + e^{-x}} \tag{2.3}$$

As funções *sigmoid* mostram desvantagens no que diz respeito ao desvanecimento do gradiente. Este problema é encontrado nos algoritmos de retropropagação, pois a retropropagação calcula as derivadas camada a camada, da última camada para a primeira, e quando a derivada da função ultrapassa um certo valor, esta sofre de saturação, tendendo para zero. Assim, o gradiente diminui exponencialmente à medida que se recua na rede neuronal. Quando o valor do gradiente é pequeno, os pesos das camadas iniciais não serão atualizados, levando à imprecisão da rede que prejudica a performance da rede neuronal [22].

$$\lim_{x \to +-\infty} g'(x) = 0 \tag{2.4}$$

2. **Função Tangente Hiperbólica**: esta função pode ser facilmente definida como o rácio entre o seno hiperbólico e o cosseno hiperbólico, que pode ser descrito pela seguinte expressão:

$$tanh(x) = \frac{sinh(x)}{cosh(x)} = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{2.5}$$

A função de ativação tangente hiperbólica é semelhante à função *sigmoid* e estas podem ser relacionadas do seguinte modo:

$$tanh(x) = 2g_{sigmoid}(2x) - 1 \tag{2.6}$$

Esta função gera *outputs* no intervalo de $[-1,1]$ e é uma função contínua, derivável em toda a sua extensão. Estas funções hiperbólicas apresentam erros de classificação mais baixos, o que leva a que haja uma preferência pelas funções hiperbólicas, em comparação com as *sigmoid*. Como as funções hiperbólicas assemelham-se às funções *sigmoid*, estas também apresentam problemas de desvanecimento do gradiente [22].

3. **Função *ReLU (Rectified Linear Unit)***

   A função *ReLU* é popular no que diz respeito à sua utilização em algoritmos de *Deep Learning* [63]. Estas apresentam mais qualidades em relação aos exemplos de funções de ativação abordados anteriormente, devido ao facto destas serem não-saturadas, o que implica que o problema do desvanecimento do gradiente, presente nas funções *sigmoid* e nas funções hiperbólicas, seja combatido [63]. Matematicamente, podem ser escritas do seguinte modo:

$$g(x) = max(0,x) = \begin{cases} x, \ se \ x \geq 0 \\ 0, \ se \ x < 0 \end{cases} \tag{2.7}$$

   No entanto, as funções *ReLU*, na derivação $g'(x) = 0$, quando o valor de x é negativo, $x < 0$, alguns neurónios nunca são ativados, sendo uma desvantagem da utilização deste tipo de funções de ativação.

   Com o intuito de combater o problema acima referido, foram desenvolvidos vários métodos matemáticos com o objetivo de melhorar as funções *ReLU*. Um dos métodos mais reconhecidos foi o *LReLU, "leaky rectified linear units"*, que permite que no caso da saturação o gradiente não seja zero. Esta expressão pode ser escrita da seguinte maneira:

$$g(x) = max(0,x) = \begin{cases} x, \ se \ x \geq 0 \\ 0.01x, \ se \ x < 0 \end{cases} \tag{2.8}$$

   Nesta expressão o valor de 0.01 corresponde à inclinação, que é um valor arbitrário e é necessário que este seja um valor bastante pequeno [22].

2.2.2 Redes Neuronais Convolucionais

As redes neuronais convolucionais, do inglês *Convolutional Neural Networks (CNN)*, são modelos computacionais inspirados no sistema nervoso biológico e são bastantes utilizadas em problemas de reconhecimento de padrões, a partir da introdução de imagens [60]. Estas redes possuem diversas camadas com variadas operações, tendo imagens como o seu *input* e como *output* a classe das imagens introduzidas [43].

Existem diversos tipos de operações básicas para ser possível construir uma rede neuronal convolucional [3]:

- **Convolução**: aplicação de *kernels* (filtros) aos dados de entrada e sua consequente operação de convolução. Esta operação pode ser útil para detetar caraterísticas gerais de uma imagem, pois partilha os parâmetros pela rede, já que os filtros são aplicados a toda a imagem de entrada.
- ***Stride***: uma opção interessante para diminuir o número de parâmetros a serem aprendidos. Consiste na aplicação de um filtro, analisando a região dos dados de entrada, percorrendo

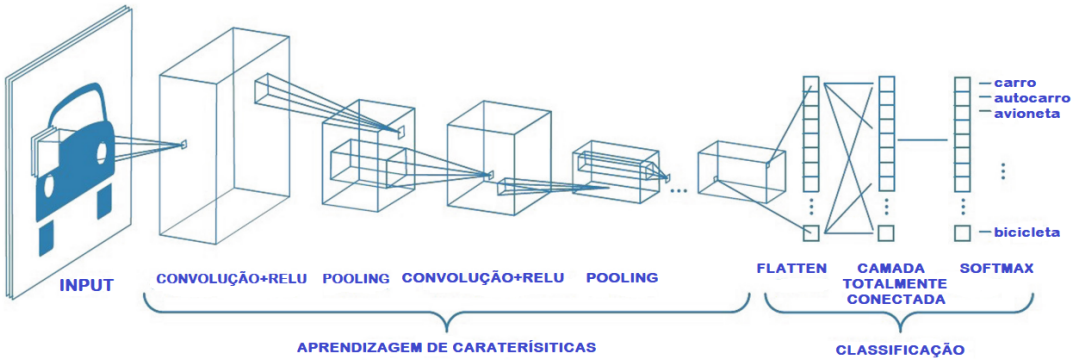

Figura 2.4: Exemplo de uma típica arquitetura de uma rede neuronal convolucional (retirado e adaptado de [43]).

toda a matriz de entrada (imagem), obtendo *outputs* de tamanho reduzido.

- ***Padding***: um dos problemas da convolução é a perda de informação nas bordas das imagens, para colmatar isso a introdução de *padding* consiste na inclusão de uma almofada de pixeis no perímetro das imagens.

Como já foi abordado, a arquitetura de uma rede neuronal convolucional divide-se em diferentes camadas, sendo que as camadas iniciais têm utilidade na aprendizagem de filtros de deteção de recursos básicos de uma imagem, como arestas, cantos, entre outros. As camadas intermediárias aprendem filtros que detetam partes de objetos, como por exemplo na área do reconhecimento facial a captação dos olhos, da boca e do nariz. As camadas finais têm como intuito o reconhecimento de objetos inteiros de diferentes formas ou posições [77]. A utilização de camadas neste tipo de redes neuronais pode ser dividida e especificada em três áreas diferentes:

- **Camada de Convolução**: como abordado nas operações básicas, esta camada aplica a operação de convolução. Ao nível de uma rede neuronal convolucional, os parâmetros a serem aprendidos são os dos *kernels* e esta camada irá determinar os neurónios conectados com uma determinada região do *input*. A camada de convolução, objetivamente, é útil em reconhecer caraterísticas aprendidas anteriormente e em aprender padrões localizados de certas partes das imagens [60].

- **Camada de *Pooling***: as camadas de *pooling* reduzem gradualmente a dimensão de regiões localizadas nos dados de entrada, e, consequentemente, o número de parâmetros a ser aprendidos é diminuído, o que reduz a complexidade computacional do modelo [60]. Existem alguns exemplos de funções *pooling*, como a operação *max-pooling* que retorna o maior valor entre vários valores de uma vizinhança retangular, ou a operação *avg-pooling* que retorna o valor médio dessa mesma vizinhança, ou uma função *pooling* que obtém na saída a sua norma L^2, ou uma operação que retorna a média ponderada baseada na distância ao pixel central [34].

- **Camada Totalmente Conectada**: esta camada conecta todos os neurónios entre duas ca-

madas adjacentes e são estas que, por norma, produzem as saídas relativas à classificação [48].

A utilização de redes neuronais convolucionais sempre mostrou grande utilidade e obteve grande sucesso na área do reconhecimento de imagens. Principalmente na última década, este tipo de redes sofreu um enorme desenvolvimento, no que diz respeito às suas arquiteturas, componentes de supervisão, mecanismos de regularização e técnicas de otimização e computação. Com esta evolução tão exponencial, o estudo do desempenho de classificação, caraterísticas e robustez computacional tem sido mais abundante, o que implica a descoberta de novos desafios e problemas para tentar combater e, consequentemente, melhorar a eficiência das redes neuronais convolucionais [67]. Por outro lado, estas redes neuronais para serem mais robustas, é necessário que possuam um grande número de parâmetros a treinar, sendo que esse fator é a causa do surgimento de problemas relacionados com a utilização deste tipo de redes, como o *overfitting* [76].

O *Overfitting* é um dos maiores problemas presentes na implementação de algoritmos de redes neuronais, tornando-se numa adversidade ainda mais evidente nas redes modernas que necessitam de um número elevado de dados para a rede treinar [59]. É uma adversidade que consiste na falta de capacidade de uma rede neuronal para aprender eficientemente os dados a treinar [60]. Um modelo apresenta *overfitting* quando este possui uma boa performance nos dados de treino, mas nos dados de validação não se comporta de forma eficiente. Este fator acontece pois o modelo memoriza os dados já analisados e é incapaz de generalizar para exemplos não vistos. A abundância ou falta de dados de treino para o modelo aprender [73] são duas possíveis razões para o *overfitting* ocorrer, que implica uma grande variação nos resultados de validação obtidos. Com o objetivo de reduzir essa variação foram desenvolvidas várias soluções como a implementação de técnicas de regularização e de *Data Augmentation* [12].

A *Data Augmentation* é bastante utilizada no reconhecimento e classificação de imagens, quando a base de dados disponibilizada não é suficiente para obter os resultados esperados, dado que esta técnica cria imagens sintéticas a partir das imagens existentes na base de dados. Este método possui diferentes abordagens possíveis e podem ser divididas em duas categorias gerais: as tradicionais transformações de imagens ou a utilização de métodos baseados em redes neuronais, como as *Generative Adversarial Networks (GAN)* [56].

As transformações de imagens em *Data Augmentation*, que combinam transformações geométricas e modificações de cor, são as transformações mais populares neste mecanismo. Estas transformações de imagens podem ser ao nível da aplicação de rotações, translações, lineares, variações de escala, entre outras. Resumidamente, para cada imagem são criadas diferentes transformações de modo a obter variados tipos das imagens. Estas variantes das imagens irão muitas vezes equilibrar os conjuntos de imagens e aumentar o número de amostras para o treino da rede neuronal [56].

As *Generative Adversarial Networks (GAN)* [35] representam uma técnica que é relativamente recente e robusta para a geração de novas imagens. É útil em problemas como: geração de imagens de baixa resolução a partir de imagens de alta resolução; conversão de esboços de imagens

em imagens, ou seja translação imagem-imagem; mistura de duas partes de imagens de modo a obter uma nova; restauro de partes perdidas da imagem; entre outras. Estas podem ser utilizadas em diversas aplicações, tais como, síntese de imagem, edição de imagem, transferência de estilo, classificação, entre outras diversas aplicações possíveis [17]. O funcionamento das *GAN* centra-se na utilização de duas redes adversárias, $G(z)$ e $D(z)$. A rede $G(z)$ (rede geradora) gera uma imagem realista de modo a enganar a outra rede. A rede $D(z)$ (rede discriminadora) irá distinguir as imagens falsas das reais. A arquitetura usada nesta técnica está esquematizada na figura 2.5 [35].

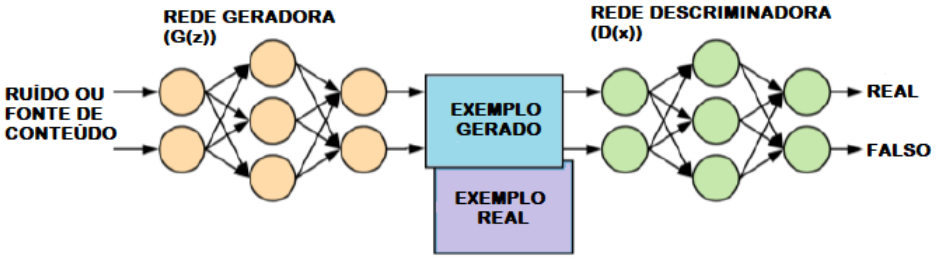

Figura 2.5: Arquitetura utilizada nas *Generative Adversarial Networks* (retirada e adaptada de [56]).

As *GAN* têm vindo a mostrar um enorme desenvolvimento em diversas áreas da tecnologia, tendo sido criadas variantes desta tecnologia. A explosão deste interesse nas *GANs* é impulsionada não apenas pelo seu potencial para aprender profundamente mapeamentos não-lineares num espaço de dados e vice-versa, mas também pelo seu potencial para fazer uso de grandes quantidades de dados de imagem não rotulados para a sua aprendizagem. As oportunidades para o desenvolvimento de novas teorias e algoritmos são bastantes, e com o poder das redes neuronais profundas existem variadas oportunidades para novas tecnologias e aplicações [17].

2.3 Sistemas de Reconhecimento e Verificação de Padrões Aleatórios

Uma solução altamente eficaz para o combate da contrafação é ”etiquetar”os produtos que requerem proteção. No entanto, algumas medidas mais simples de anti-falsificação mostram não ser as mais eficazes, apresentando lacunas que são prejudiciais à segurança dos produtos [6]. Para atenuar esta temática da contrafação, houve um desenvolvimento de sistemas tecnológicos capazes de marcar e autenticar produtos a ser comercializados. A ideia centrou-se na criação de caraterísticas geradas aleatoriamente intrínsecas ao produto para identificar eficientemente objetos. Este mecanismo tem como paralelismo as impressões digitais, que são únicas para cada pessoa e têm o poder de as identificar. Assim, a geração de padrões aleatórios para identificação de materiais tem vindo a tornar-se prática recorrente nas décadas mais recentes, acompanhado pelo desenvolvimento das funções físicas não-clonáveis [53].

2.3.1 Funções Físicas Não-Clonáveis

No início do novo milénio, Ravikanth Pappu *et al.* [62] desenvolveu a primeira formalização do conceito da geração de padrões aleatórios nos materiais, inicialmente denominado por *Physical*

One-Way Functions, que evoluiu ao longo dos anos para a atual designação de *Physical Unclonable Functions PUF*. A partir desse momento, inúmeros novos tipos de *PUF* foram desenvolvidos com uma tendência de construções mais seguras e complexas [53]. Uma *PUF* tem duas vertentes principais na sua aplicação, tanto podem ser introduzidas no momento do fabrico do material, ou podem ser intrínsecas ao material, como por exemplo as impressões digitais presentes nos humanos [29]. Um exemplo do modo de funcionamento desta metodologia de autenticação de produtos divide as *PUFs* em duas principais aplicações: 1) autenticação a baixo-custo; 2) geração de chaves de segurança. As duas aplicações referidas são descritas como "*PUF* forte", tipicamente usada para autenticação, e "*PUF* fraca"é utilizada para a geração e armazenamento de uma chave de segurança [40].

Por norma, a entrada de um sistema *PUF* é denominado por desafio (em inglês, *challenge*) e o *output* é chamado de resposta. A terminologia utilizada para estes casos é *challenge-response pair* (*CRP*), sendo que a relação entre o desafio e a resposta é medido com base no comportamento do *CRP* [53]. Uma aplicação *PUF* pode ser dividida em duas fases distintas [53]:

- Fase de Registo: um número de *CRPs* é recolhido de um *PUF* e é armazenado na base de dados.
- Fase de Verificação: utilizando a base de dados, é aplicado um desafio a uma *PUF*, a sua resposta é analisada e comparada com a resposta correspondente na base de dados.

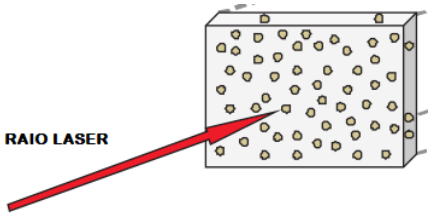

Figura 2.6: Exemplo de implementação de uma *PUF* com *laser* num material (retirado e adaptado de [71]).

Durante os últimos anos foram realizados vários estudos sobre esta área, o que desenvolveu diversos modos de aplicações das *PUFs*, tais como *PUFs* óticas, *PUFs* arbitrárias, *PUFs* intrínsecas baseadas em memória [40], *PUFs* de silício [31], entre outros.

Esta tecnologia possui diversas caraterísticas, tais como:

- Baixo custo por peça utilizada [71].
- A resposta da *PUF* é de alta complexidade, difícil de analisar [71].
- Alta segurança de modo a evitar a clonagem da PUF [71].
- Enorme dificuldade em alterar as caraterísticas físicas do modelo de uma PUF [40].
- São imprevisíveis, sendo, na teoria, impossível de prever o *output* de uma PUF [23].

Devido às caraterísticas acima enumeradas, é possível subentender a utilidade deste meca-

nismo no que diz respeito ao combate à contrafação, sendo este um processo não determinístico, que faz com que resulte uma aleatoriedade que gera um *output* muito difícil de replicar e falsificar [6].

Arppe Tabbara *et al* [7]. realizou um trabalho em 2019 com o intuito de demonstrar um exemplo de um sistema de validação e autenticação utilizando *PUFs* inseridas nos materiais, sendo que a aquisição de imagens foi realizada através de um *smartphone*. O processo de autenticação é feito pelo fabricante, registando na base de dados os dados referentes à marcação feita. Por sua vez, o segundo processo, relativo à validação, cabe ao utilizador, que a partir da aquisição de uma imagem verifica se a *PUF* do seu produto se equivale a outra *PUF* presente na base de dados.

Especificamente, o modo de registo e validação pode ser representado pela figura 2.7. No momento da realização da autenticação, a *PUF* é associada a um ID e quando o utilizador introduz a imagem adquirida, caso haja alguma correspondência entre a *PUF* da imagem do utilizador e alguma *PUF* das imagens presentes na base de dados, o sistema informa se a imagem introduzida gera uma correspondência positiva ou negativa. Esta classificação mostrou ser eficaz com a utilização de *smartphones* para reconhecer cada *PUF* como única [7].

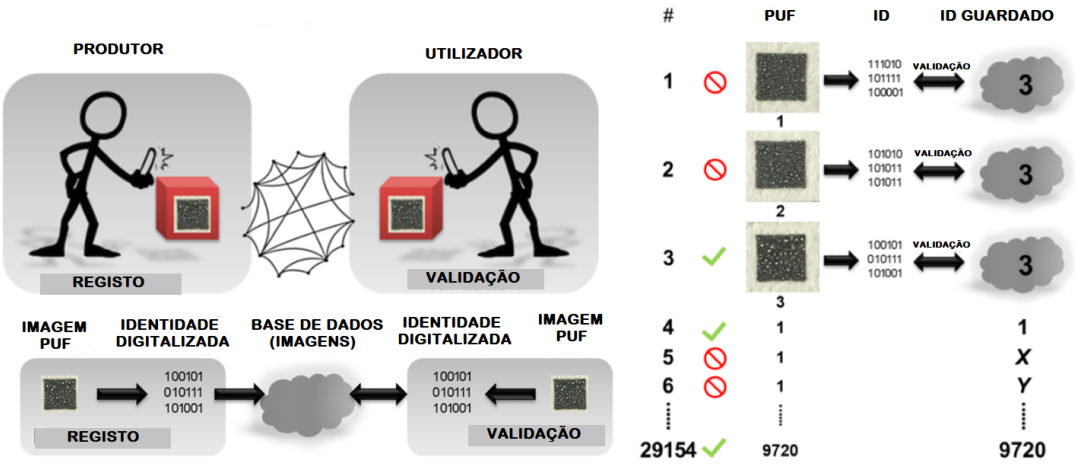

Figura 2.7: Esquemas de registo e validação de materiais, utilizando *PUFs* (retirado e adaptado de [7]).

Com o objetivo de classificar materiais metálicos utilizando as suas próprias caraterísticas, abordadas no início desta secção como *PUFs* intrínsecas, foi publicado um artigo, em 2014, por Toru Takahashi *et al.* [81] em que é proposto um método que utiliza as caraterísticas dos metais como impressões digitais intrínsecas para a sua identificação, denominado por *FIBAR, Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts*. Devido à reflexão especular, existe alguma instabilidade na captura das caraterísticas das imagens das superfícies metálicas, assim os métodos anteriores necessitavam de dispositivos de imagens especiais para proceder à captura das mesmas. O método *FIBAR*, com a utilização de uma câmara comum, possui a capacidade de capturar as caraterísticas repetíveis nas superfícies metálicas. Por exemplo, para a captura de imagens com a utilização de um telemóvel com esta técnica apenas requer um difusor, uma lente macro e um anel preto absorvedor, que é uma ferramenta de baixo custo

podendo ser desenvolvida através de impressão 3D. A imagem capturada é o padrão angular de intensidade preto/branco refletido no metal. Os processos de registo e de identificação de imagens são realizados através dos métodos convencionais de visão por computador já abordados. Esta técnica mostrou resultados positivos nos testes realizados de reconhecimento de diferentes metais com inúmeras parecenças.

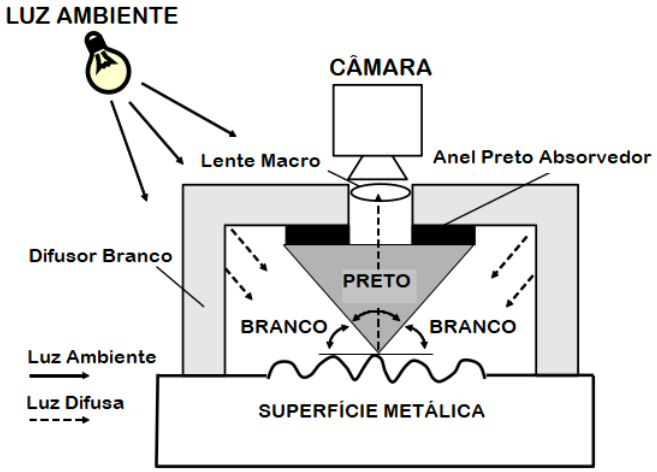

Figura 2.8: Representação esquemática do método *FIBAR* (retirado e adaptado de [81]).

