O papel do perito na análise documentoscópica de documentos digitais: estudo de casos

The role of the expert in the document analysis of digital documents: case studies

Lívia Fernandes Santos[I]
Kelly Carla Almeida de Souza Borges[I]
Ana Claudia Lednik[I]
Marina de Assis Moura Navarro[I]
[I] Polícia Civil do Estado do Rio de Janeiro, RJ, Brasil

Resumo
Com a evolução tecnológica e aceleração do uso de documentos digitais, substituindo gradativamente os documentos físicos, as formas de análise documentoscópica têm sido alteradas. Os elementos de segurança gráfica dão lugar a certificados digitais e documentos com códigos de verificação via internet. Neste contexto, nos indagamos qual será o papel da perícia documentoscópica nesse novo mundo digital. Buscando responder a este questionamento, é feito um levantamento do cenário atual, mostrando a evolução das formas de autenticação das informações, e uma análise dos possíveis meios documentoscópicos de atestar a falsidade dos documentos digitais. Para tal, são apresentados estudos de casos de perícias reais realizadas no Serviço de Perícias de Documentos (SPD) do Instituto de Criminalística Carlos Éboli da Secretaria de Estado de Polícia Civil do Rio de Janeiro, em que, utilizando como ferramenta apenas a ampliação, buscou-se detectar vestígios de montagens em documentos de origem digital. Os resultados encontrados mostram que é possível aplicar os conceitos de documentoscopia para atestar a falsidade de documentos desta natureza.
Palavras-chave: documentoscopia; alterações materiais; alterações digitais; fraudes; detecção de montagens.

Abstract
With the technological evolution and acceleration of the use of digital documents, gradually replacing physical documents, the forms of document analysis have been changing. Graphic security elements give way to digital certificates and documents with verification codes via the Internet. In this context, we ask ourselves what will be the role of document analysis in this new digital world. Seeking to answer this question, a survey of the current document scenario is made, showing the evolution of the forms of information authentication, and an analysis of the possible document analysis means of attesting the falsity of digital documents. To this end, case studies of real expert analysis carried out at the Document Analysis Service (SPD) of the Carlos Éboli Criminalistics Institute of the State Secretariat of Civil Police of Rio de Janeiro are presented, in which, using only magnification as a tool, the aim was to detect traces of montages in documents of digital origin. The results found show that it is possible to apply the concepts of document analysis to attest the falsity of documents of this nature.
Keywords: documentscopy; material alterations; digital alterations; fraud; fraud detection.

Introdução

O mundo está cada vez mais informatizado, o que tem alterado profundamente as atividades humanas, sejam elas sociais ou profissionais. O desenvolvimento de tecnologias mais avançadas proporciona agilidade nos processos e aumento da produtividade. Em vista disso, as empresas têm migrado suas atividades para o meio digital, como, por exemplo, através da utilização de assinaturas eletrônicas em seus contratos e armazenamento de documentos apenas em arquivos digitais. Os órgãos públicos também passaram a seguir esta tendência, modernizando a emissão de documentos oficiais e disponibilizando-os em formato eletrônico, como a Carteira Nacional de Habilitação (CNH), Título de Eleitor, CPF, Carteira de Trabalho e documentos veiculares.

O Poder Judiciário, com o objetivo de trazer maior celeridade à tramitação dos processos, também tem avançado na informatização e, atualmente, dispõe sistemas de processos eletrônicos instituídos pela Lei nº 11.419/2006, nos quais todas as peças estão digitalizadas (inclusive as provas documentais) ou são geradas diretamente em meio eletrônico (Oliveira, 2020).

Considerando o cenário atual, em que os documentos físicos vêm sendo paulatinamente substituídos por versões eletrônicas, podemos nos questionar qual será o papel da perícia documentoscópica. Quais serão os exames realizados pelos peritos especialistas em documentos? Quais técnicas de análise deverão ser desenvolvidas ou aperfeiçoadas? Tais pontos são indagações que necessitam de reflexão, tendo em vista a necessidade de atualização de conhecimento do profissional forense.

Na mesma medida que os sistemas empresariais e os órgãos públicos se informatizam, o acesso dos falsários a softwares de edição de imagens (como Adobe Photoshop e CorelDRAW), a scanners de alta resolução e impressoras de qualidade se amplia. Isso torna a manipulação de documentos mais fácil e barata do que nunca (James; Gupta; Raviv, 2020), e modifica drasticamente a natureza e o *modus operandi* dos crimes de colarinho branco.

Uma imagem de documento pode ser facilmente manipulada, apagando-se detalhes, cortando, copiando ou colando novas informações (Deringas, 2001), o que permite que criminosos produzam todo o tipo de documentos falsos, com ou sem assinaturas, como contratos, diplomas, certificados, notas fiscais e até documentos de identificação, muitas vezes deixando poucos vestígios.

Assim, pode-se considerar que a principal demanda atual da perícia documentoscópica, em exames envolvendo documentos submetidos a algum processo digital, consiste na identificação de alterações ou montagens. Esses documentos abrangem: (i) os gerados eletronicamente e apresentados em formato digital; (ii) a versão impressa de documentos nato-digitais; (iii) os documentos digitalizados; e (iv) as cópias resultantes dessas digitalizações.

Alguns autores apresentaram estudos de técnicas para detecção de alterações em documentos digitais baseadas na observação do perito. Um exemplo é Deringas (2001), que mostrou um estudo de caso envolvendo o confronto entre uma fotocópia e o suposto documento original, procurando encontrar evidências de manipulação digital, diferenciando-as de alterações produzidas "à mão".

Saini e Kaur (2016), por sua vez, apresentaram estudo de casos controlados em que manipulações digitais realizadas por softwares como Adobe Photoshop e Paint foram detectadas utilizando apenas ferramentas de processamento de imagens. Posteriormente, Saini e Kaur (2018) avaliaram a eficiência do MATLAB 7.10.0 e Adobe Photoshop 7.0 na detecção de vestígios de alterações digitais em documentos. O estudo revelou que o algoritmo desenvolvido no MATLAB 7.10.0 alcançou 100% de detecção das alterações simuladas, identificando exclusões, adições de texto, manipulações por "copiar-colar" e distúrbios de fundo. Já os métodos baseados no Adobe Photoshop 7.0 foram menos precisos, porém úteis em contextos nos quais não havia documento de comparação.

Outros estudos buscaram técnicas computacionais para automatizar a detecção de alterações em documentos compostos basicamente por textos, como Bertrand *et al.* (2013), que apresentaram um método computacional baseado na comparação das distâncias entre caracteres da mesma classe, identificando irregularidades estruturais no documento analisado. Posteriormente, Bertrand *et al.* (2015) usaram outro método, que focou a programação na detecção de palavras escritas com fontes diferentes, mas, muitas vezes, similares. James *et al.* (2020) também estudaram o assunto, desenvolvendo um sistema para identificação de imperfeições em textos com base na tecnologia de reconhecimento OCR (*Optical Character Recognition*).

