Capítulo 1

Crime Scene Investigation (CSI): da Ficção à Realidade.

Tiago Carvalho, Allan Pinto, Ewerton Silva, Filipe de Oliveira Costa, Giulliano Roberto Pinheiro e Anderson Rocha

Abstract

An astonishing number of digital documents, such as digital pictures, videos, text files, etc., are daily produced and broadcasted. However, their authenticity is usually a doubtful question, since tampering digital documents have been become a simple task through using existent manipulation tools. So, our trust on digital documents is constantly decreasing, making necessary to develop effective approaches to recover this trust. All these facts highlight the importance of digital forensics in our day-by-day life. Based on this, our work presents a forensics computing overview showing main kind of forensics problems and most recently approaches to treat them.

Resumo

Diariamente, um número gigantesco de documentos digitais é produzido e compartilhado com pessoas de todas as partes do mundo através da internet. Documentos como fotos, vídeos, arquivos texto e tantos outros são apenas alguns dos exemplos dos documentos digitais presentes em nosso dia-a-dia. Mas nem sempre a autenticidade de um documento digital é preservada dado que, adulterá-lo utilizando ferramentas disponíveis atualmente torna-se a cada dia mais simples. Isso diminui nossa confiança em documentos digitais a cada dia e torna necessário o desenvolvimento de métodos forenses eficazes para restaurar tal confiança. Este minicurso trás para o público uma visão geral da computação forense ao longo do tempo, bem como expõe os principais problemas tratados na computação forense e suas mais recentes soluções.

1.1. Introdução

Em um mundo onde a tecnologia avança diariamente em uma velocidade exponencial, é comum nos depararmos com situações da ficção científica dentro de nossa realidade. Cenas antes vislumbradas apenas pelos mais criativos cineastas, se tornam parte de nossa

vida cotidiana, seja de uma forma construtiva, ou não. Um exemplo disso pode ser visto hoje quando policiais utilizam avançados métodos computacionais na resolução de crimes, fato antes visto apenas na conhecida série de TV americana intitulada *Crime Scene Investigation* (CSI) [1]. No entanto, os avanços da tecnologia também produzem resultados negativos em nossa vida. É o caso do crescimento no número de crimes envolvendo documentos digitais, principalmente envolvendo imagens. Tal fato é impulsionado principalmente por dois fatores: o primeiro deles é o baixo custo e grande acessibilidade aos dispositivos de captura de imagens, o qual faz crescer a cada dia o número de imagens produzidas no mundo. O segundo é dado pelo crescente aumento na sofisticação dos softwares de manipulação de imagens, os quais se tornam a cada dia mais simples de utilizar e mais efetivos na geração de resultados.

Adulterações em imagens podem variar de um simples balanceamento de cores na imagem, o que caracteriza uma adulteração inocente, até a criação de uma imagem totalmente sintética visando confundir um observador. Utilizando softwares como o Adobe Photoshop ou o Gimp, até mesmo um usuário sem grande conhecimento é capaz de criar falsificações realistas, visando enganar pessoas, em um curto período de tempo. E devido a tal facilidade, situações envolvendo adulterações maliciosas em imagens estão presentes nos mais diversos meios de comunicação tais como jornais, revistas, *outdoors*, televisão, internet e até mesmo em artigos científicos [Rocha et al. 2011].

Fatos como os acima citados fazem com que nossa confiança no conteúdo das imagens diminua constante. O professor Hany Farid [2] define o impacto da adulteração de imagens na confiança das pessoas da seguinte forma: *qualquer forma de adulteração gera incerteza em um cenário que está se tornando cada vez mais maleável, de forma que não importa o quão pequena é a adulteração, a confiança é corroída* [Farid 2009].