Como já foi referido, as *PUFs* intrínsecas tanto podem corresponder a caraterísticas únicas nos materiais, como podem ser caraterísticas inerentes aos humanos e objetos. No caso dos humano as *PUFs* possuem a capacidade de verificar as suas identidades, na qual, normalmente, estas *PUFs* são associadas a impressões digitais, ao ADN e à face. No entanto, a utilização de outras caraterísticas humanas para a identificação de pessoas veio a tornar-se um motivo de investigação ao longo dos anos, acompanhado pelo aumento da necessidade de maiores graus de segurança presentes na sociedade. No âmbito desses estudos, Hasimah Ali *et al.* [4] produziu, em 2008, um trabalho em que são utilizadas íris do olho humano para proceder à verificação e identificação de pessoas com a finalidade de utilização em sistemas de segurança. Este processo de reconhecimento é baseado na extração de cataterísticas das imagens das íris e o modelo de classificação utilizado é a *Support Vector Machine*, que pertence aos métodos convencionais de *Machine Learning*. O sistema de verificação é repartido em dois sistemas minoritários: a fase de treino e a fase de teste. A fase de treino e a fase de teste em muito são similares nos primeiros passos, que correspondem à aquisição das imagens, localização da íris, pré-processamento da imagem e extração das suas caraterísticas. Nos passos seguintes, mais concretamente na fase de treino, o classificador é construído e, posteriormente, a fase de teste centra-se no processo de decisão, na qual o sistema decide se as cataterísticas extraídas da íris a verificar correspondem à identidade requerida, aceitando ou rejeitando essa mesma identidade. Neste trabalho, os resultados foram promissores, apresentando um bom nível de segurança. Com o desenvolvimento das redes neuronais e com o aumento da utilização de *Deep Learning* tornou-se proveitosa a sua comparação com a utilização de métodos convencionais de *Machine Learning*, como foi estudado no trabalho de Maria de Marsico *et al.* em 2016 [19]. Neste estudo foi concluído que as técnicas convencionais de *Machine Learning* não

foram suficientemente investigadas para este tipo de problemas de classificação, apesar do crescimento do número de investigações nesta área. Utilizando o exemplo do *SVM* acima referido, é possível entender que este permite o uso de variadas funções de *kernel* para evitar o mapeamento explícito dos vetores de caraterísticas num espaço dimensional superior e o objetivo desta última operação é encontrar um limite entre identidades, que poderá não ser alcançado. Assim, a evolução do *Deep Learning* veio aumentar as fronteiras com os métodos convencionais de *Machine Learning*, apresentado potencialidades para resolver os problemas acima descritos, sendo que será interessante explorar e comparar profundamente as performances entre estas duas metodologias de classificação em futuros estudos.

No mesmo âmbito dos estudos explicados anteriormente, as investigações usando caraterísticas únicas para identificar pessoas mostram várias vertentes. Nesse sentido, Chin-Chuan Han *et al.* [38] desenvolveram um trabalho na qual são utilizadas as caraterísticas de palmas das mãos para identificação de pessoas. Este processo visou extrair as caraterísticas das imagens utilizando operações de processamento de imagem, ao invés da utilização habitual dos métodos convencionais de Visão por Computador para extração de caraterísticas (como o *SIFT* ou *ORB*). De modo similar a outros trabalhos de problemas de classificação, este trabalho apresenta duas fases na sua implementação, a fase de registo e a fase de verificação. O pré-processamento é o ponto inicial deste processo e apresenta diferentes passos: 1) binarização da imagem capturada; 2) obtenção dos contornos da mão, com a utilização do algoritmo de deteção de contornos [83]; 3) localização e mapeamento dos contornos da mão; 4) geração da região de interesse onde é retirada apenas a palma da mão, com base na localização de pontos obtida anteriormente. Para a extração de caraterísticas é inicialmente utilizado o operador *Sobel* [47], e, posteriormente, foram extraídas novas caraterísticas através de diversas operações morfológicas de dilatação, erosão, entre outras, de modo a esqueletizar as imagens. Os vetores de caraterísticas são calculados dividindo a imagem em pequenas grelhas e é calculada a média dos valores dos pixeis presente em cada uma dessas grelha. O processo de criação do modelo classificador centra-se em dois passos essenciais, a aplicação de técnicas *template-matching* [51] aos vetores descritores calculados e, posteriormente, uma rede neurona é implementada com o fim de comparação com as técnicas de *template-matching* anteriormente calculadas. Neste sentido, a comparação entre os dois métodos de verificação foi um dos principais pontos desta investigação sendo que as vantagens foram notórias para a rede neuronal implementada.

Como é possível verificar pelos parágrafos anteriores a paridade entre *PUFs* e os sistemas biométricos é visível sendo que tanto pode ser aplicado o reconhecimento a materiais, a pessoas e cada vez mais portas se abrem nesta área, apresentando um grande potencial, seja para o desenvolvimento de sistemas de reconhecimento, sistemas de segurança ou sistemas de combate à contrafação.

2.3.2 *miDot*

Num trabalho de 2016, desenvolvido por Rui Ishiyama *et. al* [44], foi desenvolvido um método eficiente para identificar materiais que é denominado, do inglês, por *"micro Identifier Dot on*

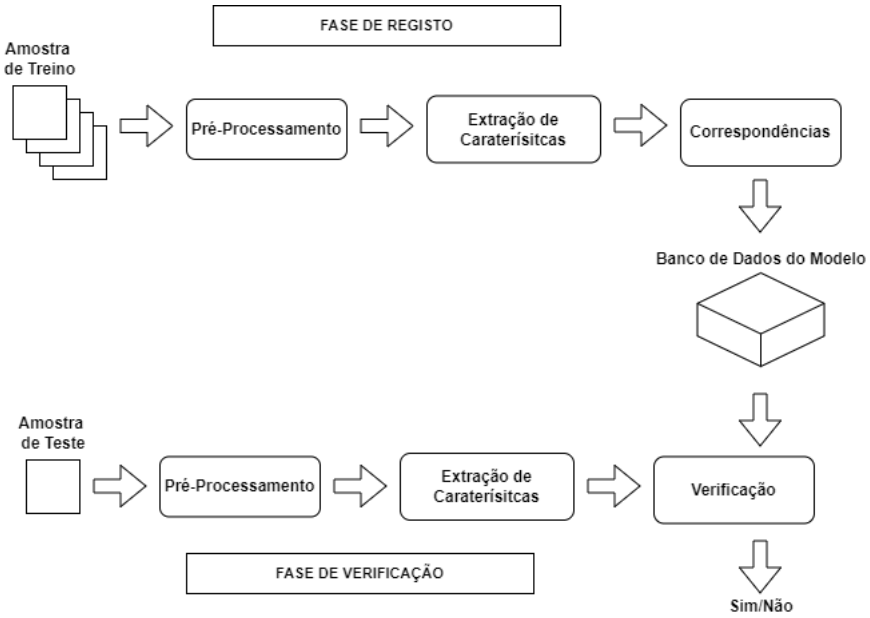

Figura 2.9: Representação processo de classificação utilizado para a classificação de palmas das mãos, que é genérico e utilizado em muitos modelos semelhantes de reconhecimento de imagens. (retirado e adaptado de [38]).

Things" ou *miDot*. Este sistema tem atenção especial aos materiais que não podem ser identificados com marcadores, códigos de barras ou códigos QR. Assim, o sistema consiste na inclusão de um ponto de tinta metálica/brilhante num objeto e esse ponto é identificado como único, sendo relacionada a sua imagem microscópica com a base de dados.

O *miDot* apresenta-se com o intuito de combater as limitações relativas aos métodos convencionais de identificação dos materiais, apresentando as seguintes vantagens:

- cada ponto apresenta caraterísticas únicas e detalhadas e o seu tamanho reduzido, com raio de 1mm, é uma vantagem pois, atualmente, em materiais elétricos como condensadores que são bastante pequenos não haveria espaço para a inclusão de identificadores convencionais.
- o custo reduzido da identificação dos materiais é uma vantagem, pois o preço apenas representa a porção de tinta utilizada por objeto.
- a facilidade e eficiência de identificação é um ponto a favor deste novo método, pois as tintas têm capacidade de aderência a diversos tipos de materiais, como metais e plásticos. De forma resumida, o ponto é aplicado no material e a captura da sua imagem é suficiente para o seu registo.

O desenvolvimento do sistema de identificação de objetos como únicos passa por três fases distintas, sendo que primeiramente ocorre a extração de caraterísticas da imagem e as suas correspondências. Posteriormente essas correspondências serão verificadas geometricamente e, por fim, é calculado o nível de correspondência obtido. Para a realização do primeiro passo pode ser utilizado o método *ORB* com base na sua capacidade de extração de caraterísticas associada ao seu baixo custo computacional. A verificação geométrica dos pares de pontos correspondentes é

executada através do algoritmo *RANSAC* [27]. Por fim, o cálculo da pontuação final é realizado através do número de correspondências corretamente identificadas na verificação geométrica dos pares de pontos, através do *RANSAC* onde é quantificada a semelhança entre a imagem introduzida pelo utilizador e a imagem presente na base de dados.

Este método tem como desvantagem principal a necessidade da utilização de material microscópico para a aquisição de imagens, o que limita a sua acessibilidade ao cidadão comum.

2.4 Sistemas de Extração de Minúcias para Reconhecimento e Verificação de Imagens

O reconhecimento e classificação de imagens tem diversas aplicações, em diferentes áreas. Um dos casos de estudo mais semelhantes ao que vai ser tratado nesta dissertação é o reconhecimento de impressões digitais, devido às suas parecenças físicas com as *PUFs*, abordadas no ponto 2.3.1.

Um sistema de reconhecimento de impressões digitais tem por base vários módulos principais de implementação: aquisição de imagem, o pré processamento das imagens, a extração de caraterísticas, a correspondência entre imagens e, por fim, a sua classificação. De modo a aumentar a precisão dos sistemas de reconhecimento é necessária a deteção e extração de minúcias, sendo que esta é a abordagem mais utilizada neste tipo de sistemas, essencialmente devido à sua interpretabilidade, alto desempenho de correspondência e capacidade de armazenamento [14].

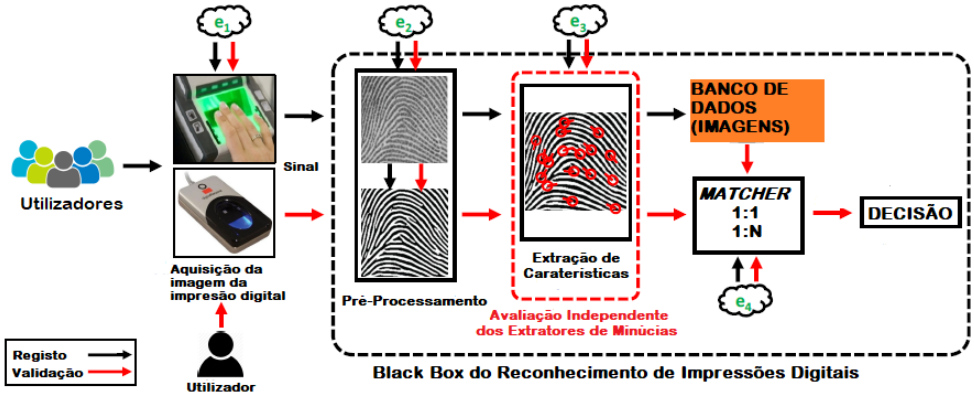

Figura 2.10: Sistema típico de reconhecimento de impressões digitais (retirada e adaptada de [14]).

Na figura 2.10 estão descritos todos os principais módulos de implementação já referidos. Em 2017, Tarang Chughet *et al.* [14] publicou um estudo em que o objetivo centrou-se na avaliação individual de cada passo da implementação, para compreender onde surgem, maioritariamente, os erros de correspondência e/ou não correspondência. É do conhecimento generalizado que os erros de reconhecimento de impressões digitais são maioritariamente localizados na extração de minúcias. Assim, é necessário perceber e encontrar soluções eficazes para a deteção e extração de minúcias.

Há vários anos que o estudo da localização de minúcias é um tema recorrente na análise de imagens de impressões digitais, como, por exemplo, mostra o trabalho de *Nalini K. Ratha et al.* de 1995 [66] ou o trabalho de *Alessandro Farina et al.* realizado em 1999 [26]. Mais recentemente foram introduzidos métodos mais robustos e completos, como em 2015 foi publicado um trabalho com a finalidade de extrair minúcias bastante fiáveis através de imagens de impressões digitais [86]. As caraterísticas locais das imagens de impressões digitais, tais como, fins de linhas, bifurcações, cruzamentos ou pequenas linhas podem ser considerados minúcias utilizados em processos de classificação. É recorrente a utilização de bifurcações e fins de linha nos sistemas de reconhecimento de impressões digitais e uma linha principal pode ser iniciada ou finalizada num ponto de junção, que corresponde ao momento em que três ou mais linhas se encontram. De modo a que as caraterísticas das impressões digitais estejam visíveis é essencial assegurar a qualidade da imagem capturada, pois a qualidade da imagem poderá ter consequências na capacidade do sistema reconhecer e extrair minúcias. Com base na aplicação de filtros, como o filtro *Gabor* ou *Log-Gabor* as caraterísticas das imagem podem ser mais evidenciadas e, posteriormente, o ruído e componentes menos relevantes são retirados das imagens, resultando uma imagem em que apenas as linhas principais são consideradas para a extração de minúcias [86], que tem uma influência positiva ao nível de carga computacional, pois reduz o número de pontos e caraterístcas a analisar [26]. Este sistema apresenta dois passos principais na sua implementação: esqueletização da imagem e localização de minúcias. No primeiro passo é retirado o fundo e, posteriormente, são aplicadas transformações na imagem de erosão e dilatação nas linhas já aprimoradas da impressão digital. Os componentes pequenos, como linhas pequenas, são removidos e os componentes que estão perto entre si sofrem uma junção. Para a localização de minúcias, cada linha da imagem é analisada e são localizados os diversos pontos de junção (quando três ou mais linhas estão conectadas). Perante um conjunto de regras relativas à distância entre linhas são detetados os pontos válidos e inválidos. Caso o fim de uma linha não seja um ponto de junção, os pixeis vizinhos são verificados com a finalidade de analisar se o ponto final da linha é uma minúcia válida [86].

Outro exemplo de aumento da robustez na deteção e extração de minúcias é o trabalho realizado por *Hartwig Fronthaler et al.* [28] em 2008, em que foram sugeridas novas técnicas comuns tanto de aprimoramento da imagem como de extração de minúcias, aplicando caraterísticas de simetria. Num primeiro momento de melhoramento da imagem é realizada uma decomposição em pirâmide com o intuito de obter pirâmides do tipo *Gaussian* e *Laplacian* que tem como objetivo a decomposição da impressão digital em sub-bandas correspondentes a diferentes escalas espaciais. A cada nível da pirâmide é realizada uma suavização da imagem e as direções de filtragem provêm dos sensores de estrutura adaptada à frequência, que coordenam de forma flexível a quantidade e a direção da suavização das caraterísticas das imagens (como as linhas das impressões digitais). No que diz respeito à localização e extração de minúcias, a simetria parabólica é acrescentada ao modelo local de impressões digitais o que permite detetar, simultaneamente, a posição e a direção de uma minúcia. Estas técnicas mostram a sua eficiência, reduzindo o nível de erro de correspondência de imagens, com a utilização de bases de dados cuja qualidade de imagem é limitada.

Os paralelismos entre os sistemas de reconhecimento de impressões digitais e os sistemas de

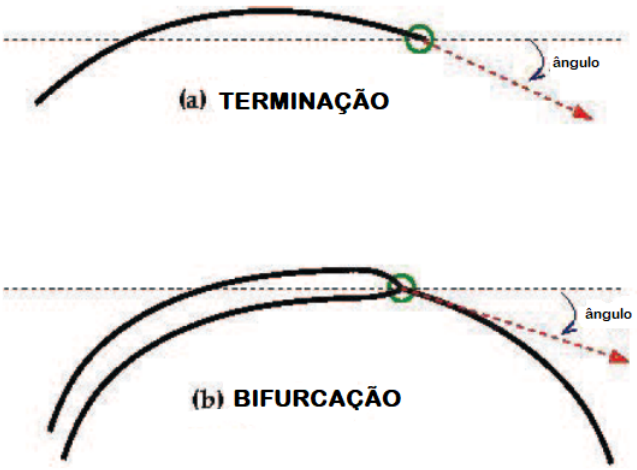

Figura 2.11: Dois exemplos de minúcias: bifurcação e terminação de linhas (retirado e adaptado de [86]).

reconhecimento de padrões são grandes. O estado da arte destes sistemas revela muita utilidade em diversas aplicações, como, em 2012, um trabalho de *Rui Ishiyama et al.* [45] utilizou minúcias recorrentemente usadas em impressões digitais para o reconhecimento de imagens de frutas e sua posterior classificação.

2.5 Evolução dos Sistemas de Reconhecimento e Verificação Biométrica

Com base no que foi abordado no decorrer deste capítulo, existe uma grande semelhança entre os sistemas de reconhecimento e verificação biométrica e o tema a tratar nesta dissertação. Um sistema biométrico pode ser definido como um sistema que usa distinções anatómicas ou caraterísticas comportamentais para reconhecer ou verificar indivíduos, onde se englobam caraterísticas tais como, impressões digitais, palma da mão, face, íris, entre outros [16]. Com o desenvolvimento das redes neuronais na área da classificação de imagens, a sua utilização em sistemas biométricos também tem vindo a desenvolver-se.

Primeiramente, torna-se importante proceder a uma comparação entre os métodos de extração de caraterísticas convencionais, anteriormente abordados, com os métodos usados de *Deep Learning*. Nesse sentido, e com base em sistemas de reconhecimento de impressões digitais, foi desenvolvido um trabalho [2], em 2021, que compara estas duas abordagens. Este trabalho pretendeu comparar diversos métodos convencionais de extração de caraterísticas, com arquiteturas já existentes, como a *Resnet50* [39] e a *VGG-19* [75], sendo que apesar dos bons resultados obtidos pela utilização dos métodos convencionais, as arquiteturas de *Deep Learning*, nomeadamente, a *Resnet* alcançou melhor precisão, principalmente, na extração de caraterísticas profundas, mostrando a sua utilidade neste tipo de sistemas.

Existem diversas aplicações e possibilidades de implementação de redes neuronais convolu-

cionais, pois os modelos tanto podem ser construídos autonomamente, como podem ser utilizadas arquiteturas já existentes e previamente treinadas. Em 2018, foi desenvolvida uma pequena rede neuronal convolucional [61], construída de raiz que mostra uma elevada eficácia no reconhecimento de impressões digitais. Apesar dos testes terem sido realizados com poucas imagens, é de realçar o potencial da utilização deste tipo de redes neuronais para construir os classificadores, com base nos bons resultados obtidos por uma rede simples e não muito profunda. Noutra vertente, para a utilização de arquiteturas já utilizadas em modelos de classificação de impressões digitais, foi desenvolvido um trabalho de comparação entre diversos modelos de *Deep Learning* [68], onde foram testadas diversas abordagens em que a *Resnet* mostrou ser melhor tanto ao nível de eficácia, como ao nível de tempo de execução computacional.

No âmbito da utilização de redes neuronais em sistemas de classificação de caraterísticas biométricas, foram também implementados algoritmos de aprendizagem por transferência, em inglês *Transfer Learning*, que utiliza um modelo pré-treinado para outras tarefas, sendo utilizado e adaptado para o problema a analisar. Este fator economiza o tempo de treino da rede neuronal, obtendo performance igual ou maior que um modelo treinado de raiz. Como exemplo desta abordagem implementada em sistemas de reconhecimento e verificação biométrica, este método foi usado e testado para a classificação de indivíduos através da análise da sua íris [57]. Para este teste, foi utilizada a *Resnet*, que, novamente, mostrou a sua eficácia para a resolução deste tipo de problemas.

Consoante o que foi abordado nesta secção, os sistemas de reconhecimento e verificação facial também sofreram uma grande evolução nos últimos anos, acompanhado pelo desenvolvimento das redes neuronais convolucionais. Em 2014, foi desenvolvido um dos primeiros sistemas de reconhecimento facial utilizando *Deep Learning*, *DeepFace* [80], publicado pelo *Facebook*, e foi o primeiro método a alcançar níveis de eficácia de reconhecimento próximo do nível de eficácia dos humanos. O desenvolvimento destes métodos nesta área é espelhado, por exemplo, na criação de uma função de perda específica para os problemas de reconhecimento e verificação facial, criada em 2019, designada por *ArcFace* [20]. Para esta implementação, as redes neuronais base utilizadas foram as *Resnet50* e *Resnet100* [39].

É possível perceber o crescimento que as abordagens de *Deep Learning* têm vindo a ter e a sua potencialidade em sistemas de reconhecimento e verificação de padrões, sendo que no futuro poderão ainda dar mais garantias de eficácia. Perante os trabalhos estudados, conclui-se, também, a boa eficácia que as *Resnet* tem na resolução problemas de Visão por Computador, utilizando *Deep Learning*, sendo das arquiteturas mais utilizadas para estas tarefas [87].

2.6 Métricas

A caraterização e a avaliação de um sistema de classificação de imagens não deve ser realizada apenas com um simples valor ou um simples teste, assim existem diversos métodos matemáticos com a capacidade de avaliar a performance dos modelos de classificação implementados. Estas métricas podem ser representadas como valores escalares ou podem ser representadas em gráficos [85].

Os sistemas de classificação binária são avaliados com base na matriz de confusão, ou seja, a matriz que representa os valores verdadeiros positivos (*TP*), verdadeiros negativos (*TN*), falsos positivos (*FP*) e falsos negativos (*FN*). Com a utilização destes valores são construídas as mais variadas métricas [36].