Com isso, o presente trabalho teve como objetivo oferecer um panorama da evolução da segurança documental e do papel do perito especialista em documentoscopia na detecção de fraudes realizadas em meio digital. Também são descritas técnicas de identificação de alterações em documentos digitalizados, com foco em vestígios perceptíveis sem o emprego de automatizações ou ferramentas avançadas. Para ilustrar, são apresentados estudos de casos de documentos contrafeitos por montagens digitais, periciados no Serviço de Perícias de Documentos (SPD) do Instituto de Criminalística Carlos Éboli (ICCE) da Secretaria de Estado da Polícia Civil do Rio de Janeiro.

1. Documentos Tradicionais

Um documento pode ser definido como qualquer material que carrega uma mensagem, explícita ou implícita (Huber e Headrick apud Silva; Feuerharmel, 2013), ou, de acordo com Del Picchia (2016), uma peça que registra uma ideia. Estes conceitos são bastante amplos e podem inclusive abarcar outras modalidades de suporte para transmissão de mensagens, como os eletrônicos. Entretanto, tradicionalmente, o conceito de documento está intimamente ligado ao suporte de papel, que é a forma como a grande maioria dos documentos são apresentados no nosso dia a dia e, consequentemente, também submetidos a exames documentoscópicos.

1.1. Classificação dos Documentos Tradicionais

Dentro do universo dos documentos tradicionais, podemos dividi-los em duas classes: aqueles que possuem elementos de segurança gráfica, que são dispositivos aplicados ao documento com a finalidade de protegê-los contra fraudes (Silva; Feuerharmel, 2013), e aqueles que não os possuem.

Os primeiros são denominados documentos de segurança e podem ser definidos, de forma pormenorizada, pela NBR 15368:2006, como:

> Todo e qualquer impresso de segurança que apresente algum valor e que desperte uma ação fraudulenta. Incorpora elemento ou elementos específicos para dificultar falsificações. Tem produção e distribuição controladas e nível de segurança dependente de quantidade, qualidade e adequabilidade dos elementos incorporados (ABNT, 2006).

Carteiras de identidade, passaportes, cédulas monetárias, documentos veiculares, diplomas e folhas de cheques são exemplos de documentos de segurança. Os documentos desprovidos de segurança gráfica, por sua vez, não possuem produção controlada e são confeccionados com materiais disponíveis no mercado, em gráficas comuns, impressoras domésticas ou através de produção manuscrita. Como exemplo, podemos citar as notas fiscais, recibos, declarações diversas, atestados médicos, receituários e cartas.

A autenticidade ou falsidade material de um documento de segurança pode ser verificada pela presença dos elementos de segurança gráfica, conforme os respectivos documentos oficiais emitidos pelo órgão ou empresa responsável. Nos documentos de emissão não controlada, a autenticidade material não pode ser garantida, cabendo ao perito confrontar as características gráficas existentes com os documentos de referência, avaliando sua compatibilidade. A detecção de falsidade, tanto em documentos de segurança quanto em não controlados, também pode ser alcançada pela identificação de alterações materiais que modifiquem seu conteúdo.

1.2. Alterações Documentais Materiais

As alterações documentais materiais são definidas como modificações realizadas por processos físicos ou químicos em qualquer parte do documento e, segundo Silva e Feuerharmel (2013), classificam-se em: subtrativas, aditivas e montagens.

As alterações subtrativas são caracterizadas pela retirada de informações do documento, por meio de rasura (Figura 1a), amputação, lavagem (Figura 1b) ou delaminação. Por sua vez, as alterações aditivas, como sugere o nome, acrescentam elementos ao documento original, seja pela impressão ou aposição de lançamentos gráficos, e podem ser do tipo: retoque, emenda (Figura 1c), inserção ou sobrecarga. Na modalidade de alteração por montagem (Figura 1d), utiliza-se de um ou mais documentos autênticos para produzir um novo documento.

Figura 1 – Exemplos de alterações materiais em documentos tradicionais

(a) (b) (c) (d)

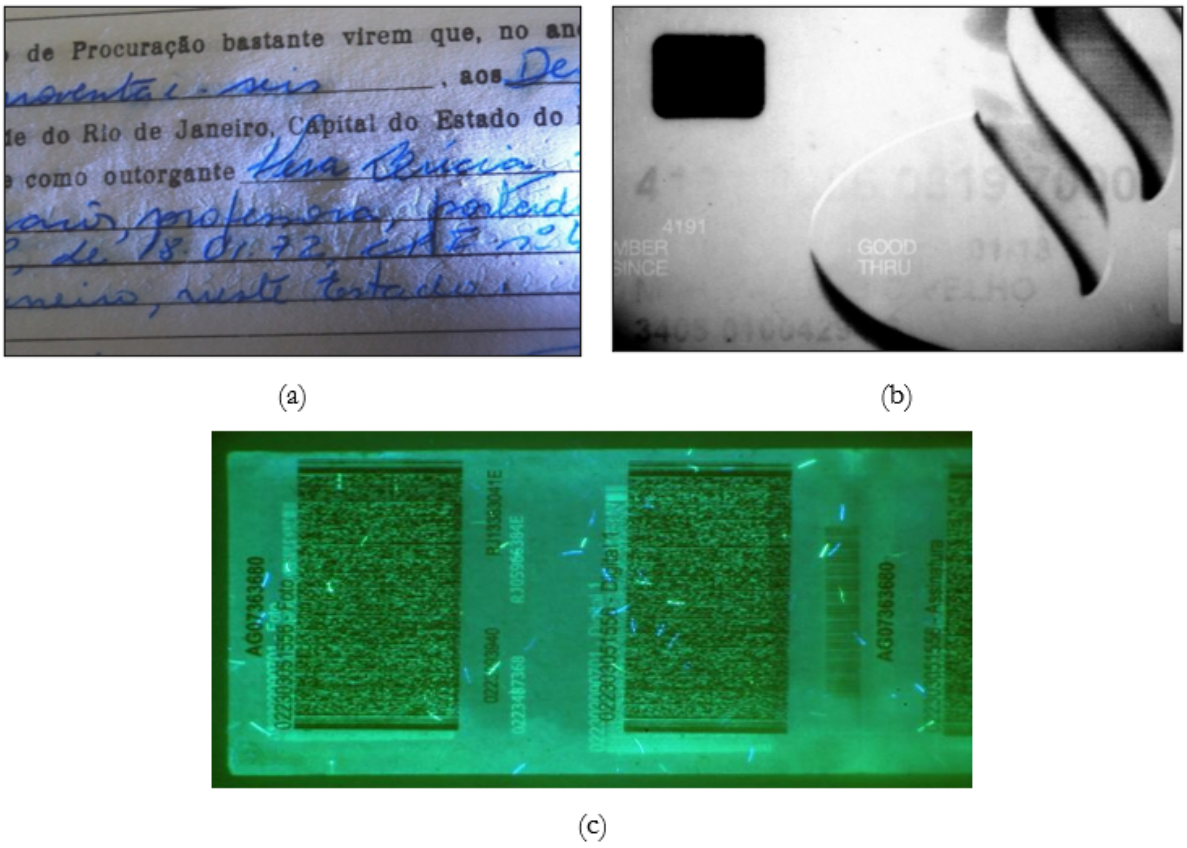
Fonte: Elaboração própria.