No processo de treino das redes neuronais é avaliada a exatidão (*accuracy* em inglês) com que o modelo classificador valida as imagens, sendo que esta métrica avalia a proporção de exemplares detetados corretamente sobre a totalidade de exemplares e pode ser definida, matematicamente, pela seguinte expressão.

$$\text{EXATIDÃO} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2.9}$$

Uma das métricas mais utilizadas nos sistemas a utilizar e a implementar nesta dissertação será o gráfico *ROC*, do inglês, *Receiver Operating Characteristics*, que se tem vindo a tornar num dos métodos de avaliação de desempenho de modelos de *Deep Learning* mais fiáveis nos últimos anos. Estas curvas mostram como o número de exemplos considerados corretamente positivos variam com o número de exemplos classificados incorretamente como negativos [18] e são representadas pela relação matemática entre a *True Positive Rate (TPR)* (equação 2.10) e a *False Positive Rate (FPR)* (equação 2.11, que são denominadas por sensibilidade e especificidade, respetivamente [78].

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2.10}$$

$$\text{FPR} = \frac{\text{FP}}{\text{TN} + \text{FP}} \tag{2.11}$$

Os pontos no canto superior esquerdo das curvas *ROC* têm alta taxa de verdadeiros positivos e baixa taxa de falsos positivos, o que os representa como classificadores inteligentes [78]. Para uma avaliação escalar da curva *ROC* é analisada a área da curva, denominada por *Area Under the Curve (AUC)*, que se apresenta como um valor fiável para a avaliação do desempenho dos modelos a testar [85]. A *ROC* também nos permite visualizar a relação entre a *False Match Rate (FMR)* e a *False Non-Match Rate (FNMR)*. A *FMR* é a probabilidade de o sistema corresponder incorretamente o padrão de entrada a um modelo não correspondente na base de dados, medindo a percentagem de entradas inválidas que são aceites de modo incorreto. Por sua vez, a *FNMR* é a probabilidade de o sistema falhar em detetar uma falha entre o padrão de entrada e um modelo correspondente na base de dados, medindo a percentagem de entradas válidas que são rejeitadas incorretamente. Estas duas taxas também apresentam utilidade na determinação do *Equal Error Rate (EER)*, que pode ser calculada no momento em que a *FMR* e a *FNMR* são iguais. Normalmente, os modelos com a taxa de erro mais baixa são os modelos mais precisos [78].

O valor da taxa de erro também pode ser retirado através da relação entre a *FMR* e a *FNMR*, e este gráfico é denominado por *Detection Error Tradeoff* (*DET*) [55]. A performance de um sistema é verificada consoante a aproximação da curva *DET* aos eixos e, esta aproximação, é caraterizada

pela o *EER*, representado na figura 2.12, ou seja o ponto de encontro entre a taxa de aceitação falsa e a taxa de rejeição falsa. Ou seja, intuitivamente, quanto menos for o valor do *EER*, mais perto a curva *DET* estará próxima dos eixos [30].

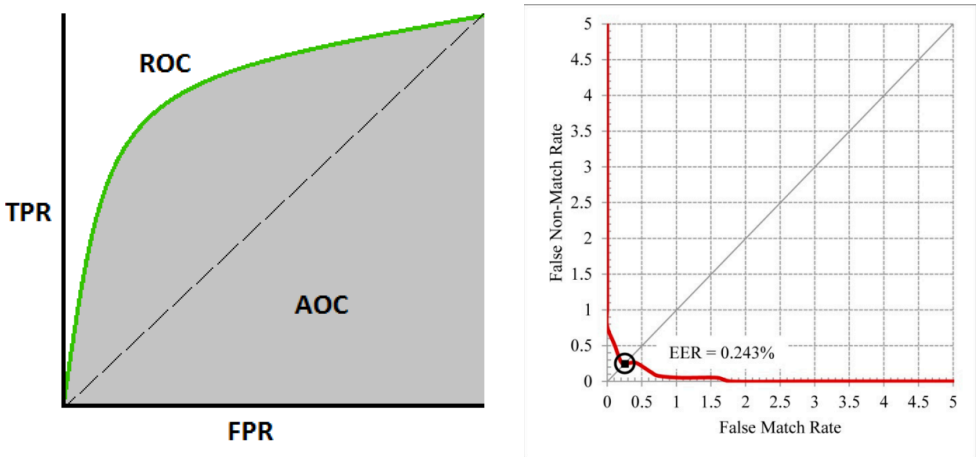

Figura 2.12: À direita, um gráfico a exemplificar uma possível curva *ROC* (retirado de [58]). À esquerda, o exemplo gráfico da relação entre a Taxa de Aceitação Falsa e a Taxa de Rejeição Falsa para obter a taxa de erro do sistema (retirado de [65])

Capítulo 3

Metodologia

3.1 Marcações a *Laser* em Metais Preciosos

A utilização de *lasers*, atualmente, é uma tecnologia mais económica em comparação com as marcações realizadas por punção e favorecem, particularmente, as marcações realizadas em materiais mais frágeis. O projeto *UniqueMark* desenvolveu este tipo de marcações que mostram segurança, devido aos seguintes fatores [33]:

- cada caminho realizado pelo *laser* é único, criando um padrão único;
- é virtualmente impossível recuperar, ou estimar com alta precisão, o caminho do *laser* observando a marcação;
- a reprodução do mesmo caminho do *laser* em diferentes objetos, à partida, terá a capacidade de produzir marcações distintas para cada um desses objetos, uma vez que os efeitos locais de derretimento são imprevisíveis e esse processo físico é caótico.

Perante estas informações é possível reparar que as marcações a *laser* são *PUFs*, devidamente abordadas no capítulo anterior. Estas marcações são realizadas pela Unidade de Contrastaria Portuguesa.

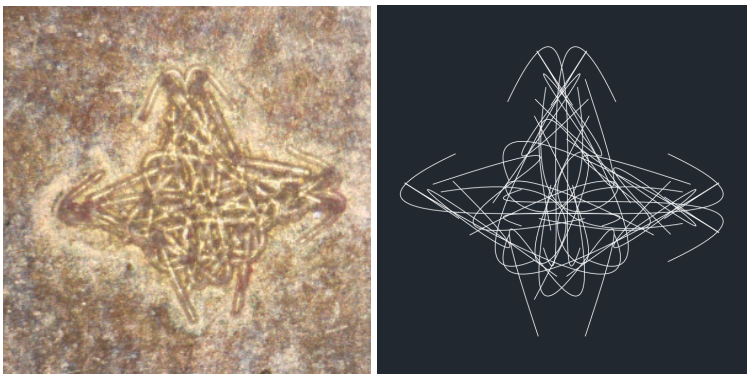

Figura 3.1: Exemplo de uma marcação a *laser* num material com base num desenho determinístico específico.

3.2 Organização dos Dados

Como mencionado anteriormente, a performance dos modelos classificadores de imagens depende de vários fatores relacionados com os dados disponibilizados. Os bancos de dados, no momento da sua construção, devem ter em conta a quantidade de dados, bem como a sua qualidade e variedade. Além disso, é necessário que o banco de dados apresente equilíbrio entre si. Para o projeto em questão, a aquisição de imagens e posterior construção de um banco de dados foi essencial para o início deste trabalho, visto que estamos perante um caso recente, sem bases de dados previamente realizadas. Num momento seguinte, em complemento ao banco de dados já construído foi disponibilizado um novo banco de dados mais completo, variado e com maior potencial de utilização. Maioritariamente, as imagens foram adquiridas com recurso a um microscópio digital. Como um dos principais objetivos deste projeto é testar a viabilidade das marcações em sistemas de classificação utilizando telemóveis, também foram usadas imagens adquiridas por telemóveis.

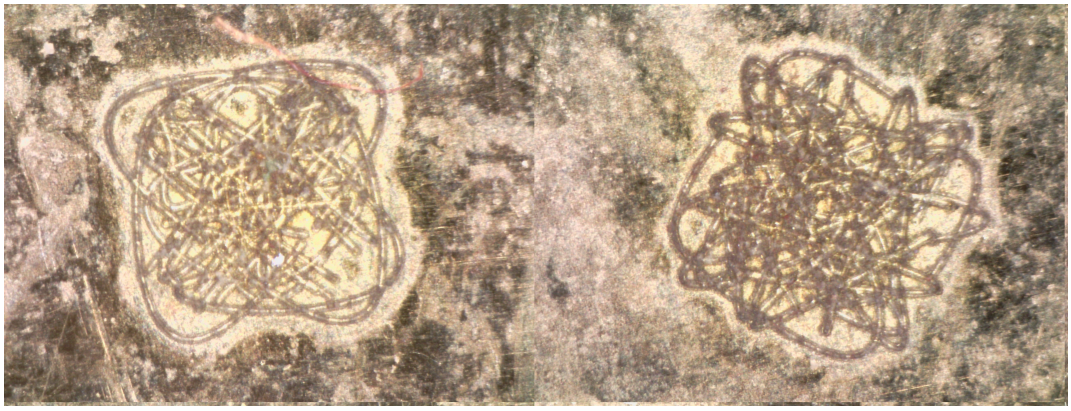

Figura 3.2: Exemplo de duas imagens de duas marcações diferentes presentes num dos bancos de dados referidos.

3.2.1 Construção Autónoma de um Novo Banco de Dados

Para a construção deste primeiro banco de dados (com imagens adquiridas pelo autor), foram fornecidas pela Unidade de Contrastaria placas com inúmeras marcações a *laser* integradas no material. Estas marcações dividiram-se em dois tipos de materiais diferentes: latão e cobre.

Como foram fornecidas 9 placas de latão e 1 de cobre, o número de marcações (identidades) disponibilizadas foram 200, sendo que as placas de latão continham 180 marcações diferentes e as placas de cobre tinham apenas 20 marcações diferentes. Por cada classe, são adquiridas 10 imagens, culminando com uma base de dados com 2000 imagens, no total. As 10 imagens por classe foram obtidas seguindo condições de luminosidade previamente registadas, de modo a acrescentar variedade à forma de aquisição das mesmas.

Para a aquisição das imagens foi utilizada uma lente microscópica digital *Dino-Lite Edge Digital Microscope* complementada com a utilização do *software DinoCapture 2.0* e esta lente é assentada e estabilizada através da utilização de uma base microscópica.

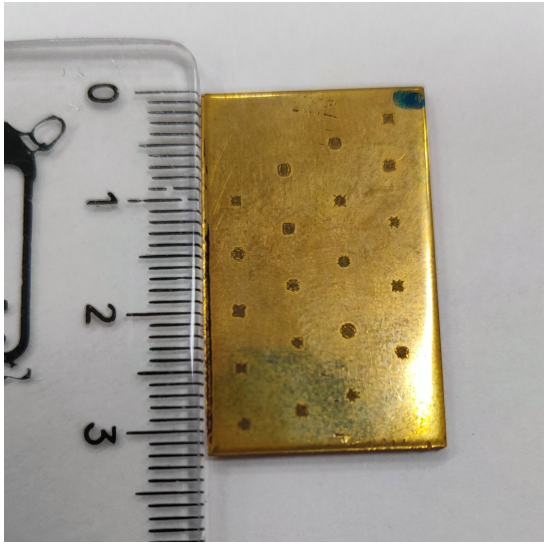

Figura 3.3: Um exemplo de uma das placas utilizadas para aquisição de imagens. Todas as placas possuem 20 marcações.

A nomenclatura relativa às marcações foi realizada consoante o material onde esta estava inserida, isto é, os nomes das marcações feitas em latão começam pela letra A, e os nomes das marcações feitas em cobre começam pela letra B. Assim, para o latão as marcações começam em A001 e terminam em A180, que correspondem às 180 identidades diferentes que são encontradas nas placas de latão. As restantes 20 identidades presentes nas placas de cobre começam em B001 e acabam em B020. As 10 imagens adquiridas por marcação foram obtidas seguindo diferentes condições de luminosidade. Estas diferentes condições foram conseguidas através das seguintes alterações realizadas nos equipamentos utilizados:

- A lente *Dino-Lite Digital Microscope* contém quatro *LEDs* brancos identificados no *software Dino Capture*, assim algumas imagens foram adquiridas com alteração no número de *LEDs* ligados. Também foram adquiridas imagens com alterações no brilho dos *LEDs* e este brilho varia numa escala de 1 a 6. Por omissão, os 4 *LEDs* estão ligados e a escala de brilho encontra-se a 6.

- A integração de duas peças diferentes na lente microscópica, como um difusor de luz e uma peça direcionadora de luz.

- A lente microscópica possui um controlador de polarização que, quando está no valor mínimo, significa que a imagem não está polarizada e quando alcança o valor máximo, significa que a imagem está polarizada ao seu nível máximo.

- Alterações na posição da placa, dando-lhe inclinação de modo a simular superfícies não planas, um ponto importante a considerar nesta dissertação, pois grande parte dos objetos e metais preciosos não apresentam caraterísticas unicamente planas. Estas imagens são distinguidas das restantes através da visualização de parte da imagem desfocada, que representa a parte irregular do objeto.

As condições de magnificação das imagens capturadas manteve-se constante, de modo a uniformizar esta condicionante de aquisição de imagens. Com o intuito de etiquetar e classificar cada condição de aquisição de imagens, a terminação utilizada nas nomenclaturas das imagens na base de dados é o fator de distinção. Em cada identidade, cada imagem é etiquetada com uma terminação de 01 a 10, em que cada uma representa um tipo de aquisição diferente. A seguinte tabela (tabela 3.1) especifica, devidamente, as condições relativas a cada terminação.

Terminação	**Descrição**
01	luz direta no material
02	luz direta no material (condição repetida)
03	integração do difusor de luz
04	integração do difusor de luz e brilho dos *LEDs*=2
05	integração difusor de luz com os *LEDs* 1, 2 e 3 desligados e o *LED* 4 ligado
06	integração da peça da direção de luz e polarização no mínimo
07	integração da peça da direção de luz (nova direção) e polarização no mínimo
08	integração da peça da direção de luz (mesma direção na imagem com terminação 06) e polarização no máximo
09	simulação de superfície não plana, com luz direta no material e inclinação da placa
10	condições similares à anterior, mas com brilho dos *LEDs*=2

Tabela 3.1: Condições de aquisição de imagem e descrição sua respetiva terminação.

Figura 3.4: Representação do sistema utilizado para capturar as imagens através do microscópio. É possível observar a base microscópica, a placa que contém as marcações e o microscópio digital *Dino-Lite Edge*. Também é visível o pormenor no microscópio digital na qual é possível regular o nível de polarização de uma imagem.

Como já foi referido, as imagens foram adquiridas com diferentes condições de luminosidade e, assim, é necessário entender alguns conceitos básicos sobre luminosidade.

- **Luz Difusa**: é uma luz suave, sem a intensidade e sem o brilho da luz direta. Está espalhada em todas as direções e, devido a essa particularidade, parece envolver objetos, sendo mais suave e tem a capacidade de não projetar sombras intensas. Nesse sentido, esta é utilizada para obter imagens com mais detalhe, como por exemplo em superfícies rugosas a nível microscópico, na qual é importante os detalhes serem explícitos [5]. Quando o difusor de luz é utilizado na lente microscópica, a luz do *LED* é distribuída uniformemente e é suavizada [42].

- **Luz Polarizada**: as vibrações elétricas e magnéticas de uma onda eletromagnética podem ocorrer em vários planos. Uma onda de luz que vibra em mais que um plano é denominada de luz não polarizada e, por sua vez, uma onda de luz polarizada é uma onda na qual as vibrações apenas ocorrem num plano [64].

- **Direcionador de Luz**: esta componente é utilizada para apenas iluminar lateralmente a imagem, cortando a luminosidade da lateral oposta, com o intuito de destacar as texturas e a profundidade dos alvos em curtas distâncias [42].

Figura 3.5: Imagens dos componentes inseridos na lente microscópica, explicados anteriormente. A imagem da esquerda corresponde ao direcionador de luz e, por sua vez, a imagem da direita corresponde ao difusor de luz.

Atualmente não existem métodos automáticos para adquirir imagens destas marcações, assim os bancos de dados têm que ser construídos manualmente. Nesse sentido, quando foi iniciada a realização deste banco de dados foi feito um estudo que simula e cronometra o tempo de aquisição de imagens. O cronómetro é iniciado no momento em que o operador agarra no material e finaliza no momento em que o material é retirado da base do microscópio. Para o teste realizado foram cronometradas 40 capturas, ou seja, foram utilizadas 2 placas diferentes. Em média, cada captura demorou 26.2 segundos a ser realizada, apresentando um desvio padrão de 10 segundos.

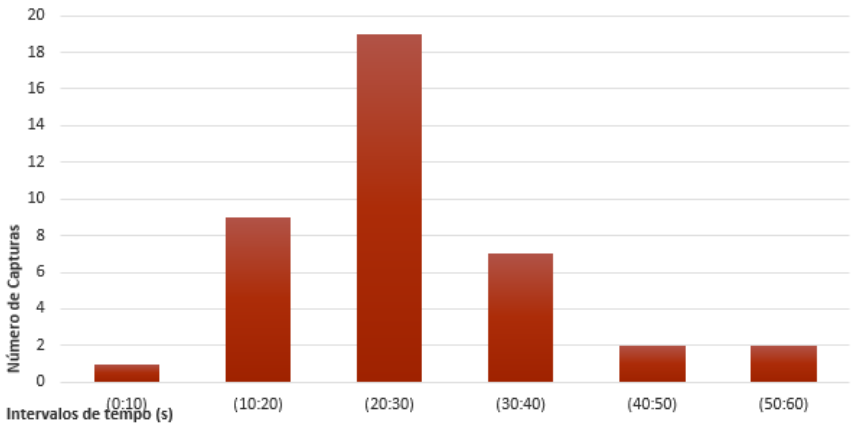

Figura 3.6: Histograma que representa o número de capturas efetuadas dentro de cada intervalo de tempo (cada intervalo de tempo tem duração equivalente ao valor do desvio padrão, ou seja, 10 segundos).

O tempo de aquisição de imagens, que é um valor elevado, pode ser uma consequência de diversos motivos que podem condicionar a velocidade com que uma imagem é adquirida. A localização da marcação do material, bem como a focagem da lente ou a forma física do material podem representar dificuldades que condicionam o tempo de aquisição das imagens.

3.2.2 Banco de Dados Disponibilizado

A pouca quantidade e variedade de imagens presentes no banco de dados abordado na secção anterior gerou a necessidade da utilização de um novo conjunto de dados, fornecido pela equipa de investigação onde este projeto está inserido, *VIS Team* do Instituto de Sistemas e Robótica da Universidade de Coimbra. Este conjunto de dados apresenta uma maior variedade, essencialmente ao nível do número de classes disponibilizadas, da inclusão de imagens capturadas com o telemóvel e do material utilizado para a realização das marcações a *laser*.

Neste novo banco de dados, o número de marcações aumentou consideravelmente, existindo imagens para 749 marcações diferentes. Como no conjunto de dados anterior, por cada marcação existem 10 imagens diferentes, fazendo um total de 7490 imagens. Deste conjunto de 10 imagens, o procedimento da divisão é realizado do seguinte modo:

- 7 imagens capturadas com a utilização da lente microscópica *Dino-Lite Digital Microscope*.
- 1 imagem obtida com a utilização do telemóvel *Huawei P40 Pro*.
- 1 imagem obtida com a integração de uma lente macro externa no telemóvel *Huawei P40 Pro*, denominada por *Nuguro Micro*.
- 1 imagem adquirida com a utilização do telemóvel *OnePlus 8 Pro*, utilizando o modo de lente macro, disponibilizado pela câmara integrada no telemóvel.

Figura 3.7: Telemóvel *OnePlus 8 Pro* utilizado para a captura de diversas imagens. É o telemóvel que possui uma câmara interna com lente macro incorporada.

Figura 3.8: À direita: telemóvel *Huawei* utilizado para a captura de diversas imagens, que possui uma câmara interna sem lente macro. À esquerda: telemóvel *Huawei* com a adição da lente macro externa *Nuguro*, também utilizada para a captura de diversas imagens.

Tal como no conjunto de dados construído pelo autor (abordado na secção anterior), este teve em conta variadas condições de aquisição de imagens devidamente referenciadas e explicitadas, tal como é apresentado pela tabela 3.2. Neste conjunto de imagens apenas existem marcações realizadas em prata.

Este banco de dados possui outra particularidade relativa ao estilo em que as marcações são realizadas:

- **Marcações com Desenhos Únicos:** marcações cujo desenho determinístico é único por objeto, onde cada padrão corresponde a uma classe. Para este caso existem 344 classes.
- **Marcações com Desenhos Repetidos:** marcações na qual o mesmo desenho determinístico é utilizado em diferentes objetos. Neste caso existem 45 desenhos determinísticos em que cada um destes é marcado em 10 materiais diferentes, existindo, assim, 450 classes.

Terminação	Descrição
01	integração do difusor de luz
02	integração do difusor de luz (condição repetida)
03	luz direta no material e polarização num nível médio
04	integração da peça de direção de luz com a polarização no máximo
05	integração da peça de direção de luz (numa direção diferente) com a polarização no máximo
06	integração do difusor de luz, com simulação de superfície não plana
07	integração do difusor de luz, com simulação de superfície não plana, com inclinação noutra direção
08	imagens obtidas através da utilização do telemóvel *OnePlus 8 Pro*, com a câmara interna em modo lente macro
09	imagens obtidas com a utilização do telemóvel *Huawei P40 Pro*
10	imagens obtidas com a utilização do telemóvel *Huawei P40 Pro* com a inclusão da lente macro externa *Nuguro Micro*

Tabela 3.2: Condições de aquisição de imagem e descrição sua respetiva terminação, no conjunto de dados referente a esta secção.

3.2.3 Comparação dos diferentes tipos de imagens

Como já foi referido, as imagens presentes em todos os conjuntos de dados abordados anteriormente foram obtidas através de lente microscópica digital e telemóveis. É possível constatar as diferenças dos tipos de imagens adquiridas com os diferentes tipos de equipamentos. Também as diferenças entre os diferentes tipos de condições de imagem são visualizáveis.

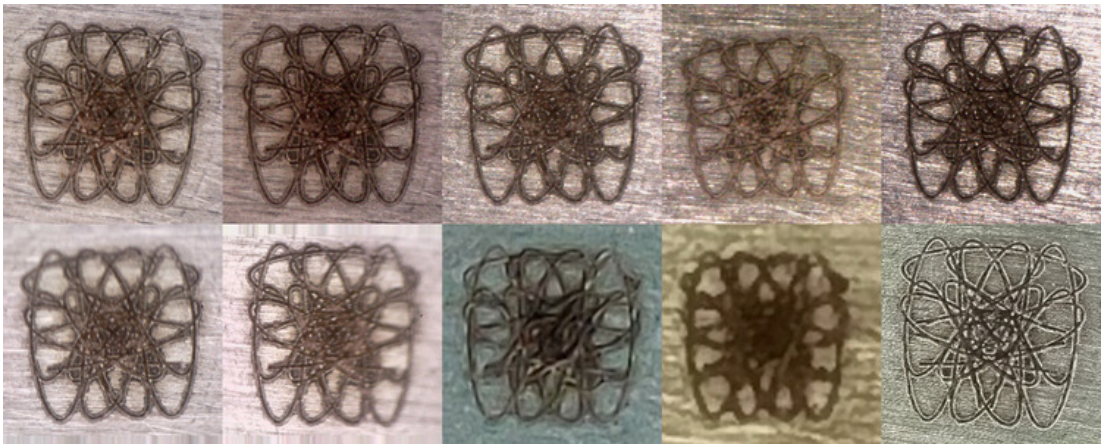

Figura 3.9: Sequência das 10 imagens com as suas condições presentes na tabela 3.2. Cada imagem está ordenada consoante a numeração de 01 a 10 na tabela 3.2.

Analisando as imagens presentes na figura 3.9, é notória a diferença de qualidade da imagem obtida com microscópio para as imagens obtidas com a utilização de um telemóvel (as últimas três imagens). A qualidade da imagem microscópica parece ser parcialmente replicada pela imagem obtida com a lente macro externa do *Huawei P40 Pro*. Ao nível da facilidade de captura de imagem, o uso da lente externa *Nuguro* não é aconselhável à utilização por parte de um utilizador comum,

devido ao facto de no momento da aquisição da imagem, o grau de minuciosidade e delicadeza dever ser elevado, de modo a conseguir estabilizar a câmara paralelamente ao objeto a fotografar e, caso este fator não seja tido em conta, a possibilidade da obtenção de imagens desfocadas é maior. Em contrapartida, a não inclusão desta lente externa (*Nuguro*) no *Huawei P40 Pro* poderá afetar a qualidade da imagem obtida, podendo ser um fator prejudicial para a análise computacional das imagens. O facto de a câmara interna do *OnePlus 8 Pro* possuir o modo de lente macro torna-se uma vantagem, realçada pela qualidade da imagem obtida apenas com o telemóvel, ainda assim, com definição notoriamente mais pequena do que as imagens microscópicas.

Como é possível verificar pelas tabelas 3.1 e 3.2 existem diversificações no modo como as imagens são capturadas com recurso a microscópio. A figura 3.9 também mostra os principais modelos de imagem existentes na totalidade das imagens de microscópio, na qual é possível notar as diferenças, tanto a nível de cor, como de qualidade das imagens presentes na figura. Como já foi abordado, a luz difusa reduz as sombras intensas da imagem, o que se torna vantajoso pois faz emergir caraterísticas das marcações mais visíveis, ao invés da luz direta, na qual se consegue perceber que, à partida, possui menos qualidade que a imagem capturada com recurso a um difusor de luz na lente microscópica. A introdução de um direcionador de luz, que limita lateralmente o ângulo de passagem de luz, fornece à imagem uma melhor visualização de diversos pormenores. Quando a imagem é polarizada, as diferenças a nível de cor e sombras entre as restantes imagens é grande e, caso não haja exemplos suficientes deste tipo de imagens no momento do treino da rede neuronal, os resultados no momento da sua aplicação a um modelo de classificação poderão ser prejudicados. Na figura 3.9 também estão presentes as imagens que simulam superfícies não planas com uma imagem normal adquirida numa superfície plana. A maior diferença notada é o facto de parte da marcação ficar desfocada causando essa sensação de profundidade existente quando existem variações e irregularidades nos planos, que se deve ao facto de a profundidade de campo da lente microscópica usada ser muito pequena, o que leva à desfocagem da imagem.

Figura 3.10: Imagens com marcações com desenhos repetidos noutros objetos. As imagens da linha cima simulam marcações originais (escolhido arbitrariamente) e as imagens da linha de baixo são marcações com desenhos repetidos noutros objetos, simulando uma marcação falsificada.

Na figura 3.10 é possível verificar o efeito ótico de um desenho de uma marcação replicado em diferentes objetos. É observável que os desenhos entre as marcações são iguais, mas são notórias diferenças na forma como o desenho é marcado no material, existindo variantes morfológicas nas imagens que, também, são possíveis de visualizar. Estas diferenças resultam da imprevisibilidade do processo de derretimento, como já foi abordado neste capítulo.

3.3 Construção do Modelo de *Deep Learning*

Após a obtenção dos dados e posterior organização dos mesmos, todas as condições estão reunidas para proceder à construção de um modelo de classificação para realizar o treino dos dados disponibilizados.

Em comparação com outros problemas de classificação comuns, a pouca abundância de dados gerou a necessidade de encontrar soluções para combater essa problemática. Uma das soluções possíveis trata-se da utilização de aprendizagem por transferência, em inglês, *Transfer Learning*, que se centra na implementação de modelos pré-treinados. Para além disso, é uma abordagem popular em casos de Visão por Computador pois permite construir modelos precisos economizando tempo. Com a aprendizagem por transferência, em vez do processo de treino iniciar do zero, este é iniciado com padrões que foram aprendidos ao resolver um problema diferente [54].

Grande parte dos modelos pré-treinados são baseados em grandes redes neuronais convolucionais e estas podem ser divididas em duas grandes partes [54]:

- **Base Convolucional**: composta por diversas camadas de convolução e de *pooling* que são úteis na deteção de caraterísticas das imagens.
- **Classificador**: geralmente, composto por camadas totalmente conectadas. O objetivo centra-se em classificar as imagens com base nas caraterísticas detetadas pela base convolucional.

Após a utilização da base convolucional do modelo pré-treinado, operando com a base de dados *ImageNet* [72], previamente treinada, camadas de classificação foram adicionadas à base convolucional. Vários modelos pré-treinados foram testados com o intuito de entender qual destes seria a melhor opção, com base em modelos já existentes na *Keras Applications*. Quatro diferentes modelos foram testados para os dados fornecidos: *Resnet50* [39]; *MobileNet* [41]; *Inception* [79] e *Xception* [13]. Cada um destes possui condições específicas de pré-processamento de imagem, sendo que, consoante o modelo a treinar, essas mesmas condições foram aplicadas e, por fim, foi realizada a normalização das imagens. De modo a evitar piores resultados no momento do treino, a técnica de *data augmentation* foi aplicada sob a forma de transformações de imagens. As transformações de imagens aplicadas foram as seguintes: variações de brilho, *flips* horizontais, *shifts* aleatórios e zoom aleatório.

3.3.1 Resnet50

Nos últimos anos, as redes neuronais sofreram enormes avanços na área da classificação de imagens, existindo inúmeras arquiteturas novas a ser desenvolvidas. Com estas inovações, uma das

questões que mais se impôs foi se a adição de mais camadas aos modelos iria melhorar o processo de treino, aumentando a profundidade da rede. Nesse sentido, as redes neuronais mais profundas começaram a ser estudadas e algumas adversidades foram encontradas. Quando, no processo de treino, as redes neuronais profundas começam a convergir, o problema da degradação da rede é exposto, isto é, com o aumento da profundidade da rede, a sua precisão fica saturada, causando uma degradação rápida da rede [39].

Para combater o problema da degradação da rede, descrito anteriormente, a *Resnet* [39] foi desenvolvida, com o intuito de facilitar o processo de treino das redes neuronais profundas, utilizando uma estrutura de aprendizagem residual.

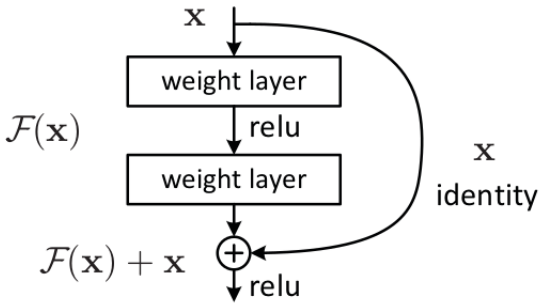

Figura 3.11: Representação esquemática da estrutura de aprendizagem residual (retirado de [39]).

As camadas são reformuladas com funções de aprendizagem residual com referência para as camadas de entrada, ao invés de funções de aprendizagem não referenciadas [39]. As arquiteturas *Resnet* desenvolvidas diferem no número de camadas que possuem, como se pode verificar pela figura 3.12, onde são mostradas, também, as camadas existentes na rede, bem como as suas operações.

layer name	output size	18-layer	34-layer	50-layer	101-layer	152-layer
conv1	112×112	7×7, 64, stride 2				
conv2_x	56×56	3×3 max pool, stride 2				
		$\begin{bmatrix} 3\times3, 64 \\ 3\times3, 64 \end{bmatrix}\times2$	$\begin{bmatrix} 3\times3, 64 \\ 3\times3, 64 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 64 \\ 3\times3, 64 \\ 1\times1, 256 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 64 \\ 3\times3, 64 \\ 1\times1, 256 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 64 \\ 3\times3, 64 \\ 1\times1, 256 \end{bmatrix}\times3$
conv3_x	28×28	$\begin{bmatrix} 3\times3, 128 \\ 3\times3, 128 \end{bmatrix}\times2$	$\begin{bmatrix} 3\times3, 128 \\ 3\times3, 128 \end{bmatrix}\times4$	$\begin{bmatrix} 1\times1, 128 \\ 3\times3, 128 \\ 1\times1, 512 \end{bmatrix}\times4$	$\begin{bmatrix} 1\times1, 128 \\ 3\times3, 128 \\ 1\times1, 512 \end{bmatrix}\times4$	$\begin{bmatrix} 1\times1, 128 \\ 3\times3, 128 \\ 1\times1, 512 \end{bmatrix}\times8$
conv4_x	14×14	$\begin{bmatrix} 3\times3, 256 \\ 3\times3, 256 \end{bmatrix}\times2$	$\begin{bmatrix} 3\times3, 256 \\ 3\times3, 256 \end{bmatrix}\times6$	$\begin{bmatrix} 1\times1, 256 \\ 3\times3, 256 \\ 1\times1, 1024 \end{bmatrix}\times6$	$\begin{bmatrix} 1\times1, 256 \\ 3\times3, 256 \\ 1\times1, 1024 \end{bmatrix}\times23$	$\begin{bmatrix} 1\times1, 256 \\ 3\times3, 256 \\ 1\times1, 1024 \end{bmatrix}\times36$
conv5_x	7×7	$\begin{bmatrix} 3\times3, 512 \\ 3\times3, 512 \end{bmatrix}\times2$	$\begin{bmatrix} 3\times3, 512 \\ 3\times3, 512 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 512 \\ 3\times3, 512 \\ 1\times1, 2048 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 512 \\ 3\times3, 512 \\ 1\times1, 2048 \end{bmatrix}\times3$	$\begin{bmatrix} 1\times1, 512 \\ 3\times3, 512 \\ 1\times1, 2048 \end{bmatrix}\times3$
	1×1	average pool, 1000-d fc, softmax				
FLOPs		1.8×10^9	3.6×10^9	3.8×10^9	7.6×10^9	11.3×10^9

Figura 3.12: Arquitetura da *Resnet* com 18 camadas, 34 camadas, 50 camadas, 101 camadas e 152 camadas. (retirado de [39])

A avaliação da performance da *Resnet* utilizou a base de dados *ImageNet* [72], que é um objeto de avaliação para algoritmos de classificação de imagens e deteção de objetos em grande escala, com uma enorme variedade de classes.

Para o treino da rede neuronal foram adicionadas camadas de classificação à base convolucional, descritas na figura 3.13.

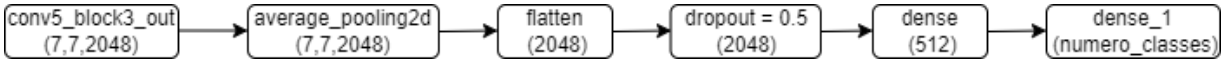

Figura 3.13: Representação esquemática do classificador construído por cima da base convolucional da *Resnet50*, sendo que a primeira camada aqui representada ainda pertence à camada convolucional.

A escolha da *Resnet50* teve por base o seu tamanho, 98 MB, que quando comparadas às outras *Resnets* é das que menos capacidade computacional pode exigir. Como já foi referenciado, outro ponto a pesar na decisão de qual a melhor arquitetura de rede a utilizar, foi a sua comparação com outros modelos existentes. O banco de dados utilizado para a realização dos treinos iniciais das redes neuronais, foi o conjunto de imagens que apenas contém imagens de marcas em placas de prata. É usual a divisão do conjunto de imagens em três sub-conjuntos diferentes, o conjunto de imagens para treino, para validação e para teste. Assim, das 749 classes existentes, inicialmente retiraram-se 80 classes para teste. Seguidamente, com as restantes imagens, a criação do conjunto de dados de validação foi gerada aleatoriamente, representando um total de 20% da totalidade dessas imagens.

Os parâmetros do treino da rede são similares a todos os modelos estudados anteriormente que, seguidamente, serão enumerados: 1) número de *epochs*: 30; 2) *batch size*: 32; 3) *learning rate*: 0.01; 4) otimizador: SGD; 5) função de perda: *CategoricalCrossentropy*; 6) função de ativação: *Softmax*.

Modelo	Função de Perda	Exatidão
Resnet50	1.08	75.5%
MobileNet	7.29	0.0%
Xception	1.14	68.9%
Inception	1.22	69.6%

Tabela 3.3: Resultados do treino dos modelos pré-treinados testados.

Como já foi referido, foram testados diferentes modelos, de modo, também, a comparar com outros modelos pré-treinados com o intuito de reforçar a escolha da *Resnet50*, e esses resultados estão mostrados na tabela 3.3. É importante referir que estes resultados serviram para encontrar uma referência de comparação, sendo que estes valores de exatidão serão trabalhados e melhorados no desenrolar do projeto.

3.3.2 Detalhes da Implementação

Este projeto foi desenvolvido utilizando *Python 3.7*, sendo que as redes neuronais foram implementadas utilizando a biblioteca *Keras*, na qual existem diversas redes neuronais, previamente treinadas, disponíveis na *Keras Applications*. Os programas foram executados na GPU (*Graphics Processing Units*), com a utilização de um computador com maior poder computacional, devido à carga que os treinos das redes implicam.

Em toda a organização de dados e tratamento de resultados foi utilizada a biblioteca *Pandas* e para as operações básicas foi utilizada a biblioteca *Numpy*. Os gráficos foram gerados utilizando a biblioteca *Matplotlib*.

O alinhamento das imagens foi disponibilizado pela equipa VIS Team, na qual a sua implementação teve por base a utilização de recursos da biblioteca *OpenCV*.

3.4 Protocolos de Treino e de Teste

O tema desta dissertação centra-se na obtenção de resultados que possibilitem a obtenção de informações relevantes relativas à viabilidade e às condicionantes da utilização de marcações a *laser* em jóias e metais preciosos. Nesse sentido, é possível analisar que a variedade das imagens utilizadas centra-se nas diferenças entre metais utilizados (prata, latão e cobre) e nas diferentes condições de aquisição da imagem, seja a nível físico ou ao nível de condições de luminosidade.

Vários treinos serão realizados consoante os testes a realizar, que terão por base todas as variantes existentes dentro dos bancos de dados disponibilizados, que serão abordados nesta secção. Os treinos de redes neuronais utilizarão o modelo e os parâmetros descritos anteriormente.

3.4.1 Protocolo 1 - Testes de verificação utilizando marcações com desenho único e repetido

Neste teste apenas foi utilizado o banco de dados com imagens de prata. Como já foi referido este banco de dados possui 749 classes que podem ser divididas em marcações com desenhos repetidos por objeto e marcações com desenhos únicos por objeto. Assim, é possível utilizar este banco de dados de três maneiras distintas:

- Usar o banco de dados na sua totalidade, com as marcações com desenho único e as marcações com desenho repetido;
- Utilizar apenas as marcações com desenho único;
- Utilizar apenas as marcações com desenho repetido.

Após a divisão dos dados, o conjunto de marcações com desenho único possui 342 classes. Existem 45 marcações com desenhos repetidos em 10 objetos diferentes, que no total significa que serão utilizadas 450 classes, pois cada marcação só é repetida em 10 materiais de cada vez. Assim,

serão treinadas três redes neuronais relativas às três maneiras possíveis de utilização deste banco de dados.

Para o processo de teste, foram utilizadas classes que não estão representadas no processo de treino, de modo a dificultar a classificação por parte do modelo classificador, sendo que esta particularidade é aplicada a todos os protocolos de teste que serão abordados nas secções seguintes. Nesse sentido, a divisão dos bancos de imagens disponíveis em dados de treino e dados de teste está representada na tabela 3.4.

Banco de Dados	Treino	Teste
Completo	669 classes	80 classes
Marcações com Desenho Único	308 classes	36 classes
Marcações com Desenho Repetido	400 classes	50 classes

Tabela 3.4: Divisão do banco de dados em treino e teste.

A camada de classificação é removida do modelo classificador criado, assim quando uma imagem é introduzida no modelo, apenas são extraídos os *features* dessa imagem. Comparando esses *features* aos de outra imagem é possível obter o nível de similaridade entre os mesmos e esse cálculo é realizado utilizando o produto interno entre os dois vetores. O modelo extrai 512 *features* por imagem. Neste sentido, os testes serão realizadas com base na técnica de verificação 1 para 1, sendo que este método de classificação será utilizado em todos os testes realizados neste trabalho. Assim, como estamos perante um processo de verificação, é necessário realizar todas as combinações possíveis de imagens (2 a 2) com todas as imagens que se pretende testar.

3.4.2 Protocolo 2 - Verificação de imagens de telemóvel

A quantidade de imagens, por classe, que foram capturadas com recurso à utilização de um telemóvel representa 30% dessa totalidade, assim existem dados suficientes para testar o poder de classificação dos modelos utilizando imagens de telemóvel.

O banco de dados utilizado é o que apenas contém exemplares de prata e, com base no que foi explicado no Protocolo 1, é utilizado o banco de dados completo e o banco de dados com marcações com desenhos únicos. Para cada um destes bancos de dados, são realizados dois treinos distintos, que são transversais aos dois conjuntos de dados:

- **Primeiro treino**: remoção de todas as imagens capturadas com telemóvel das imagens de treino, restando apenas 7 imagens por classe.
- **Segundo treino**: utilização de todas as imagens presentes nos conjuntos de dados de treino.

A realização do protocolo de teste, à partida, teria como principais obstáculos o número de combinações possíveis e a garantia de que os tipos de combinações seriam equilibrados, isto é, todas as imagens de telemóveis serem comparadas às mesmas imagens microscópicas, de modo

a que os resultados, posteriormente, fossem mais fidedignos. Nesse sentido, as imagens de telemóvel foram comparadas a todas as imagens de microscópio, sem que as imagens de telemóvel se combinem entre si. É possível obter combinações relativas às imagens obtidas com o telemóvel *Huawei*, com a lente macro externa no telemóvel, *Huawei Nuguro*, e com o telemóvel *OnePlus*. Este processo pode ser clarificado através da figura 3.14.

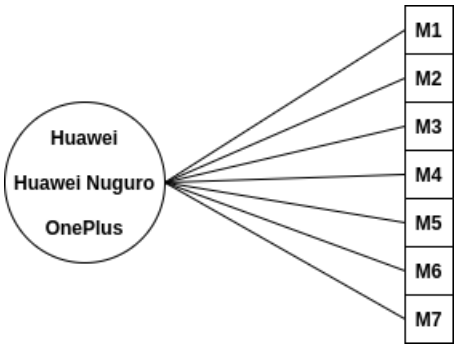

Figura 3.14: Exemplificação do protocolo de teste, em que à esquerda estão representadas os tipos de imagem de telemóvel, e à direita as restantes 7 imagens de microscópio.

Após o desenvolvimento do protocolo de teste, este é aplicado aos 4 modelos treinados, já explicados no início da explicação deste protocolo.

3.4.3 Protocolo 3 - Testes de materiais

Como foi referido no início deste capítulo, existem dois bancos de dados, o primeiro possui apenas exemplares de prata, o seguinte possui exemplares de latão e de cobre. O maior problema que existe para a construção de um teste que visa analisar o comportamento dos sistemas aplicando testes com variações de materiais, é o desequilíbrio existente entre as quantidades de exemplares de cada material diferente. Nesse sentido, foi necessário planear uma estratégia de modo a conseguir equilibrar os dados existentes. Para os exemplares de prata, foi utilizado o banco de dados com marcações com desenhos único.s No que diz respeito ao banco de dados que possui exemplares de latão e de cobre, o número de classes é muito diferente, sendo que existem 180 classes de latão e 20 classes de cobre. Para a realização deste teste, foram realizados dois treinos distintos:

- **Primeiro treino**: utilização do banco de dados de prata, utilizando 308 classes para treino (como utilizado nos protocolos anteriores).
- **Segundo treino**: utilização de exemplares de materiais de latão e prata para treino, utilizando, igualmente, 308 classes para treino, apresentando 158 classes de prata e 150 classes de latão. Assim, este treino é realizado utilizando 308 classes diferentes, de materiais diferentes, dividido de forma praticamente igual, de modo a manter coerência na quantidade de dados por material.

Para a realização do protocolo de teste, são utilizadas 30 classes de prata e de latão e são utilizadas todas as classes existentes de cobre, ou seja, 20 classes. As combinações são realizadas por materiais, para se proceder à comparação entre resultados com cada material, assim obtêm-se

protocolos de teste para prata, latão e cobre.

3.4.4 Protocolo 4 - Teste com marcações inclinadas

A construção dos conjuntos de dados teve em conta a simulação de superfícies não planas, isto é, os metais preciosos e jóias não são, necessariamente, superfícies planas, sendo que isso pode causar problemas no processo de classificação de imagens. Nesse sentido, este teste visa analisar as marcações que simulam superfícies não planas e compará-las com marcações obtidas em superfícies planas.