As alterações materiais podem ser identificadas com uso de equipamentos próprios, tais como lupas, estereomicroscópio e fontes de iluminação com diversos comprimentos de onda, nas posições incidente, emergente e oblíqua. Esses procedimentos permitem identificar: (i) máculas no substrato; (ii) vestígios de impressões ou escritas esmaecidas; (iii) manchas resultantes de lavagem química; e (iv) diferenças de comportamento de tintas sob luzes com comprimentos de banda estreita.

Como exemplo, na Figura 2a, a iluminação rasante foi utilizada para detectar sulcos no papel, que são vestígios de manuscritos anteriormente consignados em procuração. Na Figura 2b, a iluminação na faixa do infravermelho revelou dados suprimidos em um cartão bancário. Na Figura 2c, a iluminação na faixa do ultravioleta permitiu a visualização de impressões latentes, as quais são indicativas de remoção de dados anteriormente apostos em carteira de identidade.

Por se tratar de alterações físicas no suporte, a falsificação de documentos tradicionais, confeccionados em papel ou outros substratos, como os poliméricos, são, em geral, facilmente constatadas pelos especialistas com auxílio do instrumental adequado. Entretanto, quando os documentos fraudados são digitalizados ou copiados, as alterações podem ser mascaradas, tornando-se inidentificáveis.

Figura 2 – Algumas técnicas tradicionais de detecção de alterações documentais



Fonte: Elaboração própria.

2. Documentos Digitais

Quando uma informação não se encontra registrada em um suporte físico, mas em um formato digital, podemos definir o conjunto de dados como um documento digital. Os documentos digitais são classificados em duas tipologias: os nato-digitais e os digitalizados. Os primeiros são originados em um sistema eletrônico e nunca foram transferidos para um meio físico, como, por exemplo, um documento escrito em editor de texto e salvo no formato PDF. Os documentos digitalizados, por sua vez, são documentos convertidos de um formato físico para o formato digital por meio de escaneamento, fotografia, etc. (Paroti, 2018).

2.1. A Evolução Digital

Um documento digital é composto por *bits* e cada uma dessas unidades de código binário representa um fragmento da informação contida no documento (Paroti, 2018), que pode ser lida apenas através de um sistema operacional. Tal característica permite que os documentos digitais possam ser facilmente compartilhados e armazenados.

Com o crescimento da tecnologia da informação, o uso disseminado de dispositivos móveis e a necessidade de realizar ações remotamente, fortemente impulsionada pelo cenário atípico proporcionado pela pandemia do vírus Sars-CoV-2 (Covid-19), os documentos digitais têm substituído gradativamente as versões físicas.

Dentre as vantagens da utilização de documentos digitais, em relação aos impressos, estão: a redução de custos decorrente da dispensa de serviços de impressão, autenticação cartorária, transporte e armazenamento físico; a maior eficiência na gestão, com a aceleração dos fluxos processuais; e a contribuição sob o aspecto ambiental, com a redução do consumo de papel e outros insumos. Por outro lado, os principais desafios envolvem o desenvolvimento de mecanismos robustos para a segurança da informação, a implementação de soluções eficazes para o armazenamento de grande volume de dados e a garantia de acesso para todos os usuários.

Embora o advento dos documentos digitais represente um avanço significativo em termos de eficiência e acessibilidade, tanto no setor público quanto no privado, também ampliou as possibilidades de fraudes sofisticadas. A facilidade de manipulação dos documentos em meio digital, somada ao aperfeiçoamento constante das técnicas, dificulta a detecção de alterações, especialmente quando realizadas por um agente habilidoso.

2.2. Legislação

Na migração para fluxos eletrônicos, observa-se um período de transição caracterizado pela conversão de documentos físicos em digitais por meio da digitalização (Oliveira, 2020). Essa conversão pode ter a finalidade exclusiva de arquivamento ou visar a integração a diferentes processos, dentre eles os judiciais.

No âmbito dos processos judiciais, a validade jurídica dos documentos eletrônicos foi inicialmente prevista na Lei nº 11.419/2006, que disciplinou a informatização processual. A lei estabeleceu que os documentos eletrônicos possuem valor de originais, além de que extratos digitais e documentos digitalizados têm a mesma força probante, salvo quando houver alegação motivada de adulteração (Junior, 2020).

Posteriormente, o Novo Código de Processo Civil (NCPC, Lei nº 13.105/2015) reforçou esse entendimento: o artigo 411 trata da autenticidade dos documentos eletrônicos, estabelecendo sua presunção até prova contrária; o artigo 425 dispõe que reproduções digitalizadas de documentos públicos ou particulares, quando juntadas aos autos, têm a mesma eficácia probatória dos originais, salvo se houver impugnação quanto à idoneidade.

Entretanto, ainda que tratados pela legislação como originais, os documentos digitalizados apresentados em processos eletrônicos possuem qualidade muito variável, influenciada pela fonte, forma de digitalização adotada e limitações do próprio sistema.

Essa falta de padronização prejudica sobremaneira o trabalho do perito em documentoscopia, uma vez que as digitalizações de baixa qualidade não permitem a visualização de elementos importantes para a verificação de possíveis alterações na matriz ou de processamento digital. Assim, torna-se necessária a definição de padrões mínimos de digitalização. Nesse sentido, em 18 de março de 2020, foi publicado o Decreto nº10.278, que estabelece a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que as digitalizações produzam os mesmos efeitos legais dos documentos originais.