Para o processo de treino, foram utilizados os seguintes modelos gerados referidos no protocolo anterior, que incluem: 1) banco de dados de marcação com desenho único apenas com imagens de prata, com 308 padrões diferentes; 2) banco de dados com imagens de prata e de latão, de marcação com desenho único, utilizando, igualmente, 308 marcações diferentes. Para o processo de teste foram utilizados exemplares de prata e latão, com o intuito de aumentar a amostra a testar. Assim, testaram-se 34 classes de prata e 40 classes de latão.

Tanto no conjunto de dados de prata, como no conjunto de dados de latão existem 2 imagens por marcação que simulam a existência de superfícies não planas. Assim, de modo a equilibrar o número de imagens foram utilizadas mais 2 imagens por marcação, de superfícies planas.

Tipos de imagem	Banco de Dados	Terminação
Superfície Plana	Prata	06,07
Superfície Plana	Latão	09,10
Superfície Não Plana	Prata	01,02
Superfície Não Plana	Latão	01,02

Tabela 3.5: Terminação das imagens utilizadas para a realização do protocolo de teste, devidamente referenciadas nas tabelas 3.1 e 3.2.

As imagens utilizadas descritas na tabela anterior são divididas em superfícies planas e superfícies não planas. O esquema de combinações de imagens de teste, utilizados neste protocolo, é construído de modo similar ao que foi utilizado no Protocolo 2, representado na figura 3.14. As imagens de superfície planas e são combinadas com as restantes, sem se combinarem entre si e o mesmo processo é realizado para as imagens de superfícies não planas. Assim, são construídos dois protocolos de combinações diferentes de teste, com o mesmo número de amostras.

3.4.5 Protocolo 5 - Condições de aquisição de imagem

Nas tabelas 3.1 e 3.2 estão referenciadas diversas condições de aquisição de imagens presentes dos diferentes bancos de dados. Com essa diferenciação, é possível analisar o comportamento dos sistemas para variadas formas de aquisição das imagens. Neste caso, é possível verificar que existem diversas imagens que utilizam um difusor de luz no momento da sua aquisição, tal como,

a utilização da peça direcionadora de luz. Também é possível verificar que existem diversas variações de polarização das imagens. Nesse sentido, este protocolo divide-se em dois sub-protocolos de testes diferentes, que, seguidamente, serão explicados.

O primeiro modelo classificador utilizado é o modelo relativo às marcações de prata com desenho único, e o segundo utiliza o modelo treinado para os testes de materiais, que contém imagens de prata e latão, ambos com 308 classes. A utilização destes 2 modelos acontece, pois para este teste são usadas marcações desenhadas em latão e prata. Assim, para teste, foram utilizadas 34 classes de marcações desenhadas em prata e 40 classes de marcações em latão. O método de combinações utilizado para a construção dos protocolos é similar aos protocolos anteriores.

3.4.5.1 Polarização das Imagens

Nos conjuntos de dados existem diversas variações de polarização, que podem ser divididas em 3 conjuntos: 1) sem polarização; 2) com polarização a 50%; 3) com polarização a 100%. Como já foi abordado, esta variação de polarização é obtida através de um componente integrado na lente microscópica que permite regular, de forma precisa, o nível de polarização de uma imagem.

Tipos de imagem	Banco de Dados	Terminações
Sem Polarização	Prata	01,02,06,07
Sem Polarização	Latão	06,07
Polarização 50%	Prata	03
Polarização 50%	Latão	01,02,03,04,09,10
Polarização 100%	Prata	04, 05
Polarização 100%	Latão	08

Tabela 3.6: Terminação das imagens utilizadas para a realização do protocolo de teste de polarização de imagens, devidamente referenciadas nas tabelas 3.1 e 3.2.

Neste caso, o número de imagens utilizadas para testar entre os diferentes níveis de polarização não é igual, causando variação no número de amostras utilizadas para testar cada condicionante, o que pode ser um fator desprezável, pois o número de combinações entre imagens, em qualquer um dos casos, é elevado. Do mesmo modo que foi realizado anteriormente, as imagens utilizadas em cada nível de polarização não se cruzam entre si no processo de verificação 1 para 1.

3.4.5.2 Inclusão de Difusor de Luz e do Direcionador de Luz

Para a aquisição das imagens, em certos casos, foi utilizado um difusor de luz, e noutras imagens, foi utilizado um direcionador de luz, na qual apenas deixa a luz passar numa direção. A adição destes componentes à lente serão utilizados para teste, a par da comparação com as imagens obtidas com luz direta no material, ou seja, sem nenhum componente adicional na lente.

Tipos de imagem	Banco de Dados	Terminações
Luz Direta no Material	Prata	03
Luz Direta no Material	Latão	01,02,09,10
Difusor de Luz	Prata	01,02,06,07
Difusor de Luz	Latão	03,04,05
Direcionador de Luz	Prata	04, 05
Direcionador de Luz	Latão	06,07,08

Tabela 3.7: Terminação das imagens utilizadas para a realização do protocolo de teste da inclusão do difusor e do direcionador de luz, devidamente referenciadas nas tabelas 3.1 e 3.2.

A particularidade descrita no protocolo de teste de polarização é aplicada a este caso. Também, nesta situação o número de imagens a testar, e o consequente número de combinações entre elas não é equilibrado entre cada componente utilizado para adquirir as imagens. O número de combinações entre as imagens é, novamente, elevado, o que pode atenuar o efeito da diferença existente entre o número de amostras. É garantido, de novo, que, no processo de verificação 1 para 1, as imagens obtidas de cada componente não se cruzam com outras imagens obtidas com esse mesmo componente.

Capítulo 4

Resultados e Discussão

O presente capítulo visa mostrar o resultado dos testes realizados, com base nas metodologias exploradas no capítulo 3. Os protocolos de teste, anteriormente explicados, serão os objetos de avaliação deste projeto. Nesse sentido, neste capítulo é pretendido:

- Avaliar o comportamento dos sistemas de classificação com marcações com desenhos únicos por objeto, comparando-as com marcações com desenhos repetidos em diferentes objetos.
- Testar imagens capturadas com a utilização de telemóveis, comparando os tipos de telemóvel utilizados para entender a influência da introdução das imagens de telemóvel nos dados de treino.
- Comparar os 3 diferentes tipos de materiais presentes nos bancos de dados, percebendo se a sua utilização no momento de treino das redes neuronais, tem influência no poder de classificação sobre esses mesmos materiais.
- Comparar a utilização de imagens que simulam superfícies não planas com imagens de superfícies planas e verificar se esta condicionante é um fator a ter em conta na viabilidade das marcações desenhadas a *laser*.
- Verificar o efeito que as variações de aquisição de imagem têm nos modelos de classificação, nomeadamente, ao nível de polarização de imagem e ao nível da introdução de componentes externos nas lentes microscópicas.

4.1 Testes de Verificação Utilizando Marcações com Desenho Único e Repetido

Como já foi abordado, este teste pretende analisar as diferenças existentes entre introduzir uma marcação por objeto ou replicar marcações em diferentes objetos e verificar o comportamento de um sistema de verificação, tendo em conta estas duas variantes. Os conjuntos de dados são divididos em três: 1) marcações com desenho único por objeto; 2) marcações com desenho repetido em diferentes objetos; 3) junção entre marcações com desenhos únicos e repetidas. As marcações que têm desenhos repetidos em diferentes objetos poderão ser úteis no sentido de perceber se um sistema de verificação tem a capacidade de classificar marcas que podem ser falsificadas.

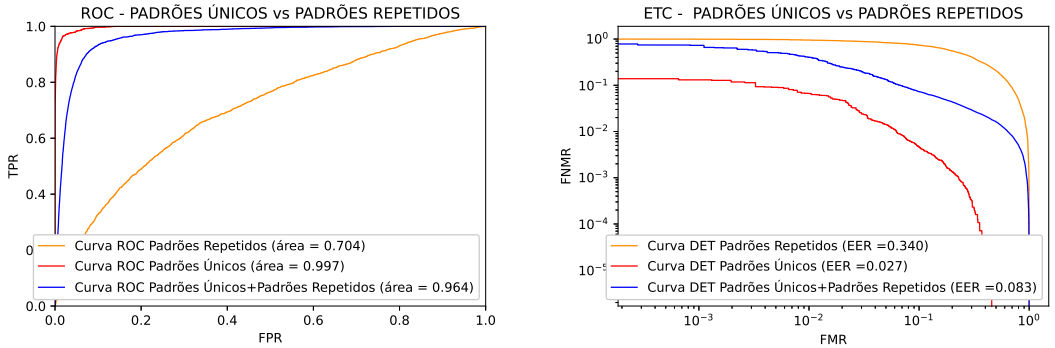

Figura 4.1: Curvas *ROC* e *DET* geradas quando são testados os modelos criados com marcações com desenhos únicos por objeto e com desenhos repetidos em diferentes objetos. Também estão representadas as curvas referentes à junção dos dois tipos de marcações.

Concordando com o que seria expectável, pela análise dos gráficos presentes na figura 4.1, as marcações com desenhos únicos obtêm resultados melhores em relação às restantes opções. Isto acontece, pois a utilização de apenas um desenho único por objeto causa uma maior facilidade de distinção entre as marcações, pois cada uma possui o seu próprio desenho determinístico, alcançando diferenças notórias, tanto ao nível das curvas *ROC* e *DET*, como ao nível do valor de *EER*. Este é um bom resultado, pois a capacidade de distinção de marcações é alta, apresentando uma taxa de erro de apenas 3%. A curva *ROC* e *DET*, referentes às marcações com desenhos repetidos em diferentes objetos, é a que piores resultados obtém, devido ao facto de estas possuírem o mesmo desenho determinístico, o que mostra que, nestas condições, o modelo de classificação não teria boa capacidade de distinguir as marcações falsificadas das originais. De modo a aumentar a performance do sistema de verificação, no sentido de melhorar os resultados, foi usado o banco de dados na sua totalidade, sendo consideradas marcações com desenhos únicos e com desenhos repetidos no processo de treino da rede neuronal. Com estas condicionantes, os resultados tendem a ser melhores e, derivado do facto de existirem marcações com desenhos únicos e com desenhos repetidos, é realizada uma melhor distinção entre as marcações. Assim, é possível entender que a utilização das duas variedades de marcações no momento do treino da rede, irá influenciar o desempenho do sistema de classificação positivamente, tendo uma boa capacidade de distinguir marcações com desenhos repetidos, como é possível verificar pelas curvas *ROC* e *DET* (representadas pela cor

azul na figura 4.1).

4.2 Verificação de Imagens de Telemóvel

Um dos principais pontos do projeto na qual esta dissertação está inserida, é o desenvolvimento de um sistema capaz de verificar marcações utilizando apenas um telemóvel. Como já foi explicado, nos bancos de dados existem três tipos de imagens capturadas com telemóvel com as suas variantes, e o objetivo é perceber a influência que estas variantes possuem e se podem ser consideradas, futuramente, para a utilização de um sistema deste tipo usando telemóveis. Também será analisada a influência da inclusão de imagens capturadas com telemóveis no momento do treino da rede neuronal, comparando ao treino de rede realizado apenas com imagens obtidas com o microscópio. Este teste será realizado treinando 4 modelos diferentes.

Modelos	Marcações	Condições
1.1	Marcações com desenho único	Imagens de microscópio
1.2	Marcações com desenho único	Imagens de microscópio e telemóvel
2.1	Marcações com desenho único e repetido	Imagens de microscópio
2.2	Marcações com desenho único e repetido	Imagens de microscópio e telemóvel

Tabela 4.1: Descrição dos modelos de classificação treinados o teste de verificação das imagens de telemóvel.

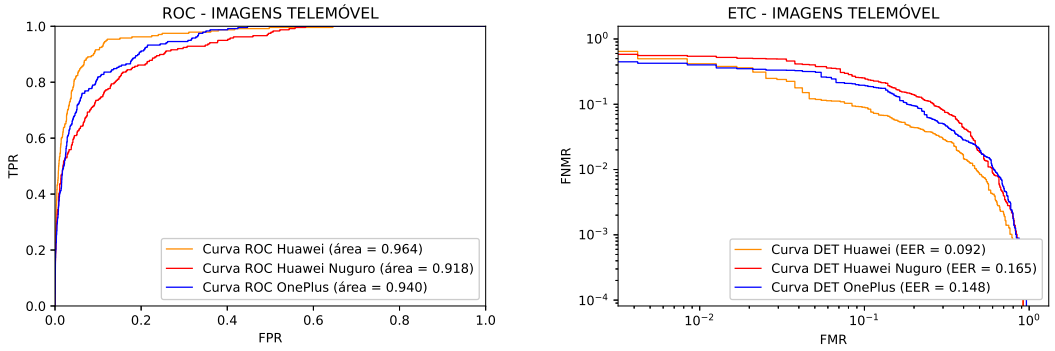

Figura 4.2: Curvas *ROC* e *DET* geradas quando são testados os diferentes tipos de imagens de telemóvel no modelo de classificação 1.1 (referido na tabela 4.1).

A figura 4.2 refere-se ao modelo treinado apenas com imagens obtidas com microscópio, onde é possível perceber a real influência de cada tipo de imagem, pois estas não estão representadas no treino da rede. Assim, a diferença entre as curvas *ROC* referentes a cada modelo é notória. Seria expectável que a utilização de lentes macro para a captura das imagens poderia influenciar positivamente os sistemas de classificação, pois, teoricamente, a utilização de uma lente macro aumenta a resolução da imagem obtida. Mas, contrariamente ao expectável, as imagens capturadas com o único dispositivo que não possui lente macro, o *Huawei P40 Pro*, foram as que obtiveram que melhores resultados. A utilização do modelo de telemóvel que possui lente macro na câmara interna, *OnePlus 8 Pro*, foi a que obteve o resultado, em que tanto o valor de *EER* e as curvas

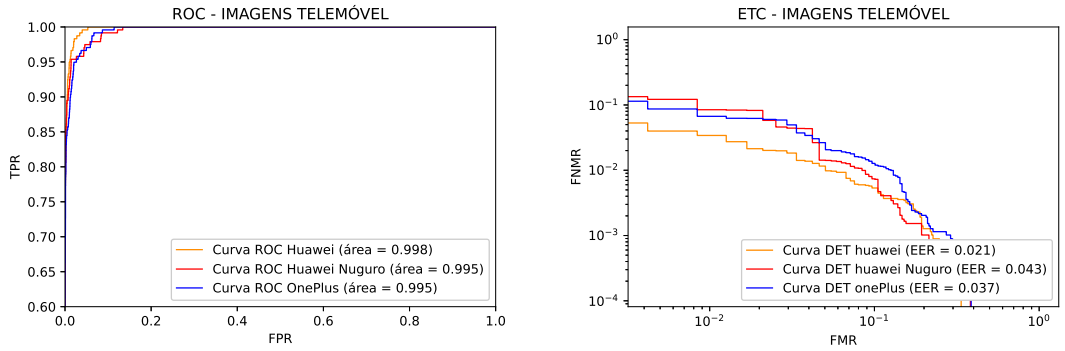

Figura 4.3: Curvas *ROC* e *DET* geradas quando são testados os diferentes tipos de imagens de telemóvel no modelo de classificação 1.2 (referido na tabela 4.1).

ROC e *DET* mais se aproximaram do *Huawei*. Por sua vez, a utilização da lente macro *Nuguro*, introduzida no modelo de telemóvel *Huawei* não obteve o resultado esperado, sendo o pior dos 3 casos. É possível concluir que a utilização de uma lente macro externa ou interna degrada os resultados do modelo de classificação de padrão único. Esta situação poderá ser explicada através de diversas distorções da imagem que a utilização de uma lente macro poderá causar, o que poderá ser uma razão para os resultados mais negativos apresentados. Também a qualidade da imagem obtida com as lentes macro é sensível à estabilidade do telemóvel. A figura 3.9, no capítulo 3, poderá comprovar as diferenças entre as opções aqui representadas, onde visualmente é possível, efetivamente, perceber que a resolução das imagens é melhor, quando adquiridas com uma lente macro, mas que são bastante diferentes morfologicamente das restantes. Uma possível solução para este problema é a introdução de exemplares de todos os tipos de imagens utilizadas no treino da rede neuronal.

Nesse sentido, foi realizado o mesmo teste, presente na figura 4.3, utilizando um modelo de classificação na qual todos os tipos de imagem de telemóvel foram incluídos no treino da rede neuronal. Os efeitos desta introdução mostraram ser bastante positivos, melhorando os resultados obtidos nos três tipos de imagens de telemóvel adquiridas para valores muito interessantes, bem como a proximidade entre as curvas *ROC* e *DET* geradas e os valores de *EER* que vincam a importância da necessidade da existência de exemplares de todos os tipos de imagens no treino da rede neuronal.

De modo similar, as imagens obtidas com telemóvel foram testadas com o modelo classificador que utiliza marcações com desenhos únicos e marcações com desenhos repetidos no treino da rede. Esta análise teve o objetivo de perceber se algum destes dispositivos poderia fazer com que o sistema de classificação obtivesse uma melhor reação, visto que, como já foi comprovado, a inclusão de marcações com desenhos repetidos pode ter influência negativa na performance dos modelos classificadores. A figura 4.4 mostra que, realmente, existem diferenças em relação ao que foi analisado no modelo classificador anterior, que apenas utiliza marcações com desenhos únicos. Neste caso, a curva *ROC* mais satisfatória, aliada ao melhor valor de *EER* é a relativa às imagens obtidas com a utilização do *OnePlus*. A curva *ROC* do telemóvel *Huawei* aproxima-se bastante

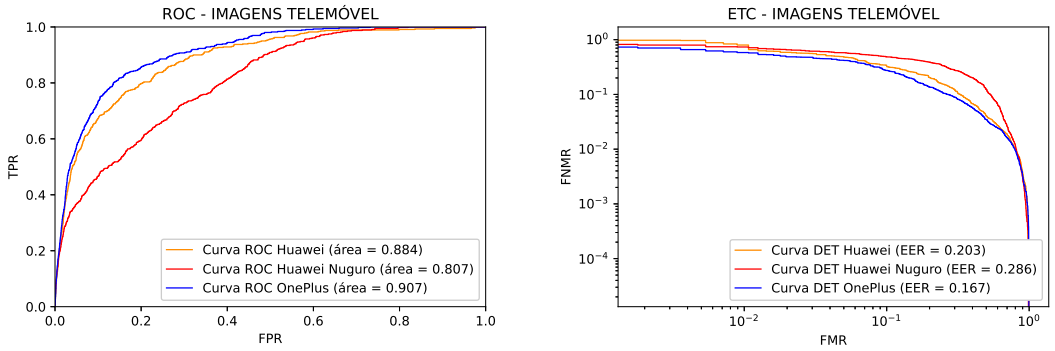

Figura 4.4: Curvas *ROC* e *DET* geradas quando são testados os diferentes tipos de imagens de telemóvel no modelo de classificação 2.1 (referido na tabela 4.1).

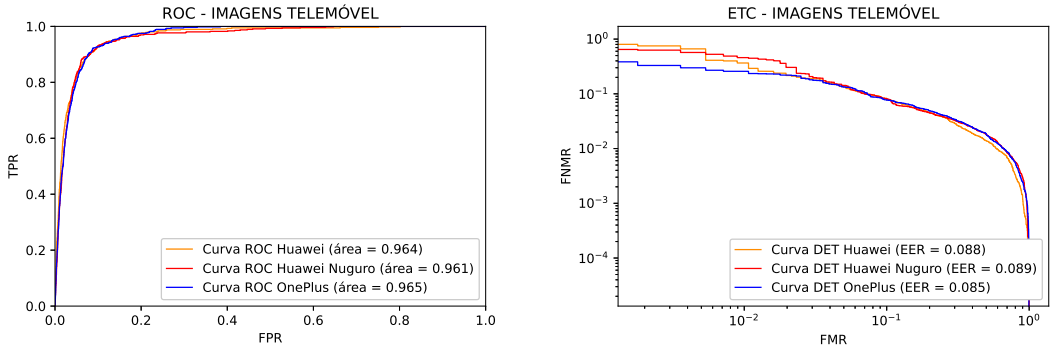

Figura 4.5: Curvas *ROC* e *DET* geradas quando são testados os diferentes tipos de imagens de telemóvel no modelo de classificação 2.2 (referido na tabela 4.1).

da curva *ROC* do *OnePlus* e, por sua vez, a diferença é aumentada para com a utilização da lente macro externa *Nuguro* no telemóvel *Huawei*. O ponto relevante neste caso será a possibilidade das imagens do *OnePlus* possuírem particularidades específicas que ofereçam a capacidade de distinguir padrões que sejam repetidos em diferentes objetos, o que é um resultado a ter em consideração em abordagens futuras.

Como aconteceu anteriormente, após a introdução dos exemplares de todos os tipos de imagens de telemóveis no treino da rede neuronal os resultados obtidos foram bastante melhores e equilibrados, comprovando mais uma vez a vantagem da introdução de variedade aos conjuntos de dados de modo a fornecer capacidade aos modelos classificadores, como é possível analisar pela figura 4.3.

4.3 Testes de Materiais

Os sistemas de classificação poderão obter diferentes resultados em função do tipo de material utilizado, devido às suas diferentes propriedades e condicionantes e é necessário entender se essas diferenças entre as suas propriedades são relevantes. Nesse sentido, e pelo que já foi abordado no capítulo anterior, foram disponibilizados três diferentes tipos de metais: prata, latão e cobre.

Treinando apenas um tipo de material, neste caso a prata, pretende-se observar o efeito de um teste com outro material não presente no treino da rede, o latão, e verificar, inicialmente, se o tipo de material pode ter relevância nos sistemas de classificação. Também é pretendido perceber se a inclusão de exemplares de outros tipos de materiais no treino da rede, influencia positivamente os resultados. Por fim, testando as imagens de cobre, o objetivo é analisar se com o aumento de exemplares de diferentes materiais no treino da rede neuronal, esta vai possuir a capacidade de reconhecer novos materiais não presentes no treino da rede.

Modelos	Materiais	Classes
1	Prata	308 (prata)
2	Prata e Latão	158 (prata) + 150 (latão)

Tabela 4.2: Descrição dos modelos de classificação treinados o teste de verificação das imagens de telemóvel.

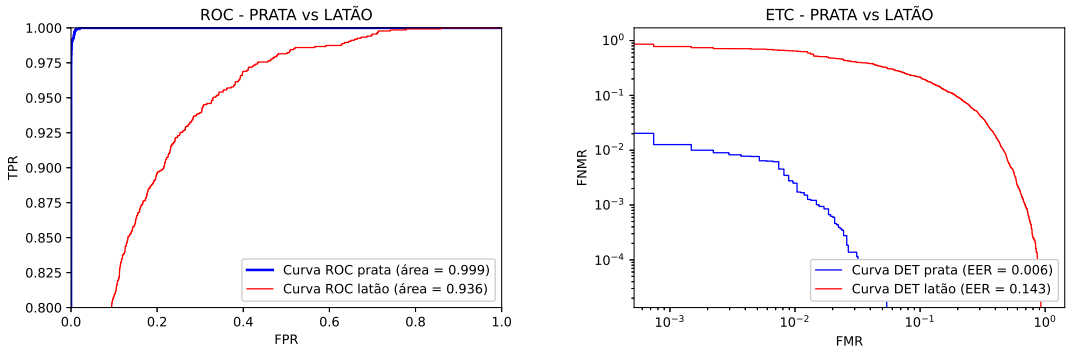

Figura 4.6: Curvas *ROC* e *DET* geradas quando são comparados os materiais prata e latão, com o modelo de classificação 1 (representado na tabela 4.2).

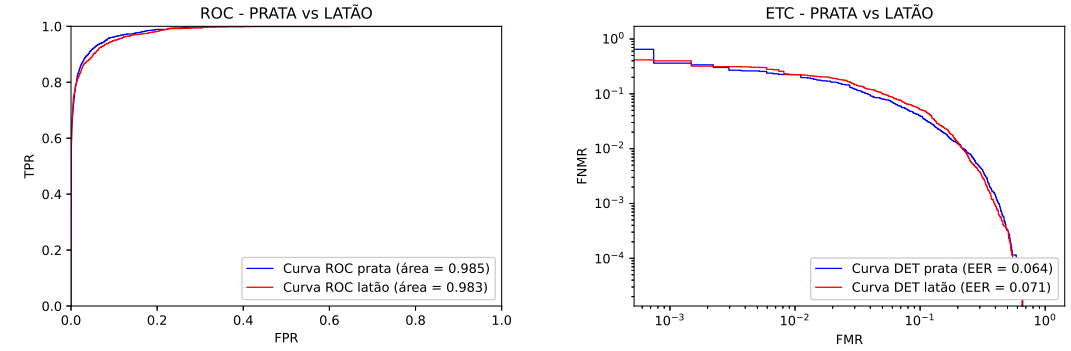

Figura 4.7: Curvas *ROC* e *DET* geradas quando são comparados os materiais prata e latão, com o modelo de classificação 2 (representado na tabela 4.2).

Esta metodologia de teste é semelhante à apresentada na secção anterior, relativa aos testes com imagens de telemóveis. Primeiramente, são testadas imagens de prata e latão num sistema de classificação que apenas utiliza imagens de prata no treino da rede. Este teste está presente na figura 4.6, onde se pode verificar que, efetivamente, a utilização de diferentes tipos de materiais

terá efeito na performance do modelo de classificação. Isto é demonstrado pelo facto da curva *ROC* das imagens de prata ser tão satisfatória que está muito próxima dos eixos e, por sua vez, as imagens de latão, quando testadas neste modelo de classificação obtêm uma grande diferença para a curva anteriormente abordada, que é vincada com a diferença presente entre os dois valores de *EER* obtidos.

Na figura 4.7, o número de imagens de prata e de latão presentes no momento do treino da rede neuronal são equivalentes, dando equilíbrio ao conjunto de imagens. Pela análise dos resultados obtidos, é possível verificar, novamente, que a variedade dos materiais presente no treino da rede tem bastante influência na performance dos modelos, quando esses mesmos materiais são testados. Este fator é comprovado pela proximidade obtida entre as duas curvas *ROC* calculadas, bem como a proximidade entre os valores de *EER*. De modo negativo, a curva *ROC* das imagens de prata sofreu alterações não desejadas, piorando a sua performance em relação ao que está representado na figura 4.7, o que poderá ser explicado com o facto de no momento de treino da rede o número de exemplares de prata utilizados ter sido reduzido para metade. Assim, uma possível solução para aumentar o poder de classificação destes modelos é o aumento de exemplares de imagens de cada material utilizado, contrariamente ao que foi realizado neste caso, pois não existiam mais exemplares de cada material. Para verificar se a solução aqui referida pode ser viável, foi realizado um novo teste, que está presente na figura 4.8.

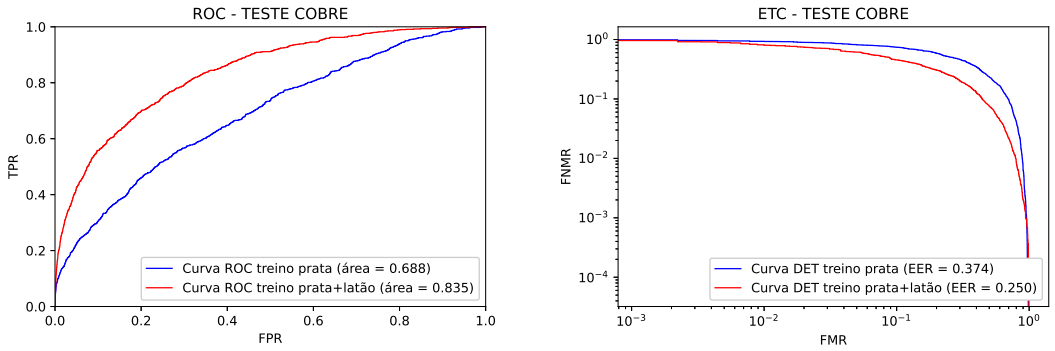

Figura 4.8: DET geradas quando as imagens de cobre são testadas em 2 modelos diferentes, um com apenas imagens de prata no treino da rede e o outro com exemplares de imagens de prata e de latão no treino da rede neuronal.

O facto de existirem apenas 20 marcações de cobre tornou-se num fator limitador à sua utilização para testes. Tornou-se útil no sentido de verificar se a variedade de materiais utilizados no treino da rede neuronal, irá melhorar o poder de classificação de materiais não presentes no treino. Especificamente, são comparados dois modelos classificadores: o primeiro apenas utiliza imagens de prata no treino da rede e o segundo utiliza imagens de prata e latão para o treino da rede, do mesmo modo que foi explicado anteriormente. Assim as mesmas imagens de cobre foram testadas nos 2 modelos diferentes e, de facto, foram verificadas alterações entre estes modelos de classificação. É possível verificar que quando apenas um tipo de material existente no treino da rede neuronal, a curva *ROC* não é satisfatória, bem como o *EER* calculado. Nesse sentido, a introdução do latão no treino da rede veio oferecer maior variedade às imagens, no que diz respeito

aos tipos de materiais utilizados e, assim, a sua introdução influenciou positivamente os resultados obtidos. Como se pode verificar na figura 4.8, a curva *ROC* melhora bastante quando é adicionada esta variedade de materiais, mostrando a sua capacidade de reconhecer materiais não utilizados no treino da rede, quando se tem em conta o acrescento de variedade de materiais aos dados treinados.

4.4 Teste com Marcações Inclinadas

Todos os tipos de materiais preciosos ou jóias apresentam particularidades morfológicas que podem condicionar, tanto o método de desenho das marcações no material, como afetar a performance dos sistemas de verificação dessas mesmas marcações. A minuciosidade presente nas marcações, quando aplicadas nos materiais, influenciam a resolução da imagem devido às variedades de profundidade causadas pelas irregularidades do material. A construção dos conjuntos de dados teve este obstáculo em conta, com a captura de imagens que simulam situações semelhantes às que foram agora abordadas. Para simular a superfície irregular, foram capturadas imagens na qual metade da marcação se encontra desfocada. Assim, foram comparadas as imagens com a simulação de inclinação e as imagens capturadas em superfícies planas, de modo a verificar se as marcações inclinadas afetam consideravelmente os resultados do modelo de classificação.

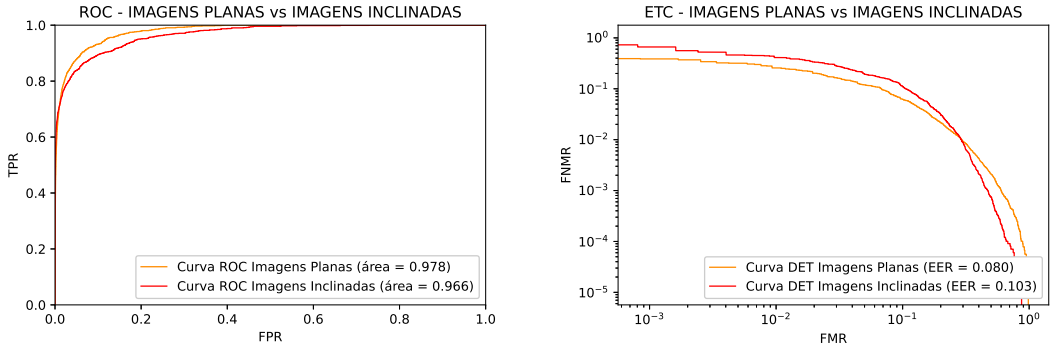

Figura 4.9: Curvas *ROC* e DET geradas quando as imagens de superfícies não planas são comparadas com imagens de superfícies planas, com a utilização de o modelo de classificação que apenas utiliza imagens de prata (de padrão único) no treino da rede neuronal.

A figura 4.9 mostra a comparação entre os dois tipos de imagens referidos na introdução deste teste. É possível verificar que, efetivamente, existem diferenças entre as duas curvas *ROC* e entre os dois valores de *EER*. Existe uma aproximação entre os resultados, sendo que as marcações em superfícies não inclinadas, como seria expectável, obtêm os resultados mais favoráveis, pois a totalidade da marcação está a ser considerada para o processo de classificação, sendo que o facto de metade da marcação estar desfocada poderia ter um efeito mais negativo. Contrariamente ao expectável, os resultados obtidos para as imagens com marcações em superfícies inclinadas são promissores, mostrando que estas não são um entrave grande ao poder de classificação dos modelos construídos, o que, a nível industrial, oferece uma grande vantagem. Ainda assim, esta diferença entre os dois tipos de imagem não será a ideal, pois é necessário que o facto de as marcações estarem inclinadas não influencie a capacidade de verificação dos sistemas. A variedade deste

tipo de imagens já é considerada dentro dos conjuntos de imagens utilizados e não mostra ser um fator determinante, neste caso, para a obtenção de melhores resultados. Uma possível solução seria aumentar a profundidade de campo dos sistemas óticos, o que não é financeiramente rentável. Nesse sentido, foi procurada uma solução no sentido de atenuar estas diferenças existentes entre os resultados obtidos.

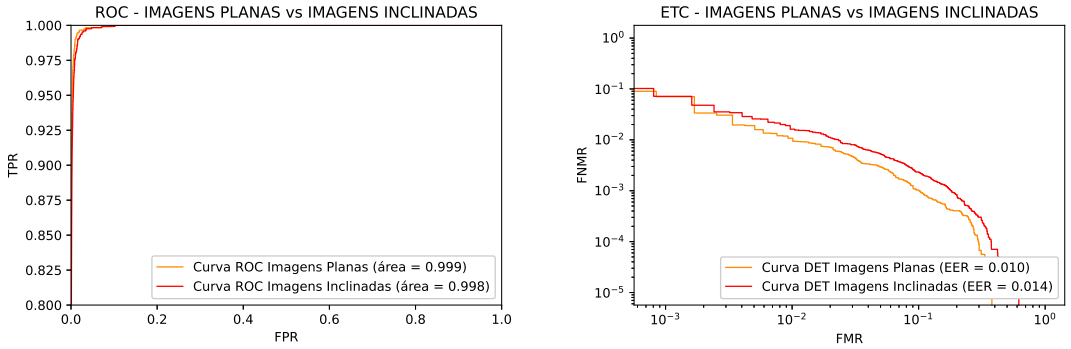

Figura 4.10: Curvas *ROC* e *DET* geradas quando as imagens de superfícies não planas são comparadas com imagens de superfícies planas, com a utilização do modelo de classificação que utiliza imagens de prata e de latão (de padrão único) no treino da rede neuronal.

Para o teste realizado na figura 4.9 o modelo de classificação que apenas utiliza imagens de prata no treino da rede foi o modelo utilizado. No caso da figura 4.10, foi utilizado o modelo de classificação 2 (representado na tabela 4.2), referente à introdução de variedade dos materiais no treino da rede neuronal. Esta utilização visa perceber se a variedade de materiais no treino da rede neuronal, pode influenciar positivamente os resultados relativos às imagens a testar, já descritas. De facto, com a utilização deste modelo, tanto as curvas *ROC* como os valores de *EER* mostraram bastantes melhorias e a diferença entre os resultados dos dois tipos de imagem foram atenuados, de modo a que se conclua que, neste caso, utilizar imagens planas ou imagens inclinadas é um fator que não provoca diferença neste sistema de classificação, o que é o ideal para uma posterior utilização destas marcações a *laser*.

4.5 Teste de Condições de Aquisição de Imagens

As diversas condições de imagens e da sua aquisição, como já abordado, foram consideradas na construção dos conjuntos de dados utilizados. Essas condicionantes foram adquiridas através do que é disponibilizado pelas funcionalidades do *Dino-Lite Microscope*, ainda que algo limitadas. Fundamentalmente, as variações introduzidas centraram-se na variação de polarização das imagens e, também, na variação dos componentes utilizados na lente microscópica que variam a condição de aquisição de imagem. Estes pontos abordados serão os objetos de avaliação, devidamente explicados nas secções seguintes.

4.5.1 Polarização

As variações entre as condições de luminosidade das imagens, em muitos casos, poderão gerar alguns casos em que certas condições serão mais favoráveis em relação a outras. Outro objetivo, de forma generalizada, é perceber se a variação das condições de luz, neste caso de polarização, tem efeitos nos resultados dos sistemas de classificação. O modelo classificador utilizado, primeiramente, é o que apenas contém imagens de prata no treino da rede neuronal. Seguidamente, foi utilizado o modelo classificador que contém imagens de prata e latão no treino da rede, no sentido de verificar se, também, a introdução de variedade de materiais no conjunto de dados, poderá colmatar falhas provocadas pelas variações de condições de luminosidade.

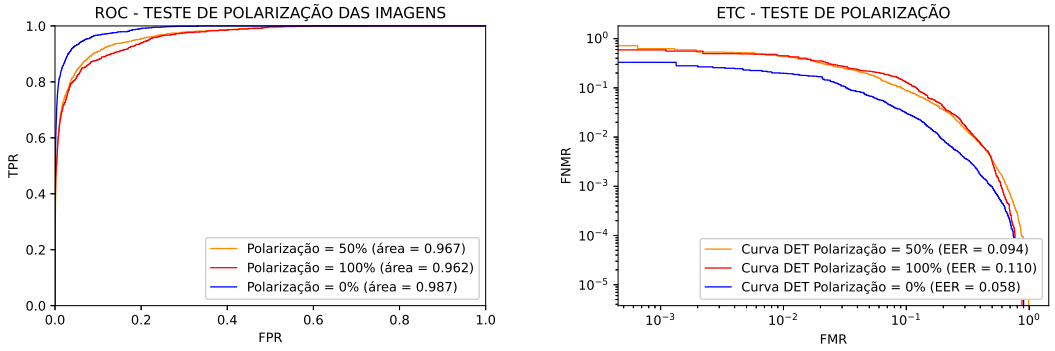

Figura 4.11: Curvas *ROC* e *DET* geradas que comparam os tipos de polarização de imagens quando aplicadas no modelo de classificação com apenas imagens de prata (de padrão único) no treino da rede neuronal.

Na figura 4.11 estão representados os testes realizados com as variações de polarização de imagem, que apresentam três níveis distintos: polarização nula, polarização a 50% e polarização no seu nível máximo (100%), sendo que estes tipos de imagens estão presentes na figura 3.9, no capítulo 3. É possível verificar a diferença existente entre as curvas *ROC* de quando a imagem não está polarizada, ao invés de quando a imagem apresenta algum nível de polarização. A partir do momento em que a imagem já possui alguma polarização, nota-se alguma proximidade entre as curvas *ROC* e entre os valores de *EER*, o que significa que o nível de polarização da imagem poderá não ser um fator relevante a considerar, mas sim o facto de a imagem estar polarizada. Como nos teste anteriores, a inclusão de imagens do tipo que se pretende testar no treino da rede neuronal se revela útil, melhorando os resultados consideravelmente, mas, neste caso, essa situação não se verifica, pois existe variedade de imagens polarizadas e não polarizadas nos conjuntos de dados construídos. Assim, é necessário procurar uma solução que possa ser viável para reduzir a diferença entre os resultados obtidos.

Com o objetivo de perceber quais as particularidades que possam colmatar as diferenças de resultados entre as diferentes condicionantes de polarização, foi realizado um teste utilizando o modelo classificador treinado com imagens de prata e latão, ou seja, foi adicionada variedade de materiais ao sistema de classificação, com o mesmo número de imagens utilizadas no modelo classificador anterior, presentes no treino da rede neuronal. Esta adição mostrou ser uma solução

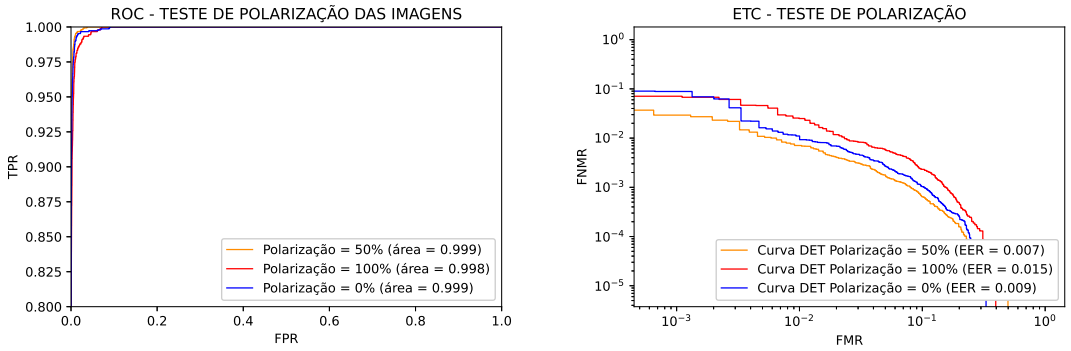

Figura 4.12: Curvas *ROC* e *DET* geradas que comparam os tipos de polarização de imagens quando aplicadas no modelo de classificação com imagens de prata e de latão (de padrão único) no treino da rede neuronal.

bastante eficaz, pois melhorou bastante os resultados de um modo geral, e extinguiu as diferenças obtidas entre as variadas condições. Estes dados, presentes na figura 4.12, mostram que tanto as curvas *ROC*, como os valores de *EER* são bastante próximos entre si e, para além disso, apresentam resultados bastante bons. Novamente, a maior diferença notada, que, ainda assim, é bastante reduzida, é a diferença entre uma imagem totalmente polarizada e as restantes imagens, o que pode significar, devido à incidência dos resultados, que a utilização de polarização de imagens, tendencialmente, não se mostra favorável.

4.5.2 Inclusão de Difusor de Luz e Direcionador de Luz

Como já foi abordado, a inclusão de componentes na lente microscópica tem o objetivo de melhorar as imagens, tanto a nível de luminosidade, como ao nível de resolução. A inclusão de luz difusa irá melhorar a imagem ao nível dos seus detalhes microscópicos, pois nesta situação a luz encontra-se espalhada em todas as direções. A utilização de um direcionador de luz também melhora a qualidade da imagem, destacando texturas e profundidades. A adição destes dois componentes, teoricamente, irá aumentar a qualidade dos detalhes das imagens e, por consequência, obter melhores resultados do que quando é apenas utilizada luz direta para adquirir imagens. Para este teste, novamente, é utilizado o modelo classificador que utiliza apenas imagens de prata no treino da rede neuronal. Similarmente ao que foi realizado no outro teste desta secção, é procurada uma solução para colmatar as diferenças que possam existir entre os resultados obtidos, utilizando o modelo de classificação com imagens de prata e de latão no treino da rede.

Como seria expectável, e pela análise da figura 4.13, a introdução dos componentes na lente microscópica obteve resultados mais promissores que quando as imagens são apenas adquiridas com recurso à luz direta do microscópio. A análise das curvas *ROC* e *DET* e dos valores de *EER* mostram a semelhança entre os resultados obtidos quando é utilizado um difusor de luz e um direcionador, com ligeira vantagem para a utilização de um difusor de luz. Este acontecimento pode dever-se ao facto de a utilização de luz difusa favorecer particularidades em superfícies rugosas microscópicas, que é um caso que se aplica ao que está a ser estudado. A utilização de luz direta é

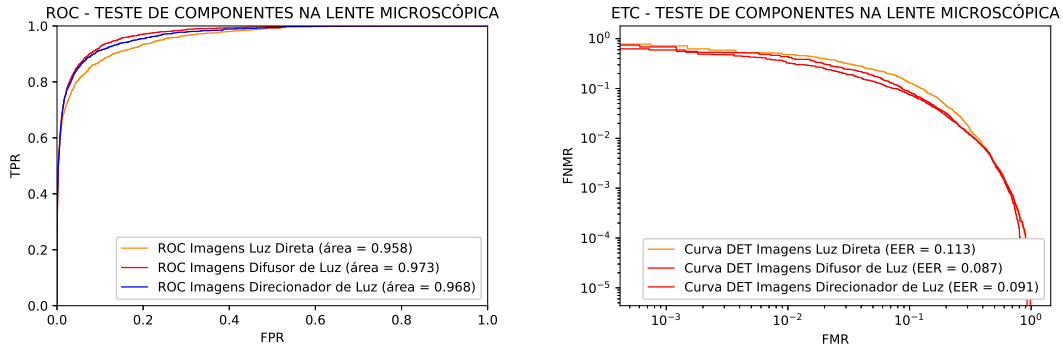

Figura 4.13: Curvas *ROC* e *DET* geradas que comparam os tipos de componentes utilizados na lente microscópica aplicados ao modelo de classificação com apenas imagens de prata (de padrão único) no treino da rede neuronal.

a opção cuja capacidade do sistema de verificação é pior. Seguidamente, um dos objetivos principais centra-se em tentar colmatar as diferenças entre os diferentes componentes, à medida que se melhoram os resultados, pois, é comprovado, novamente, que a inclusão deste tipo de imagens no treino das redes neuronais não é suficiente para reduzir essas diferenças. Então a adição de variedade de materiais ao treino da rede (prata e latão) foi, de novo, o objeto de avaliação, no sentido de compreender se tem efeitos positivos nos resultados obtidos. Esta introdução de variedade foi realizada de modo análogo ao que foi realizado anteriormente, ou seja, com a utilização do mesmo número de imagens do modelo anterior no processo de treino da rede neuronal.