A regulamentação estabelece, dentre outros critérios, a resolução mínima de digitalização (em geral, 300 dpi); a configuração de cor — monocromático para textos impressos; escala de cinza para manuscritos em preto e branco; colorido para manuscritos em cores —; o formato do arquivo (na maioria das situações PDF/A) e os metadados obrigatórios. De acordo com o art. 5º do referido decreto, para que o documento digitalizado seja equiparado ao documento físico original, em relações envolvendo entidades públicas, é necessária a assinatura digital certificada no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Apesar dos avanços normativos, a realidade forense demonstra que a observância das exigências técnicas nem sempre é efetiva. Não é incomum a apresentação de digitalizações propositalmente de baixa qualidade, com o intuito de dissimular eventuais adulterações (Paroti, 2018), assim como a alegação de inexistência do documento original por parte de quem deveria preservá-lo até o trânsito em julgado. Esse descompasso entre o previsto em lei e a prática cotidiana impõe à perícia documentoscópica obstáculos significativos, tornando ainda mais necessária a análise minuciosa das peças, de modo a identificar vestígios de alterações e aferir a confiabilidade material das digitalizações apresentadas.

2.3. Características de Segurança dos Documentos Eletrônicos

Antes do advento dos documentos digitais, a segurança documental, do ponto de vista da autenticidade, baseava-se em elementos de segurança gráfica, como impressão calcográfica, marca d'água, impressos reativos à luz ultravioleta e hologramas. A integridade, por sua vez, apoiava-se na própria natureza física do suporte, uma vez que qualquer intervenção deixa vestígios, ainda que pouco perceptíveis.

Por outro lado, documentos eletrônicos, devido ao seu formato digital, demandam mecanismos distintos para assegurar propriedades fundamentais da segurança da informação — integridade, autenticidade, não repúdio (irretratabilidade) e confiabilidade — dos dados consignados (ABNT, 2005). Para tal, são utilizadas técnicas de criptografia, que consistem na codificação de uma informação, convertendo-a em um formato que não pode ser lido por quem não é autorizado (Naser; Jasim; Al-Mashhadi, 2020).

Dentre os recursos de segurança que utilizam a criptografia na sua construção, aplicados aos documentos digitais, estão as assinaturas digitais e os códigos do tipo QR (QR-Codes). Entretanto, as assinaturas digitais somente podem ser verificadas quando o documento se encontra no formato digital, enquanto os QR-codes fazem a interface de autenticação entre os documentos nato-digitais e suas versões impressas.

Ainda que os escritórios "sem papel" já sejam uma realidade em algumas empresas, certos tipos de documentos públicos ainda necessitam da via física, como a carteira de identidade, a carteira de habilitação e o passaporte. Uma das alternativas é a apresentação desses documentos na forma impressa de um nato-digital, a qual não possui elementos de segurança gráfica. No entanto, tal via continua a exigir algum mecanismo de validação da emissão (NASER; JASIM; AL-MASHHADI, 2020), função a qual o QR-Code tem sido amplamente utilizado.

QR-Code é a sigla de *Quick Response Code*, que significa código de resposta rápida. Segundo a definição da ISO/IEC 18004:2015 (ISO, 2015), consiste em uma matriz de símbolos, em duas dimensões, capaz de armazenar grande quantidade de caracteres numéricos e alfanuméricos, bem como caracteres binários e até mesmo caracteres logográficos chineses. Esse tipo de código pode ser lido por meio da câmera de smartphones, associada ou não a aplicativos específicos, que decodificam as informações nele armazenadas e as disponibilizam ao usuário. Quando protegidos por mecanismos de criptografia, que garantem a segurança da informação, permitem a validação dos documentos mediante o confronto entre os dados impressos e aqueles constantes no banco de dados do emissor que deu origem ao documento.

O uso do QR-Code em documentos oficiais já é disseminado, como na validação da Carteira Nacional de Habilitação e dos documentos veiculares (Figura 3) por meio do aplicativo Vio. Outra forma menos sofisticada de validação das informações contidas em documentos consiste em códigos alfanuméricos que possibilitam a consulta no site do emissor. Esse recurso é empregado atualmente na autenticação de certidões, notas fiscais, atos cartorários (Figura 4), entre outros.

Ainda que esta forma de garantia da autenticidade dos dados seja segura, os falsários têm buscado formas de driblá-la, por exemplo, por meio da criação de aplicativos e sites falsos, que levam a informações armazenadas em bancos de dados espúrios.

Figura 3 – CRLV digital, cuja autenticidade na via impressa é garantida apenas pelo QR-Code. O código foi parcialmente encoberto para preservar os dados pessoais

Fonte: Elaboração própria.

Figura 4 – Exemplos de documentos que utilizam códigos alfanuméricos para validação digital. (a) Selo de Fiscalização Eletrônico emitidos por cartórios. (b) Documento Auxiliar da Nota Fiscal Eletrônica

Fonte: Elaboração própria.

No cenário em que os mecanismos digitais de validação podem ser burlados ou se tornam ineficazes quando o documento nato-digital é convertido em suporte físico, a documentoscopia revela-se especialmente relevante. Compete ao perito identificar alterações, sejam elas produzidas por meios físicos ou digitais, e assegurar a execução da análise técnica mesmo na falta dos recursos de segurança originalmente disponíveis.

3. Alterações em Documentos Digitais

Paroti (2016) define montagem digital como:

> Criação de um documento falso contendo as características e informações de interesse do falsário, através do uso de equipamentos informáticos (computadores, escâneres, impressoras, copiadoras etc.) e softwares de várias naturezas.

Esse tipo de fraude pode deixar poucos vestígios, dependendo do grau de habilidade do falsário e dos recursos tecnológicos empregados, e é difícil de mitigar, uma vez que tais documentos não apresentam elementos de segurança gráfica e podem ser produzidos por qualquer pessoa com acesso a um computador e softwares simples de edição de imagens (James *et al.*, 2020).

No exame de documentos digitais, os recursos tradicionais de documentoscopia são limitados, pois os vestígios de alterações materiais, tais como deformações nas fibras do papel e diferenças na luminescência, não estarão presentes. Não obstante, com base nos conhecimentos já consolidados em documentos sem elementos de segurança gráfica, o perito consegue reconhecer parte dos indícios de manipulação digital.

Contudo, a análise completa requer a integração com áreas correlatas, como a perícia de imagens e a informática forense, que permitem explorar metadados, estruturas de arquivos e outras inconsistências gráficas. Esse cenário tem demandado atualização dos

profissionais, de forma a incorporar novas ferramentas, acompanhando a crescente sofisticação das fraudes digitais.

Ainda assim, a experiência prática tem mostrado que grande parte das falsificações em contextos de fraudes de baixo valor econômico permanece pouco elaborada, contando com a pouca atenção dada aos documentos em formato digital ou impressos sem elementos de segurança gráfica. Nesse sentido, os conhecimentos de documentoscopia mantêm-se importantes para a identificação desses vestígios, servindo como ponto de partida para análises mais amplas.

3.1. Procedimentos de Falsificação

A maior parte dos casos de alterações de documentos digitais, sejam eles nato-digitais ou digitalizados, ou até mesmo as versões impressas destes, tem como objetivo manipular figuras ou palavras que consequentemente irão alterar o conteúdo do documento. Em geral, os falsários têm como base inicial um ou mais documentos autênticos, que contêm elementos e informações a serem utilizadas no documento contrafeito (Paroti, 2016). Muitas vezes o documento matriz é pouco alterado, sendo substituídas apenas algumas informações de interesse.