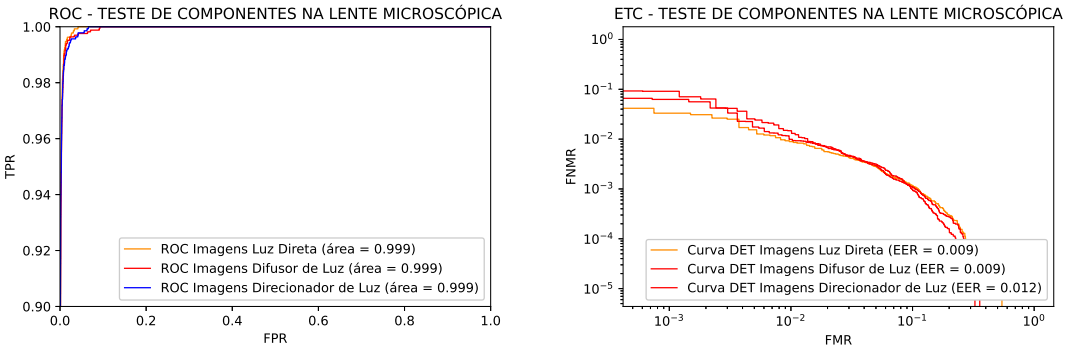

Figura 4.14: Curvas *ROC* e *DET* geradas que comparam os tipos de componentes utilizados na lente microscópica aplicados ao modelo de classificação com imagens de prata e de latão (de padrão único) no treino da rede neuronal.

Após a realização deste teste, foi reforçado o poder que a variedade de materiais no treino da rede tem quando existem diversas variações de imagens nos testes realizados. Neste caso, tanto os resultados obtidos são melhorados, como as diferenças entre os resultados são desprezáveis, pois existe uma enorme aproximação entre as três curvas *ROC* geradas e uma grande aproximação entre os três valores de *EER* calculados, presentes na figura 4.14. Assim, é possível concluir, de novo, que a variedade de materiais poderá colmatar diversas falhas relativas a diferenças existentes nas condicionantes de aquisição de imagens.

Capítulo 5

Conclusões e Trabalho Futuro

Este capítulo visa abordar as considerações finais deste documento, no sentido de analisar, de forma conclusiva, os procedimentos experimentais realizados ao longo desta dissertação. Neste trabalho foi devidamente evidenciada a novidade que são estas marcações realizadas a *laser* nos metais preciosos e esse fator leva a que inúmeras novas experiências e vertentes possam ser desenvolvidas para verificar se, efetivamente, este tipo de marcações poderá vir a ser uma solução viável para a sua utilização em sistemas de combate à contrafação. Assim, este capítulo será concluído com algumas abordagens para complementar e continuar o estudo em que este projeto se encontra inserido.

5.1 Conclusões

Toda a implementação e, posterior, trabalho experimental centrou-se unicamente na análise do comportamento de um sistema de *Deep Learning* no momento em que são introduzidas diversas variações, tanto a nível físico, como a nível de variações nas condições de aquisição das imagens. Estas verificações são realizadas no sentido de entender as suas potencialidades de industrialização e quais as condicionantes que poderão afetar, tanto positivamente, como negativamente os sistemas de verificação de imagens aplicados.

Um dos pontos a analisar neste projeto é a utilização de marcações com desenho único por objeto e de marcações com desenhos que são repetidos em diferentes objetos, pois, idealmente, quando o desenho de uma marcação é repetido noutro objeto, pode significar que esta tenha sofrido uma falsificação e é conveniente que os sistemas de classificação tenham a capacidade de reconhecer a diferenças dos mesmos desenhos determinísticos em diferentes objetos. Foi concluído que os resultados de classificação de marcações com desenhos repetidos são, naturalmente, piores em comparação com a utilização apenas de marcações com desenhos únicos, mas ainda assim, o sistema possui elevada capacidade de distinção entre marcações com desenhos repetidos (quando aumentado o tamanho do banco de dados e a sua variedade, com marcações de desenho único e repetido), o que é um bom princípio para o combate à contrafação.

É um objetivo deste projeto que o reconhecimento das imagens das marcações seja possível utilizando apenas fotografias capturadas através de um telemóvel, de modo a que a utilização deste sistema possa ser acessível ao cidadão comum, sem a necessidade de recorrer ao uso de equipamentos microscópicos. Assim, a execução de diferentes modelos serve para perceber o efeito que poderá ter uma câmara interna, com alta qualidade, em sistemas de reconhecimento. Com a inclusão interna ou externa de uma lente macro, que aumenta a qualidade da imagens ao nível dos seus pormenores, a performance do modelo classificador ressentiu-se, concluindo que a sua utilização, em modelos de classificação que são construídos com marcações únicas por objeto, não terá os efeitos desejados. Quando o modelo classificador é construído utilizando uma mistura de imagens de marcações únicas e repetidas, as imagens que foram capturadas com a utilização de uma lente macro interna à câmara do telemóvel (o modelo *OnePlus*) são as que melhor performance geraram ao modelo de classificação. Com este acontecimento é possível denotar que podem existir certas particularidades capturadas pela lente macro interna que poderão ser determinantes para proceder à classificação de marcações com desenhos repetidos em variados objetos. Outro fator a realçar, é a importância da utilização das imagens de telemóvel no treino das redes neuronais, pois foi visível a influência positiva nos resultados dos diferentes tipos de telemóvel, aumentado a performance do sistema de verificação, reduzindo a diferença da performance da rede para os diferentes tipos de câmara.

Como estamos perante jóias e metais preciosos, irão sempre existir variadas diferenças entre os diferentes materiais utilizados, no sentido de perceber se, efetivamente, estas diferenças podem ser fatores determinantes na performance dos sistemas de reconhecimento de marcações. Assim, primeiramente, verificou-se que a utilização de apenas um material no treino da rede irá prejudicar a performance dos sistemas, se outro tipo de material for testado nessa mesma rede neuronal. Quando os materiais a testar são incluídos no processo de treino da rede, o desempenho desse modelo anula as diferenças entre os dois materiais utilizados no teste. Também foi concluído que a existência de variedade de materiais no treino das redes neuronais tem influência no reconhecimento de materiais novos, não presentes nesse processo de treino.

Fisicamente, as jóias e metais preciosos apresentam superfícies não planares e, de modo a ter esse fator em conta, a construção dos conjuntos de dados simulou a existência de superfícies irregulares, desfocando metade das marcações em certos casos. Assim foi possível verificar que a diferença da performance dos modelos de reconhecimento de imagens foi melhor quando as superfícies irregulares não são consideradas, sendo que a diferença para as restantes era reduzida. Com a introdução de variedade de materiais no processo de treino da rede, tanto essa diferença ficou nula, como o desempenho do modelo de classificação melhorou para as duas opções de teste.

Todas as variantes presentes nas imagens foram os objetos propostos a avaliar nesta dissertação e as diferentes condições de imagem, tanto a nível de aquisição como a nível de luminosidade não foram esquecidas. Foi concluído que quando as imagens apresentam algum nível de polarização, a performance dos sistemas de classificação poderá sair prejudicada, obtendo melhores resultados para imagens não polarizadas. A inclusão de difusor de luz e direcionador de luz na lente microscópica também foi um ponto a considerar, devido ao facto de estes componentes, nas

suas propriedades, terem a capacidade de melhorar a qualidade da imagem e, de facto, a sua introdução surtiu o efeito desejado, mostrando resultados melhores do que quando é apenas utilizada luz direta para adquirir as imagens. Estas diferenças foram colmatadas com a introdução de variedade dos tipos de materiais que, tal como no caso anterior, mostrou ser uma opção viável para atenuar as diferenças existentes entre as diferentes condições de imagem, bem como mostrou a sua capacidade para melhorar o desempenho do modelo classificador para qualquer uma das opções.

5.2 Trabalho Futuro

O facto de as marcações a *laser* em artefactos e materiais preciosos serem uma novidade faz com que não existam, ainda, estudos realizados nesse sentido, sendo que esta dissertação é o primeiro trabalho científico relacionado com este tipo de marcações a *laser* desenvolvidas no âmbito do projeto *UniqueMark*. Este fator leva a que existam inúmeras possíveis abordagens, futuramente, de encontrar os melhores métodos e soluções, de modo a que estas marcações possam ser utilizadas, de forma viável, em sistemas de segurança e de combate à contrafação.

A utilização de apenas marcações com desenhos repetidos em diferentes objetos é dos pontos que mais importância deverá ter no futuro, pois os resultados foram bastante promissores, por isso, existe a necessidade, utilizando outras abordagens, de encontrar o melhor classificador para as marcações com desenhos repetidos, de modo a poder distinguir possíveis falsificações, bem como encontrar o modelo de classificação generalizado mais adequado para este tipo de marcações a *laser*.

Visto que apenas foram utilizados métodos de *Deep Learning* neste trabalho, o desenvolvimento de métodos convencionais de *Machine Learning* é uma abordagem interessante, sendo que pela revisão da literatura é possível verificar que podem ser boas opções. Devido à particularidade deste tipo de marcações, o desenvolvimento de um algoritmo de obtenção de caraterísticas específicas nestes desenhos determinísticos poderá ser interessante, mostrando em outros trabalhos similares as suas potencialidades, por exemplo ao nível de deteção e extração de minúcias. Para a realização de todas estas abordagens, primeiramente, seria necessária a construção de um conjunto de imagens com todas as particularidades consideradas nesta dissertação, pois, é notória a influência que a variedade de imagens nos bancos de dados tem para alcançar melhores modelos de classificação.

Bibliografia

[1] Ebtsam Adel, Mohammed Elmogy, and Hazem Elbakry. Image stitching system based on orb feature-based technique and compensation blending. *International Journal of Advanced Computer Science and Applications*, 6(9), 2015.

[2] Shivang Agarwal, Ajita Rattani, and C Ravindranath Chowdary. A comparative study on handcrafted features v/s deep features for open-set fingerprint liveness detection. *Pattern Recognition Letters*, 147:34–40, 2021.

[3] Saad Albawi, Tareq Abed Mohammed, and Saad Al-Zawi. Understanding of a convolutional neural network. In *2017 International Conference on Engineering and Technology (ICET)*, pages 1–6. Ieee, 2017.

[4] Hasimah Ali, Momoh JE Salami, et al. Iris recognition system by using support vector machines. In *2008 International Conference on Computer and Communication Engineering*, pages 516–521. IEEE, 2008.

[5] Anjali Amit. What is diffused light? `https://sciencing.com/diffused-light-5470956.html`, 2018. Accessed: 2022-01-11.

[6] Riikka Arppe and Thomas Just Sørensen. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nature Reviews Chemistry*, 1(4):1–13, 2017.

[7] Riikka Arppe-Tabbara, Mohammad Tabbara, and Thomas Just Sørensen. Versatile and validated optical authentication system based on physical unclonable functions. *ACS applied materials & interfaces*, 11(6):6475–6482, 2019.

[8] Shai Avidan. Support vector tracking. *IEEE transactions on pattern analysis and machine intelligence*, 26(8):1064–1072, 2004.

[9] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool. Surf: Speeded up robust features. In *European conference on computer vision*, pages 404–417. Springer, 2006.

[10] Sergio Bermejo and Joan Cabestany. Adaptive soft k-nearest-neighbour classifiers. *Pattern Recognition*, 33(12):1999–2005, 2000.

[11] Michael Calonder, Vincent Lepetit, Christoph Strecha, and Pascal Fua. Brief: Binary robust independent elementary features. In *European conference on computer vision*, pages 778–792. Springer, 2010.

[12] Rahul Chauhan, Kamal Kumar Ghanshala, and RC Joshi. Convolutional neural network (cnn) for image detection and recognition. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 278–282. IEEE, 2018.

[13] François Chollet. Xception: Deep learning with depthwise separable convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1251–1258, 2017.

[14] Tarang Chugh, Sunpreet S Arora, Anil K Jain, and Nicholas G Paulter. Benchmarking fingerprint minutiae extractors. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8. IEEE, 2017.

[15] Corinna Cortes and Vladimir Vapnik. Support-vector networks. *Machine learning*, 20(3):273–297, 1995.

[16] Valter Costa. Vision methods to find uniqueness within a class of objects. Master's thesis, Faculdade de Engenharia da Universidade do Porto, 2019.

[17] Antonia Creswell, Tom White, Vincent Dumoulin, Kai Arulkumaran, Biswa Sengupta, and Anil A. Bharath. Generative adversarial networks: An overview. *IEEE Signal Processing Magazine*, 35(1):53–65, 2018.

[18] Jesse Davis and Mark Goadrich. The relationship between precision-recall and roc curves. In *Proceedings of the 23rd international conference on Machine learning*, pages 233–240, 2006.

[19] Maria De Marsico, Alfredo Petrosino, and Stefano Ricciardi. Iris recognition through machine learning techniques: A survey. *Pattern Recognition Letters*, 82:106–115, 2016.

[20] Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. Arcface: Additive angular margin loss for deep face recognition. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 4690–4699, 2019.

[21] Li Deng and Dong Yu. Deep learning: methods and applications. *Foundations and trends in signal processing*, 7(3–4):197–387, 2014.

[22] Bin Ding, Huimin Qian, and Jun Zhou. Activation functions and their characteristics in deep neural networks. In *2018 Chinese control and decision conference (CCDC)*, pages 1836–1841. IEEE, 2018.

[23] Shlomi Dolev, Łukasz Krzywiecki, Nisha Panwar, and Michael Segal. Optical puf for non-forwardable vehicle authentication. *Computer Communications*, 93:52–67, 2016.

[24] AD Dongare, RR Kharde, and Amit D Kachare. Introduction to artificial neural network. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(1):189–194, 2012.

[25] Europol. 2017 situation report on counterfeiting and piracy in the european union. `https://www.europol.europa.eu/sites/default/files/documents/counterfeiting_and_piracy_in_the_european_union.pdf`. Accessed: 2022-01-12.

[26] Alessandro Farina, Zsolt M Kovacs-Vajna, and Alberto Leone. Fingerprint minutiae extraction from skeletonized binary images. *Pattern recognition*, 32(5):877–889, 1999.

[27] Martin A Fischler and Robert C Bolles. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*, 24(6):381–395, 1981.

[28] Hartwig Fronthaler, Klaus Kollreider, and Josef Bigun. Local features for enhancement and minutiae extraction in fingerprints. *IEEE Transactions on image processing*, 17(3):354–363, 2008.

[29] Yansong Gao, Said F Al-Sarawi, and Derek Abbott. Physical unclonable functions. *Nature Electronics*, 3(2):81–91, 2020.

[30] L. Paola Garcia-Perera, Juan A. Nolazco-Flores, Bhiksha Raj, and Richard Stern. Optimization of the det curve in speaker verification. In *2012 IEEE Spoken Language Technology Workshop (SLT)*, pages 318–323, 2012.

[31] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 148–160, 2002.

[32] Ikbal Gazalba, Nurul Gayatri Indah Reza, et al. Comparative analysis of k-nearest neighbor and modified k-nearest neighbor algorithm for data classification. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, pages 294–298. IEEE, 2017.

[33] Nuno Gonçalves and Leandro Cruz. Uniquemark - a method to create and authenticate a unique mark in precious metal artefacts. In *Jewelry Materials Congress*, London, UK, july 2019.

[34] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. MIT Press, 2016. `http://www.deeplearningbook.org`.

[35] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. *Advances in neural information processing systems*, 27:2672–2680, 2014.

[36] Margherita Grandini, Enrico Bagli, and Giorgio Visani. Metrics for multi-class classification: an overview. *arXiv preprint arXiv:2008.05756*, 2020.

[37] Surbhi Gupta, Munish Kumar, and Anupam Garg. Improved object recognition results using sift and orb feature detector. *Multimedia Tools and Applications*, 78(23):34157–34171, 2019.

[38] Chin-Chuan Han, Hsu-Liang Cheng, Chih-Lung Lin, and Kuo-Chin Fan. Personal authentication using palm-print features. *Pattern recognition*, 36(2):371–381, 2003.

[39] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778, 2016.

[40] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

[41] Andrew G Howard, Menglong Zhu, Bo Chen, Dmitry Kalenichenko, Weijun Wang, Tobias Weyand, Marco Andreetto, and Hartwig Adam. Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*, 2017.

[42] https://www.dino lite.com/. Dino-lite am5212ztl. `https://www.dino-lite.com/products_detail.php?index_m1_id=29&index_m2_id=30&index_id=79`. Accessed: 2022-01-14.

[43] Mahbub Hussain, Jordan J Bird, and Diego R Faria. A study on cnn transfer learning for image classification. In *UK Workshop on computational Intelligence*, pages 191–202. Springer, 2018.

[44] Rui Ishiyama, Yuta Kudo, and Toru Takahashi. midot: Micro identifier dot on things—a tiny, efficient alternative to barcodes, tags, or marking for industrial parts traceability. In *2016 IEEE International Conference on Industrial Technology (ICIT)*, pages 781–786. IEEE, 2016.

[45] Rui Ishiyama, Yoichi Nakamura, Akira Monden, Lei Huang, and Seiji Yoshimoto. Melon authentication by agri-biometrics-identifying individual fruits using a single image of rind pattern. In *International Conference on Computer Vision Theory and Applications*, volume 2, pages 698–704. SciTePress, 2012.

[46] Shambhavi Jain, BL Sunil Kumar, and Ramesha Shettigar. Comparative study on sift and surf face feature descriptors. In *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pages 200–205. IEEE, 2017.

[47] Zhang Jin-Yu, Chen Yan, and Huang Xian-Xiang. Edge detection of images based on improved sobel operator and genetic algorithms. In *2009 International Conference on Image Analysis and Signal Processing*, pages 31–35. IEEE, 2009.

[48] Nikhil Ketkar and Eder Santana. *Deep learning with Python*, volume 1. Springer, 2017.

[49] JINHO Kim[1], BS Kim, and Silvio Savarese. Comparing image classification methods: K-nearest-neighbor and support-vector-machines. In *Proceedings of the 6th WSEAS international conference on Computer Engineering and Applications, and Proceedings of the 2012 American conference on Applied Mathematics*, volume 1001, pages 48109–2122, 2012.

[50] M Manoj Krishna, M Neelima, M Harshali, and M Venu Gopala Rao. Image classification using deep learning. *International Journal of Engineering & Technology*, 7(2.7):614–617, 2018.

[51] CL Li and Kin Chuen Hui. Feature recognition by template matching. *Computers & Graphics*, 24(4):569–582, 2000.

[52] David G Lowe. Object recognition from local scale-invariant features. In *Proceedings of the seventh IEEE international conference on computer vision*, volume 2, pages 1150–1157. Ieee, 1999.

[53] Roel Maes and Ingrid Verbauwhede. Physically unclonable functions: A study on the state of the art and future research directions. In *Towards Hardware-Intrinsic Security*, pages 3–37. Springer, 2010.

[54] Pedro Marcelino. 90transfer learning from pre-trained models. `https://towardsdatascience.com/transfer-learning-from-pre-trained-models-f2393f124751`. Accessed: 2022-01-11.

[55] Alvin Martin, George Doddington, Terri Kamm, Mark Ordowski, and Mark Przybocki. The det curve in assessment of detection task performance. Technical report, National Inst of Standards and Technology Gaithersburg MD, 1997.

[56] Agnieszka Mikołajczyk and Michał Grochowski. Data augmentation for improving deep learning in image classification problem. In *2018 international interdisciplinary PhD workshop (IIPhDW)*, pages 117–122. IEEE, 2018.

[57] Shervin Minaee and Amirali Abdolrashidi. Deepiris: Iris recognition using a deep learning approach. *arXiv preprint arXiv:1907.09380*, 2019.

[58] Sarang Narkhede. Understanding auc - roc curve, Jun 2021.

[59] Michael A Nielsen. *Neural networks and deep learning*, volume 25. Determination press San Francisco, CA, 2015.

[60] Keiron O'Shea and Ryan Nash. An introduction to convolutional neural networks. *arXiv preprint arXiv:1511.08458*, 2015.

[61] Bhavesh Pandya, Georgina Cosma, Ali A Alani, Aboozar Taherkhani, Vinayak Bharadi, and TM McGinnity. Fingerprint classification using a deep convolutional neural network. In *2018 4th International Conference on Information Management (ICIM)*, pages 86–91. IEEE, 2018.

[62] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002.

[63] Dabal Pedamonti. Comparison of non-linear activation functions for deep neural networks on mnist classification task. *arXiv preprint arXiv:1804.02763*, 2018.

[64] physicsclassroom.com. Polarization. `https://www.physicsclassroom.com/class/light/Lesson-1/Polarization`. Accessed: 2022-01-11.

[65] Yutthana Pititheeraphab, Nuntachai Thongpance, Hisayuki Aoyama, and Chuchart Pintavirooj. Vein pattern verification and identification based on local geometric invariants constructed from minutia points and augmented with barcoded local feature. *Applied Sciences*, 10(9):3192, 2020.