São duas as principais técnicas de produção de um documento falso por meio de manipulação digital (Bertrand *et al.*, 2013), ambas utilizam softwares de edição de texto ou de imagem:

- **Copia e cola**: um conjunto de características, geralmente caracteres, é copiado de um documento autêntico e colado em outro local do próprio documento (automontagem) ou de um segundo documento autêntico. Com a técnica de "copia e cola" também podem ser facilmente criados documentos novos e inseridos neles elementos autênticos retirados de documento matriz autêntico, como assinaturas, carimbos, timbres etc;
- **Imitação**: o falsário adiciona ou modifica informações buscando imitar as características do documento autêntico, utilizando fontes com propriedades semelhantes às vistas no original.

O resultado da fraude pode ser apresentado no formato digital, em geral JPG ou PDF, e acostado a um processo eletrônico, por exemplo, ou impresso, como um Certificado de Registro e Licenciamento de Veículo ou um Documento Auxiliar de Nota Fiscal, facilitando a prática de crimes de roubo e venda ilegal.

3.2. Métodos Visuais para Detecção de Montagens

As técnicas para detecção de alterações em documentos digitais ou de origem digital, sob o ponto de vista exclusivo da documentoscopia, são baseadas na identificação de vestígios dos processos digitais de "copia e cola" e imitação. Esses vestígios podem manifestar-se como diferenças nas características tipográficas e de formatação, distorções no fundo, variações de resolução, desalinhamentos e outros elementos discrepantes.

Para a constatação dessas anomalias, o perito deve analisar atentamente os detalhes dos documentos, confrontando-os com outros trechos da própria peça questionada ou com paradigmas de mesma natureza. O exame deve ser realizado com auxílio de softwares dotados de ferramentas de ampliação digital.

Em uma análise mais aprofundada, o perito pode recorrer a softwares especializados na análise de imagens, como por exemplo, o Peritus ou o ImageJ. Esses programas dispõem de ferramentas de filtros úteis, como o CLAHE (*Contrast Limited Adaptive Histogram Equalization*), que melhora o contraste em regiões localizadas da imagem, destacando diferenças sutis de textura e facilitando a visualização de manchas ou padrões irregulares, e o ELA (*Error Level Analysis*), que evidencia variações nos níveis de compressão JPEG, revelando áreas potencialmente manipuladas.

De modo geral, os vestígios de alterações digitais identificáveis apenas por recursos visuais podem ser classificados em três categorias, aqueles relacionados ao(à)(s): i) caracteres e outras propriedades de formatação; ii) distorções no fundo e diferenças de resolução; iii) demais anomalias e defeitos.

4. Estudo de Casos

Nesta seção, como forma de ilustrar os vestígios de alterações documentais comumente observados em falsificações perpetradas com uso recursos digitais, são apresentados alguns casos de documentos físicos, desprovidos de elementos de segurança gráfica, periciados no Serviço de Perícias de Documentos (SPD) do Instituto de Criminalística Carlos Éboli da Secretaria de Estado de Polícia Civil do Rio de Janeiro.

Apesar dos documentos selecionados como ilustração não terem sido encaminhados à perícia no formato digital, tratam-se de documentos nato-digitais convertidos em suporte físico por meio da impressão. Os vestígios de alteração perceptíveis nas vias impressas também seriam identificáveis na versão digital.

No entanto, a chegada apenas do documento impresso restringe o exame, pois implica a perda de informações intrínsecas ao arquivo digital. Caso as matrizes nato-digitais tivessem sido submetidas diretamente à perícia, seria possível aplicar ferramentas adicionais, como a análise de metadados, a avaliação da estrutura do arquivo e o uso de filtros digitais para potencializar a análise perceptual. Essa limitação, recorrente na prática forense, evidencia a fragilidade probatória em função da conversão de nato-digitais em papel e reforça a importância de preservar e apresentar os documentos em sua forma original, sempre que possível.

4.1. Amostras

Para as ilustrações, foram selecionados os seguintes documentos, remetidos ao SPD com solicitação de exame pericial documentoscópico de autenticidade: Nota de Arrematação; Documentos Auxiliares de Nota Fiscal Eletrônica (DANFE); Notas Fiscais de Serviço Eletrônicas (NFS-e).

4.2. Metodologia

Os documentos foram digitalizados com resolução entre 600 dpi e 1200 dpi, utilizando escâner Epson Perfection V19, e submetidos a análise perceptual, apenas com uso de ampliação digital. O objetivo foi identificar vestígios de alterações documentais perpetradas com uso de softwares de edição de imagem.

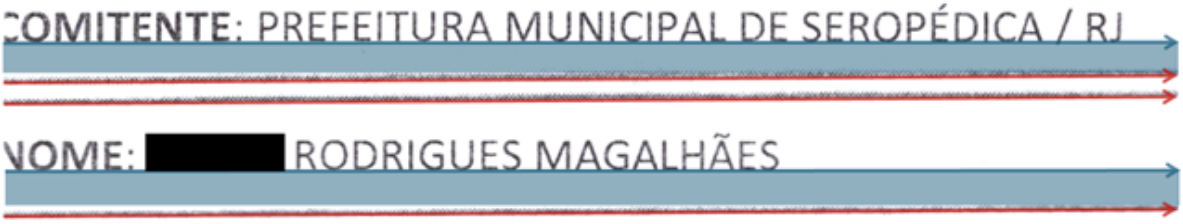
4.3. Resultados

Os elementos constatados são listados a seguir, bem como outros aspectos que podem ser buscados pelo perito na identificação deste tipo de fraude.

i) Pequenos desalinhamentos, tanto verticais como horizontais;

Deve ser observada a homogeneidade do documento, comparando o direcionamento das linhas e verificando o paralelismo entre elas. Na direção vertical, os documentos autênticos, em geral, apresentam parágrafos com mesmo recuo. A figura 5 mostra o desalinhamento constatado entre o texto e as linhas que delimitam os campos de umas das notas de arrematação.

Figura 5 – Desalinhamento entre o texto e as linhas que delimitam os campos, observado em uma das notas de arrematação

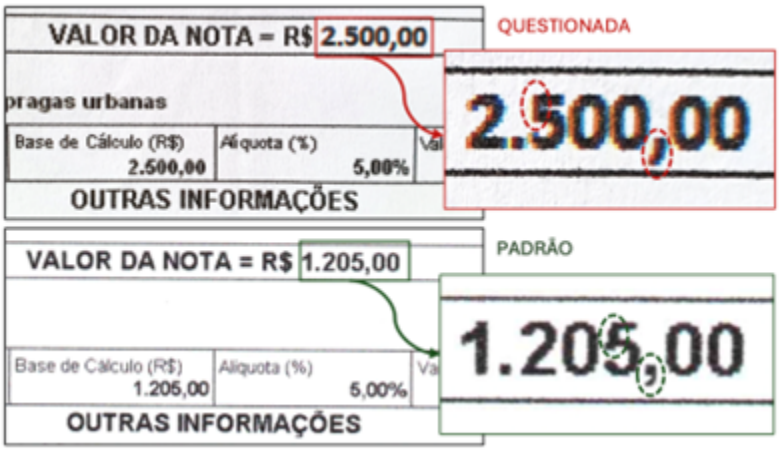


Fonte: Elaboração própria.

ii) Discrepâncias no tipo, tamanho, espessura e tonalidade das fontes;

Em condições normais, as fontes utilizadas no preenchimento de um formulário ou em uma mesma frase apresentam características homogêneas. Pode-se também realizar o confronto com um documento autêntico de mesma natureza, buscando identificar divergências, como a constatada na Figura 6.

Figura 6 – Divergência no tipo e tamanho da fonte no campo "valor da nota" de um dos DANFEs, constatada no confronto com um documento padrão de mesma natureza



Fonte: Elaboração própria.

Uma das dificuldades encontradas pelos falsários está na identificação correta da fonte utilizada no documento autêntico. Muitas vezes a fonte utilizada na porção alterada é similar à utilizada no documento íntegro, mas pequenas diferenças nas proporções e alguns detalhes podem revelar o uso da fonte incorreta. Algumas fontes não estão disponíveis para o público comum.

No que diz respeito ao tamanho da fonte, o principal desafio reside no fato das digitalizações causarem algumas distorções nos caracteres, como pequenas reduções ou ampliações, que são difíceis de serem contornadas com os tamanhos padronizados.

iii) Diferenças no espaçamento interliteral e interlinear;

Geralmente resultante do mau posicionamento das caixas de texto e uso de configurações diferentes para o espaçamento entre as letras (expandido, normal ou condensado) ou *kerning*, que é o espaçamento entre pares específicos de letras.

iv) Não uniformidade das características do fundo, como diferenças na tonalidade, descontinuidades e irregularidades no arranjo dos pixels;

Quando o documento contrafeito apresenta cores ou demais elementos impressos que constituem o fundo do suporte, a alteração das informações apostadas sobre ele revela-se mais difícil, uma vez que exige a reprodução fiel desse fundo na área afetada, o que demanda elevada habilidade do falsário para minimizar vestígios.

v) Presenças ou ausência de pontilhados em áreas específicas do documento;

Os pequenos pontos observados no fundo de documentos podem decorrer da impressão da cor de fundo do documento original — por exemplo, realizada em impressora jato de tinta — ou de sombras originadas durante a digitalização de documentos com dobras, amassados ou mau posicionados.

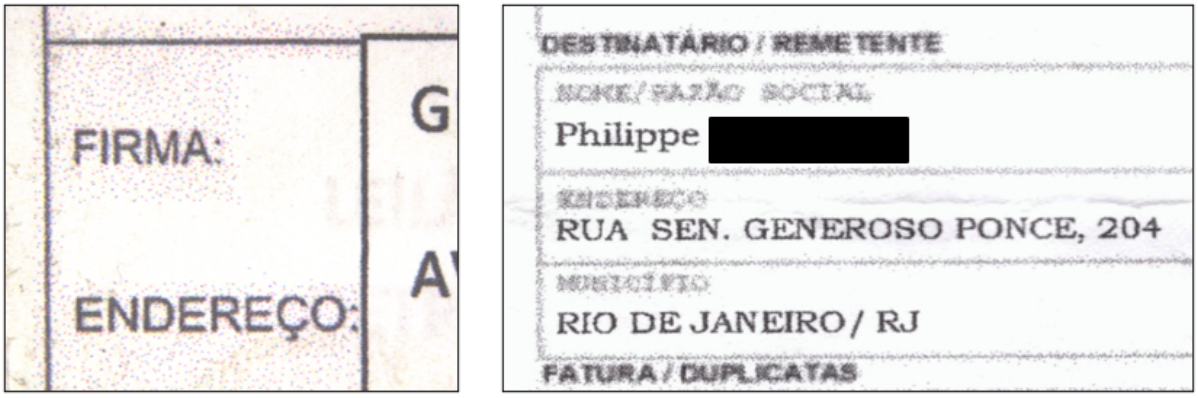
Quando se procede à remoção digital de partes do documento ou à inserção de elementos oriundos de outro documento, é comum que o falsário deixe vestígios, caso não atente para sutis diferenças na tonalidade do fundo. A Figura 7a exemplifica esse tipo de alteração: em uma das notas de arrematação, a supressão de informações do documento-matriz resultou em alteração do fundo e em heterogeneidade do padrão pontilhado.

vi) Diferenças de resolução entre os elementos que compõem o documento;

Um documento, ao ser digitalizado e transformado em imagem, assume um tamanho adimensional, em pixels (*picture elements*), e a resolução é uma medida de qualidade desta imagem, definida como a razão entre o número de pixels e o tamanho da imagem real, em geral medida em dpi (*dots per inch*) (SCURI, 2002).

Quando a imagem do documento é impressa, a resolução é refletida na nitidez e definição. Nos sucessivos processos de impressão e digitalização que um documento contrafeito pode ser submetido, a qualidade dos elementos que o compõe se diferencia em virtude das distintas resoluções de digitalização e características de impressão, tornando possível identificar aqueles que foram inseridos em momentos diferentes dos demais. A Figura 7b ilustra tais contradições de resolução constatadas em uma das notas de arrematação e em um dos DANFEs.