[66] Nalini K Ratha, Shaoyun Chen, and Anil K Jain. Adaptive flow orientation-based feature extraction in fingerprint images. *Pattern Recognition*, 28(11):1657–1672, 1995.

[67] Waseem Rawat and Zenghui Wang. Deep convolutional neural networks for image classification: A comprehensive review. *Neural Computation*, 29(9):2352–2449, 2017.

[68] Beanbonyka Rim, Junseob Kim, and Min Hong. Fingerprint classification using deep learning approach. *Multimedia Tools and Applications*, 80(28):35809–35825, 2021.

[69] Edward Rosten and Tom Drummond. Machine learning for high-speed corner detection. In *European conference on computer vision*, pages 430–443. Springer, 2006.

[70] Ethan Rublee, Vincent Rabaud, Kurt Konolige, and Gary Bradski. Orb: An efficient alternative to sift or surf. In *2011 International conference on computer vision*, pages 2564–2571. Ieee, 2011.

[71] Ulrich Rührmair, Christian Hilgers, Sebastian Urban, Agnes Weiershäuser, Elias Dinter, Brigitte Forster, and Christian Jirauschek. Optical pufs reloaded. *Eprint. Iacr. Org*, 2013.

[72] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, et al. Imagenet large scale visual recognition challenge. *International journal of computer vision*, 115(3):211–252, 2015.

[73] Amazon Web Services. *Amazon Machine Learning - Developer Guide*, volume 1. Amazon Web Services, 2016. `https://docs.aws.amazon.com/machine-learning/latest/dg/what-is-amazon-machine-learning.html`.

[74] Pramila P Shinde and Seema Shah. A review of machine learning and deep learning applications. In *2018 Fourth international conference on computing communication control and automation (ICCUBEA)*, pages 1–6. IEEE, 2018.

[75] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.

[76] Nitish Srivastava, Geoffrey Hinton, Alex Krizhevsky, Ilya Sutskever, and Ruslan Salakhutdinov. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1):1929–1958, 2014.

[77] Matthew Stewart. Simple introduction to convolutional neural networks. *Towards Data Science*, 27, 2019.

[78] Mala Sundaram, Ambika Mani, and S Ramakrishnan. *Face recognition: demystification of multifarious aspect in evaluation metrics*. Intech, 2016.

[79] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2818–2826, 2016.

[80] Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. Deepface: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2014.

[81] Toru Takahashi and Rui Ishiyama. Fibar: Fingerprint imaging by binary angular reflection for individual identification of metal parts. In *2014 fifth international conference on emerging security technologies*, pages 46–51. IEEE, 2014.

[82] Shaharyar Ahmed Khan Tareen and Zahra Saleem. A comparative analysis of sift, surf, kaze, akaze, orb, and brisk. In *2018 International conference on computing, mathematics and engineering technologies (iCoMET)*, pages 1–10. IEEE, 2018.

[83] Debora Testi, Cinzia Zannoni, Angelo Cappello, and Marco Viceconti. Border-tracing algorithm implementation for the femoral geometry reconstruction. *Computer methods and programs in biomedicine*, 65(3):175–182, 2001.

[84] P Thamilselvana and JGR Sathiaseelan. A comparative study of data mining algorithms for image classification. *Int. J. Educ. Manage. Eng*, 5:1–9, 2015.

[85] Alaa Tharwat. Classification assessment methods. *Applied Computing and Informatics*, 2020.

[86] Kamlesh Tiwari, Gunakesh Tiwari, and Phalguni Gupta. Extraction of high confidence minutiae points from fingerprint images. In *2015 International Conference on Computer and Computational Sciences (ICCCS)*, pages 238–243. IEEE, 2015.

[87] João Francisco Gomes Tremoço. *Improving deep learning face recognition for ID and travel document applications with quality assessment*. PhD thesis, Universidade de Coimbra, 2021.

[88] M Krishna Satya Varma, NKK Rao, KK Raju, and GPS Varma. Pixel-based classification using support vector machine classifier. In *2016 IEEE 6th International Conference on Advanced Computing (IACC)*, pages 51–55. IEEE, 2016.

Apêndice

Como referido anteriormente, nesta secção é apresentado o artigo científico submetido à *International Conference in Image Processing*. O artigo encontra-se na página seguinte.

AUTHENTICATION OF LASER ASSAY MARKINGS OF PRECIOUS METAL ARTEFACTS USING DEEP LEARNING

António Madaleno[⋆†] *Andoni Santos*[⋆] *Nuno Gonçalves*[†]

[⋆] University of Coimbra, Institute of Systems and Robotics, Coimbra, Portugal
[†]INCM Lab - Portuguese Mint and Official Printing Office, Lisbon, Portugal
{antonio.madaleno,andoni.santos}@isr.uc.pt nunogon@deec.uc.pt

ABSTRACT

The project UniqueMark aims at creating a system to provide precious metal artefacts with a unique, unclonable and irreproducible assay marking, and at building a system for the validation of their authenticity. Markings are engraved in the metal surface using a laser beam and have approximately 1 mm width. Artificial neural networks are the approach used to create classification models and the image classification process is carried out using a 1-to-1 verification system. This paper presents a deep learning approach based on a Resnet50 network. Extensive experiments underwent different variations of conditions and image acquisition devices (microscopes and smartphone cameras are tested), both at the time of training and in the testing process, represented in the created dataset, which has 9490 images. The proposed network is able to accurately distinguish different markings in different conditions, as so considered as a fingerprint of the artefact, useful for anti-counterfeiting of artefacts of precious metals.

***Index Terms*—** Assay Markings; Physical Unclonable Functions; Authentication System; Deep Learning; Anti-counterfeiting.

1. INTRODUCTION

Jewels, particularly those made from precious metals, and many times enriched by gems, are high-valued objects that for long have been exhibited by humans as a demonstration of wealth. Long ago sovereignty has identified the necessity to secure the value of precious metal artefacts in general, particularly of jewels, mainly to protect the manufactures and the purchasers. This necessity arose more than a century ago due to a high pressure on the accurate validation of these objects. In Portugal, the Assay Office, which is part of the Portuguese Mint and Official Printing Office, started its hallmarking activity about 125 years ago, being one the oldest in the world [1]. Small assay markings of 1 or 2 mm side are added to be objects legally stating the metal and its fineness or purity too.

Traditional centennial hallmarks are no longer the solution for the counterfeiting problem since forgers are more and more technologically sophisticated and able to produce fake markings with very high quality. The ideal solution is to provide the object with a unique unclonable identifier. In this regards, in 2018 the UniqueMark project have created a system to provide an object with a unique unclonable mark applied to precious metal artefacts [1]. Firstly, the unique mark can be created by punching a small portion of diamond particles on the artefact surface which is, in practice, irreproducible since the exact dispersion of the particles results from a random chaotic process [2]. Secondly, an alternative process for creating an irreproducible mark can be achieved by marking the artefact with a laser in a deterministic path described by a proper mathematical form [3]. Experiments clearly show that the repetition of the same deterministic path will produce random effects due to melting on the surface and consequently, achieving a irreproducible laser mark.

In this paper, we present a deep learning authentication system for the recognition of markings, particularly solving the 1-to-1 verification problem of laser markings in precious metal artefacts. The classification model is built using a Resnet50 [4] and trained with a new dataset acquired within this project.

The dataset itself has 9490 images of 949 different markings in silver, copper and brass metal plaques. The images were acquired using a digital microscope and also three different mobile phones and in different light conditions.

Extensive experiments were then performed to improve the accuracy of the verification of markings and comprehensive ablation studies were also performed.

Finally, the main contributions of this paper are threefold: (1) the first deep learning authentication system for the verification of laser markings in metal artefacts, (2) the study of several conditions for the acquisition of images to enhance the authentication system and (3) the building of a dataset of laser markings which can also be used in further studies.

2. RELATED WORK

As far as the authors know, there is no literature work related to the authentication of laser markings in metals. As such, in

this section we will present related work regarding different perspectives of the UniqueMark project.

A highly effective solution for combating counterfeiting is to tag products that require protection. However, some of the simplest anti-counterfeiting measures prove not to be the most effective, with gaps detrimental to product security [5]. Tech creation of randomly generated characteristics that are intrinsic to the product to identify objects efficiently has become a viable solution in recent decades, accompanied by the development of physical unclonable functions (PUF) [6].

PUFs can exist in at least two ways. Either it can be introduced at the time of the material's manufacture or it can be intrinsic to the material, such as the human fingerprints [7]. An example of how this product authentication methodology works divides PUFs into two main applications: 1) low-cost authentication; 2) security key generation. The two applications mentioned are described as "strong PUF", typically used for authentication, and "weak PUF" when used for the generation and storage of a security key [8]. As a rule, the input of a PUF system is called a challenge and the output is called a response. The terminology used for these cases is challenge-response pair (CRP), and the relationship between challenge and response is measured based on the behaviour of the CRP [6]. Toru Takahashi et al. presented a method to classify metallic materials using their characteristics (intrinsic PUFs) [9]. In this work the authors proposed a method that uses metal characteristics as intrinsic fingerprints for identification, called FIBAR, Fingerprint Imaging by Binary Angular Reflection for Individual Identification of Metal Parts. Due to specular reflection, there is some instability in capturing the imaging features of the metal surfaces, so previous methods required special imaging devices to capture them. The FIBAR method, using a common camera, can capture repeatable features on metal surfaces. For instance, to capture images using a smartphone with this technique only requires a diffuser, a macro lens and a black absorber ring, which can be 3D printed. The captured image is the angular pattern of black/white intensity reflected in the metal. Image registration and identification processes are performed using conventional methods. This technique showed positive results to recognise different metals with numerous similarities.

Although FIBAR can be used to authenticate metal artefacts, it is important to notice that there is a key difference to UniqueMark, since FIBAR cannot be used to distinguish between two objects of the same metal and UniqueMark markings are used exactly to distinguish individual objects.

3. METHODOLOGY

In this section we will characterising the laser markings produced by the UniqueMark technology. Then we will present the dataset built to test our technology and finally the deep learning model used to classify the marking identities is described.

3.1. Laser Assay Markings

Laser markings for metal artefacts are relatively new, when compared to punched markings. Rather than being faster and cheaper, they present one key advantage which is the fact that it favours the assay markings of more fragile materials, avoiding the physical impact of the punching process. The laser markings of the UniqueMark, so considered as PUFs, exhibit anti-counterfeiting properties due to the following facts [1]: (1) each path taken by the laser is distinctive, creating a unique pattern; (2) it is virtually impossible to recover, or estimate with high accuracy the laser path by observing the marking; (3) reproducing the same laser path on different objects will produce distinct assay markings since local melting effects are unpredictable and this physical process is chaotic and uncontrollable. Figure 1 shows an example of a laser deterministic path and the created laser marking in a brass metal plaque. The markings used in this work fit in a 1 mm wide square.

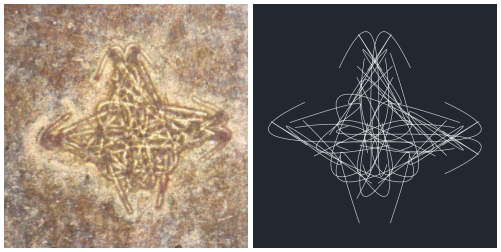

Fig. 1. Example of a laser marking on a brass metal plaque and its specific deterministic drawing.

3.2. Dataset

To construct and train a deep learning model for the verification and recognition of assay markings, a new dataset was built, being divided in two parts:

Brass and Copper Dataset. This dataset is built entirely from images acquired with a digital microscope. The microscope used was the Dino-Lite Edge Digital Microscope coupled with DinoCapture 2.0 software, and lens is placed and stabilised through a microscope base. The number of produced assay markings (classes) was 200, with 180 engraved in brass and the remaining 20 in copper. There are ten images per class which makes a total of 2000 images. The 10 images of each class were acquired in 10 different lighting conditions, using a light diffuser and a sidelight cap to make variations on the incident and reflected light.

Silver Dataset. Similar to what was described in the previous dataset, this one has very similar characteristics in terms of image acquisition conditions. The difference is the use of different smartphones to acquire part of the images. Three different devices were used: (1) Huawei P40 Pro, which has an internal camera without a macro lens; (2) Huawei P40 Pro

equipped with a Nuguro Micro external macro lens; (3) OnePlus 8 Pro, which has an inner macro lens. This dataset has only silver images, with 749 classes and ten images per class. Of those ten images per class, seven are captured through a microscope, and the remaining three are taken through smartphones. Regarding the uniqueness of the marking we can split this dataset in two parts:

Uniquely Marked Drawings: Assay markings whose deterministic draw is unique per object, with each pattern corresponding to a single class. For this case, there are 344 classes;

Repeated Marked Drawings: Assay markings with the same deterministic drawing are used on different objects. In this case, there are 45 deterministic drawings marked on ten different objects, so there are 450 classes. Notice that from these 450 classes, 45 are also counted for in the previous set of uniquely marked drawings.

3.3. Assay Markings Recognition

To recognise assay markings we train deep convolutional neural networks via classification task. As a backbone architecture we choose ResNet50 [4] due to its low size within the ResNet family (98MB) and suitability for real-time mobile applications. We initialise the network with the weights, which are pretrained on the ImageNet dataset [10] and train it with the SGD optimiser (learning rate = 0.01) and Softmax loss function for 30 epochs:

$$L_{softmax} = \frac{1}{N}\sum_{i}^{N} -\log(\frac{e^{w_{y_i}^T x_i}}{\sum_j^C e^{w_j^T x_i}}), \quad (1)$$

where C is the number of classes (depends on the protocol), y_i is the index of the class of the $i-th$ sample, N is the number of samples in a batch (32 in our work), $\mathbf{w_j}$ are the weights of classification layer. Disctiminative features $\mathbf{x_i}$ are enclosed in the penultimate network layer. The similarity of two markings is computed as the dot product between their corresponding feature vectors. To estimate the performance of the model in different scenarios (including unseen data) we perform 1-1 verification tests.

4. EXPERIMENTS AND RESULTS

With the image variations present in the constructed datasets, several test protocols were developed to evaluate these same variations. In general, the following test protocols were performed: (1) analysis of the effect of assay markings with repeated drawing on different objects on the classifier model; (2) analysis of the verification system's ability when images from smartphones with different camera characteristics are tested; (3) analysis of the effect on the classification model for different types of metal. Protocol 1 is the main result of this work, while protocols 2 and 3 are ablation studies to increase the knowledge on the authentication of these assay markings. To evaluate the performance of the authentication system, we used two distinct metrics [11]: (1) AUC - Area Under the Curve; (2) EER - Equal Error Rate.

Protocol 1 - Verification of assay markings with unique versus repeated drawings. This test aims to analyse the differences between introducing one unique assay marking drawing per object, and replicating it on different objects to check the behaviour of a verification system given these two variants. The datasets are divided into three: (1) assay markings with a unique drawing; (2) assay markings with repeated drawing; (3) using both. These may be useful in understanding whether a verification system has the ability to classify assay markings as unique, as a measure against forged or counterfeited markings.

Assay Markings Uniqueness	AUC	EER
Unique Drawing	99.7%	0.027
Repeated Drawing	70.4%	0.340
All together	96.4%	0.083

Table 1. Performance results in the verification test in assay markings with unique and repeated drawing.

Table 1 presents the AUC and EER for the protocol 1 experiments. It can be concluded that the model using only assay markings with unique drawing offer the best results because, as expected, with a single deterministic drawing per marking, there is a more straightforward distinction between the assay markings. In turn, when only markings with repeated drawing are used, the classification model has much worse results. When both types of assay markings are used to train the neural network, there is a considerable improvement in the distinction between the repeated drawings. This result is of key importance to the application of this verification system for authentication purposes, since it shows that even if a forger could reconstruct one deterministic drawing and repeat it in a laser marking, the system would have high ability to detect it as a distinct marking and, thus, detect the attack.

Protocol 2 - Verification test with different smartphone camera. One of the main points of this project is the use of images captured with smartphones to distinguish between different assay markings. The three smartphones models used are referred in the section 3.2. The smartphone images were compared to all microscope images in the verification protocol. Only assay markings with a unique drawing per object were used. The first network was trained with only microscope images, and the second training was performed using both microscope and smartphone images.

Table 2 presents the results of protocol 2. When the training process only used microscope images, one would expect that images obtained through a macro lens (internal

	Train: M		Train: M + S	
Models	**AUC**	**EER**	**AUC**	**EER**
Huawei	96.4%	0.092	99.8%	0.021
Huawei+Nuguro	91.8%	0.165	99.5%	0.043
OnePlus	94.0%	0.148	99.5%	0.037

Table 2. Performance results in the verification test with smartphone images. Firstly, the training process only uses microscope images (M), and, secondly, uses both microscope (M) and smartphone images (S).

or external) would have better results. However, this did not occur and surprisingly the better results were obtained with a smartphone regular lens. Distortions of the images caused by macro lenses and image quality that are extremely sensitive to the smartphone's stability, may explain the poorer results from this type of lenses. As it is also shown in Table 2, with the introduction of images from different smartphone cameras in the training process, the results considerably improved. In this case, there are no major differences between the three tested models, suggesting that introducing a variety of smartphone images into the images used in the training is a key factor to improve the results.

Protocol 3 - Verification test with different types of metal. In this work, we also want to evaluate if the classification performance depends on the material type. To study this dependency, three different metals are used: silver, brass, and copper.

	Train: Silver		Train: Silver+Brass	
Materials	**AUC**	**EER**	**AUC**	**EER**
Brass	93.6%	0.143	98.3%	0.071
Silver	99.9%	0.006	98.5%	0.064

Table 3. Performance results in the verification test with two different materials. Firstly, the training process only uses images from silver objects, and, secondly, uses images from silver and brass objects.

As can be seen Table 3, when the classifier model only uses images from silver objects in its training process, there are clear differences when testing the different materials, with markings in brass obtaining worse results. On the other hand, as can be seen in Table 3, using both materials in the training process had the expected effect. There is the same number of silver and brass classes in this test in the training. The difference between the two metals is small, and the classification ability of the model is slightly worse in the silver results. This could be solved by introducing more images in the training.

Finally, we want to understand whether increasing the types of materials gives the classification model the ability to classify materials not present in training. In Table 4, it can be seen that this factor is confirmed, as the results, using copper images, improve when there are more types of materials in the training.

	Test: Copper	
Train	**AUC**	**EER**
Silver	68.8%	0.374
Brass+Silver	83.5%	0.250

Table 4. Performance results in the verification test with copper images, comparing the training process only with silver images with the training process with silver and brass images.

5. CONCLUSIONS

In this paper, we constructed a deep learning model to authenticate laser assay markings and to investigate the variables that can influence the model's performance. These variables are tested to understand the potential for laser markings industrialisation, and which constraints could positively and negatively affect the applied images in verification systems.

This work has shown the importance of the variety of images in the datasets used in the training process to predict all the possibilities of image types that a user might present to the authentication system. To summarise, the classification results of assay markings with repeated drawings are worse when compared to the results of assay markings with unique drawings. Nevertheless, the system has high ability to distinguish between assay markings with repeated drawings, which is a critical property for fighting counterfeiting. When smartphone images are used for testing, we showed that using a macro lens for these assay markings does not improve results, possibly due to the difficult stabilisation of the lens. Still, if each type of image is represented in the network training, there are no differences between using a macro lens or a normal lens on smartphones. Regarding the use of different types of materials, we concluded that it affects the results of the classification models, which can be improved when the type of material to be tested is introduced in the training. Finally, we also conclude that the greater the variety of materials, the greater the ability of the verification system to classify unseen materials.

To conclude, this first deep learning model to authenticate the precious metals has proved to be an accurate system for tagging artefacts of precious metals. As UniqueMark laser assay markings are new, we expect that our dataset can help future research projects to evolve in the recognition of markings and fighting against counterfeiting.

As a future perspective, we expect to research an optimised classifier authentication of metals, and also building a model that ensures that assay markings with repeated drawings are even better recognised. We also expect to extend the existing dataset with more assay markings and with a wider variety of parameters to help future research projects.

6. REFERENCES

[1] Nuno Gonçalves and Leandro Cruz, "Uniquemark - a method to create and authenticate a unique mark in precious metal artefacts," in *Jewelry Materials Congress*, London, UK, july 2019.

[2] Nuno Gonçalves, Bruno Patrão, Leandro Cruz, João Barreto, João Duarte, Renato Monteiro, João Dias, and Albano Cavaleiro, "Patent EP3810432A1 (WO2019244081 (A1)). a method for providing and object with a unique mark. applicants: University of Coimbra and Imprensa Nacional Casa da Moeda.," Publication date: April 2021. Priority date: 2019-june-19.

[3] Nuno Gonçalves, Ricardo Barata, Bruno Patrão, and Leandro Cruz, "Patent EP3846107 (A1) (WO2020046155 (A1)). method for enhancing the security level of an object by means of a deterministic design, object with enhanced security level and method, computing device, computer programs, reading means and apparatus adapted for the preparation of the object. applicants: University of Coimbra and Imprensa Nacional Casa da Moeda.," Publication date: Mar 2020. Priority date: 2019-aug-30.

[4] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[5] Riikka Arppe and Thomas Just Sørensen, "Physical unclonable functions generated through chemical methods for anti-counterfeiting," *Nature Reviews Chemistry*, vol. 1, no. 4, pp. 1–13, 2017.

[6] Roel Maes and Ingrid Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, pp. 3–37. Springer, 2010.

[7] Yansong Gao, Said F Al-Sarawi, and Derek Abbott, "Physical unclonable functions," *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.

[8] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[9] Toru Takahashi and Rui Ishiyama, "Fibar: Fingerprint imaging by binary angular reflection for individual identification of metal parts," in *2014 fifth international conference on emerging security technologies*. IEEE, 2014, pp. 46–51.

[10] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, et al., "Imagenet large scale visual recognition challenge," *International journal of computer vision*, vol. 115, no. 3, pp. 211–252, 2015.

[11] Mala Sundaram and Ambika Mani, *Face recognition: demystification of multifarious aspect in evaluation metrics*, Intech, 2016.