Figura 7 – (a) Ausência de pontilhados em áreas específicas de uma das notas de arrematação e qualidade distinta entre as linhas que delimitam os campos. (b) Nítida diferença de resolução entre os títulos dos campos e o preenchimento em um dos DANFEs



(a) (b)

Fonte: Elaboração própria.

vii) Diferenças na forma de armazenamento das informações de um texto;

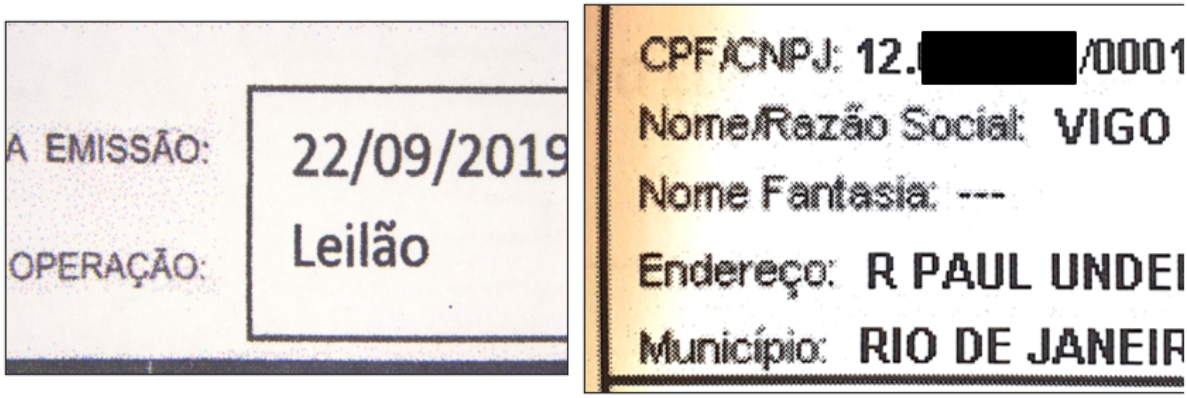
Um documento pode conter textos e/ou imagens, que são armazenados de maneiras diferentes em um único arquivo. As imagens são armazenadas como um conjunto de pixels (imagens *raster*) e os textos são lidos caractere por caractere (imagens vetoriais), cada um representado por uma única unidade de código. Essa diferença na forma de armazenamento dos dados influencia na qualidade da impressão, uma vez que o processo de impressão de texto é mais eficiente (Feuerharmel, 2020).

Caso um texto tenha sido digitalizado, ele se transforma em uma imagem e perde as suas propriedades de texto. A distinção decorrente da forma de armazenamento pode ser identificada em documentos impressos por meio da análise da qualidade de impressão — refletida na nitidez, na definição das bordas e, ocasionalmente, na presença de pontos coloridos quando os trechos são impressos como imagem. A Figura 8 apresenta, para uma das notas de arrematação e para diversas NFS-e, as diferenças nas características gráficas entre informações impressas como texto e como imagem.

viii) Anomalias, como restos de imagens e sinais de corte;

Outros elementos que podem indicar a remoção ou inserção digital de informações em um documento é a observação de defeitos não vistos em documentos autênticos, como cortes em palavras, partes faltantes e vestígios de imagens apagadas. São pequenos detalhes deixados para trás por falsários pouco cuidadosos. A Figura 9 ilustra o observado em NFS-e, em especial no campo onde estão consignados, o número e código de verificação do documento. Constatou-se corte de palavras, provavelmente ocasionado pelo mau posicionamento da caixa de texto utilizada para inserção de dados falsos.

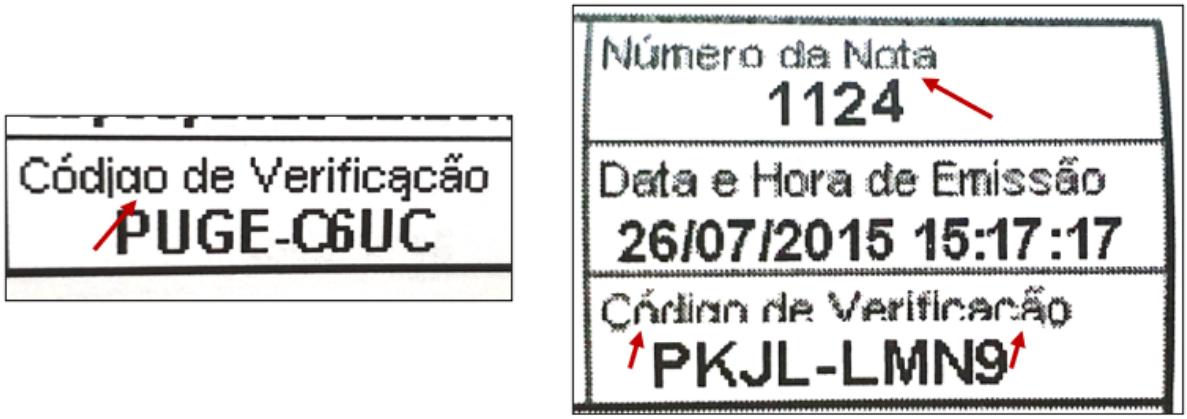
Figura 8 – Diferentes características de impressões no formato texto e imagens, em uma das notas de arrematação (a) e em uma das NFS-e (b)



(a) (b)

Fonte: Elaboração própria.

Figura 9 – Corte de palavras observado nas NFS-e



(a) (b)

Fonte: Elaboração própria.

ix) Conferência lógica dos dados.

Outro recurso para determinar a falsidade do documento que, no entanto, não envolve a detecção de vestígios de montagens digitais, consiste na verificação da existência de anacronismos, erros ortográficos e de inconsistências lógicas.

A Figura 10 apresenta o erro lógico observado em um dos DANFEs: a não correspondência das numerações do documento. Também foi verificado que a chave de acesso para conferência dos dados junto ao emissor apresenta menos dígitos que o devido, impossibilitando a consulta.

Figura 10 – Erro lógico constatado na numeração de um dos DANFEs e erro na quantidade de caracteres da chave de acesso

Fonte: Elaboração própria

4.4. Discussão

Das análises realizadas nos documentos selecionados, foi possível, apenas com o uso de ampliação, detectar vestígios de alterações em documentos sem elementos de segurança gráfica, resultantes da impressão de documentos nato-digitais. Foram observadas inconsistências relacionadas à formatação, à resolução e presença de anomalias gráficas e lógicas que permitiram aos peritos constatar a falsidade dos documentos questionados.

Cabe ressaltar que, sob o ponto de vista puramente documentoscópico, não é possível atestar a autenticidade de um documento digital, uma vez que este não possui elementos que garantam a sua origem, verificáveis apenas pela análise perceptual. Por outro lado, é possível constatar sua falsidade a partir da identificação de vestígios de alteração que, quando analisados em conjunto, constituem um argumento fortemente probante. Quando

não são observadas alterações, o exame é considerado inconclusivo, pois a ausência de indícios de uma ocorrência não constitui, necessariamente, prova de que ela não tenha ocorrido (Feuerharmel, 2017).

Outras análises podem complementar o exame documentoscópico, especialmente quando se dispõe da versão digital original do arquivo. Nesses casos, é possível recorrer a ferramentas próprias da perícia de imagens, como a aplicação de filtros que destacam diferenças de compressão ou de contraste, e da informática forense, voltada à interpretação de metadados, estruturas internas dos arquivos e validação de assinaturas eletrônicas. No entanto, tais procedimentos exigem conhecimentos específicos, demonstrando a necessidade de atuação interdisciplinar e atualização dos peritos em documentoscopia, visando a obtenção de conclusões mais robustas sobre a integridade e a autenticidade dos documentos digitais.

Considerações finais

A migração dos documentos para o meio digital, seja por meio da criação de versões eletrônicas de documentos de identificação, veiculares, fiscais e outros que possibilitam ao cidadão exercer seu papel na sociedade, seja pela instituição dos processos judiciais eletrônicos, que validam a apresentação de vias digitalizadas dos documentos, tem trazido diversos desafios à perícia documentoscópica. Todas as mudanças já ocorridas, e aquelas que certamente virão, têm forçado os especialistas em análise de documentos a se atualizarem e adaptarem seus métodos e recursos para atenderem a uma nova demanda de exames.

Observa-se que os fundamentos clássicos da documentoscopia permanecem indispensáveis, mesmo quando aplicados a documentos digitais, servindo como base para a detecção de incongruências gráficas e indícios de manipulação. Entretanto, para que a análise seja abrangente e tecnicamente robusta, torna-se necessária a integração com a perícia de imagens e a informática forense, áreas que possibilitam o exame de metadados, assinaturas eletrônicas, estruturas de arquivos e manipulações digitais de imagens. A depender da organização do órgão, tal integração pode ocorrer por meio do aprendizado de novos conhecimentos pelo perito em documentoscopia ou pela colaboração entre os profissionais das áreas.

Como proposta de trabalhos futuros, sugere-se que sejam realizados testes controlados, simulando montagens digitais em diferentes níveis de complexidade, permitindo observar os vestígios característicos deixados e as principais dificuldades enfrentadas pelos falsários. Com os resultados encontrados, os peritos poderão ampliar seu repertório técnico, consolidando o uso de ferramentas de análise de imagens e recursos da informática forense.

Esse conjunto de conhecimentos, aliado à experiência da documentoscopia, fortalecerá a capacidade de identificar novas modalidades de fraude e assegurará a efetividade da perícia documental no contexto digital.

Referências

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005: Tecnologia da informação — Técnicas de segurança — **Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 15368:2006: Tecnologia gráfica - **Terminologia de elementos para uso em impressos de segurança**. Rio de Janeiro, 2006.

BERTRAND, Romain; GOMEZ-KRÄMER, Petra; TERRADES, Oriol Ramos; FRANCO, Patrick; OGIER, Jean-Marc. **A System Based on Intrinsic Features for Fraudulent Document Detection**. In: International Conference on Document Analysis and Recognition, 12., 2013, Washington, DC, United States. p. 106-110.

BERTRAND, Romain; RAMOS, Oriol; GOMEZ-KRÄMER, Petra; FRANCO, Patrick; OGIER, Jean-Marc. **A Conditional Random Field Model for Font Forgery Detection**. In: International Conference on Document Analysis and Recognition (ICDAR), 13., 2015, Nancy, France. p.576 -580.

DEL PICCHIA, José Filho; DEL PICCHIA, Celso Mauro Ribeiro; DEL PICCHIA, Ana Maura Gonçalves. **Tratado de documentoscopia**: da falsidade documental. 3ª ed. São Paulo: Editora Pillares, 2016.

DERINGAS, Audrys. **Traces of Forgery in Digitally Manipulated Documents**. Problems of Forensic Sciences, v. 46, p. 375-382, 2001.

FEUERHARMEL, Samuel. **Análise Grafoscópica de Assinaturas**. Campinas: Millennium, 2017

FEUERHARMEL, Samuel. **Documentoscopia 3** - Estudos de Casos. 2020. Notas de Aula. Instituto de Pós-Graduação – IPOG.

ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 18004:2015: I**nformation technology - Automatic identification and data capture techniques** - QR Code bar code symbology specification. Suíça, 2015.

JAMES, Hailey; GUPTA, Otkrist; RAVIV, Dan. **OCR Graph Features for Manipulation Detection in Documents**. ArXiv, abs/2009.05158, 2020.

JUNIOR, Roberto Delmanto. **Prova documental. Tomo Processo Penal**, Edição 1, Ago. 2020. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/447/edicao-1/prova-documental. Acesso em: 1 jun. 2021.

NASER, Maysaa Abd Ulkaree; JASIM; Eman Talib; AL-MASHHADI, Haider M. **QR code based two-factor authentication to verify paper-based documents**. TELKOMNIKA Telecommunication, Computing, Electronics and Control, v. 18, n. 4, p. 1834-1842, Ago. 2020.

OLIVEIRA, Fernanda Rosa de Vasconcelos. **A Força Probante dos Documentos Digitalizados**: Eficiência Versus Segurança Jurídica. Caderno Virtual, Brasília, v. 1, n. 46, jan/abr. 2020.

PARODI, Lorenzo. **Falsificação de Documentos em Processos Eletrônicos**. Rio de Janeiro: Brasport, 2018.

SAINI, Komal; KAUR, Shabnam Preet. **Forensic Examination of Computer-Manipulated Documents Using Image Processing Techniques**. Egyptian Journal of Forensic Sciences, v. 6, p. 317–322, 2016.

SAINI, Komal; KAUR, Shabnam Preet. **Examination of Digitally Manipulated Documents Using Matlab 7.10.0 and Adobe Photoshop 7.0. Problems of Forensic Sciences**, v. 111, p. 31-44, 2018.

SILVA, Erick Simões da Câmara; FEUERHARMEL, Samuel. **Documentoscopia**: aspectos científicos, técnicos e jurídicos. Campinas: Millennium, 2013.

SCURI, Antonio Escaño. **Fundamentos da Imagem Digital**. Setembro de 2002. Notas de aula. PUC-Rio.

Lívia Fernandes Santos
(livia.pericia@gmail.com)

Engenheira Civil, Mestra em Engenharia Civil, Perita Criminal do Instituto de Criminalística Carlos Éboli Polícia Civil/RJ e Especialista em Documentoscopia.
https://orcid.org/0009-0004-6803-2911

Kelly Carla Almeida de Souza Borges
(almeida_kc@yahoo.com.br)

Engenheira Florestal, Doutora em Ciências, Perita Criminal do Instituto de Criminalística Carlos Éboli Polícia Civil/RJ e Especialista em Documentoscopia.
https://orcid.org/0009-0004-7533-5232

Ana Claudia Lednik
(vet.anaclaudia@gmail.com)

Médica Veterinária, Perita Criminal do Instituto de Criminalística Carlos Éboli, Polícia Civil/RJ e Especialista em Documentoscopia.
https://orcid.org/0009-0009-0771-0113

Marina de Assis Moura Navarro
(marinaamouranavarro@gmail.com)

Médica Veterinária, Perita Criminal do Instituto de Criminalística Carlos Éboli, Polícia Civil/RJ e Especialista em Documentoscopia.
https://orcid.org/0009-0005-9563-6742

Recebido: 20/05/2025
Aprovado: 30/09/2025
Editor responsável: Carolina Luz