Para tentar restaurar tal confiança, desenvolveu-se dentro do campo da Ciência da Computação uma nova área de pesquisa denominada Computação Forense (CF). Segundo o professor Edward Delp [3] a CF pode ser definida da seguinte forma: *"É o conjunto de técnicas científicas para a preservação, coleção, validação, identificação, análise, interpretação, documentação e apresentação de evidências derivadas de meios digitais com a finalidade de facilitar e/ou permitir a reconstrução de eventos, usualmente de natureza criminal".*

Dentro da CF, uma sub-área que vem ganhando cada vez mais destaque é a Análise Forense de Documentos Digitais (AFD), a qual foca no desenvolvimento de novos métodos para tratar problemas como a identificação de dispositivos de origem de imagens, detecção de criações sintéticas, detecção de composições, entre outras.

Assim esse trabalho tem como objetivo apresentar para o público alguns dos principais problemas enfrentados pela comunidade forense dentro da AFD, bem como apresentar algumas das técnicas mais recentes desenvolvidas para tratar tais problemas.

O restante deste trabalho é dividido da seguinte forma: na Seção 1.2 descrevemos brevemente a evolução das adulterações em imagens ao longo da história. Nas

[1] `http://en.wikipedia.org/wiki/CSI:_Crime_Scene_Investigation`
[2] `http://www.cs.dartmouth.edu/farid/Hany_Farid/Home.html`
[3] `https://engineering.purdue.edu/~ace/`

Seções 1.3 e 1.4 apresentamos, respectivamente, os principais tipos de problemas abordados pela AFD bem como alguns dos métodos mais recentes desenvolvidos para resolução de cada um dos problemas. Por fim, na Seção 1.5 apresentamos nossas conclusões a respeito do trabalho bem como alguns dos problemas ainda em aberto na área.

1.2. Falsificações ao Longo da História

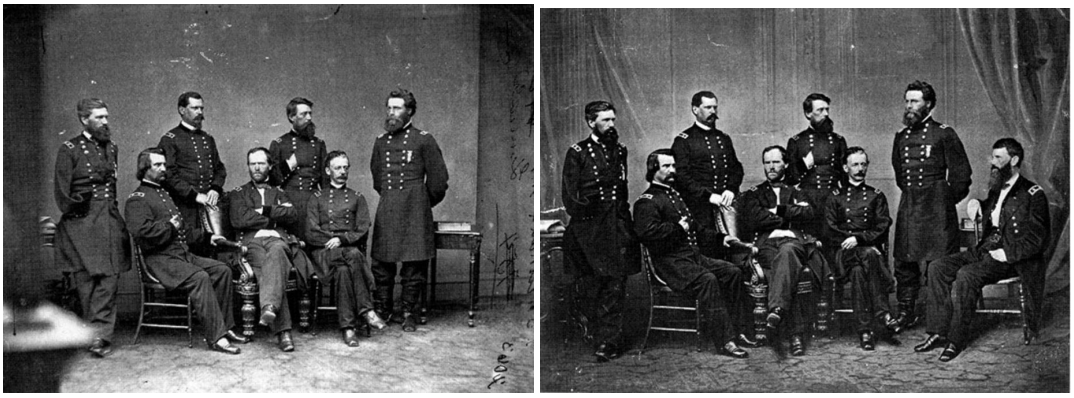
Apesar de se popularizar após o surgimento da fotografia digital, as adulterações em imagens, principalmente aquelas com o intuito de enganar o observador, surgiram bem antes da era digital, sendo as primeiras adulterações datadas de 1814 [Rocha and Goldenstein 2010]. A Figura 1.1 exibe a primeira falsificação em imagens de que se tem notícia, a qual foi produzida por Oscar G. Rejland e é conhecida como *The two ways of life* [4].

Figure 1.1. A imagem *The two ways of life* foi produzida por Oscar G. Rejland em 1857 e exibida em Manchester, gerando grande polêmica na época. Rejland utilizou mais de 30 negativos de fotos na composição da imagem final.

Uma célebre imagem, que também descobriu-se tratar de uma falsificação, data de 1865 e retrata os generais da guerra civil americana como mostra a Figura 1.2. Tratado na maioria das vezes como o primeiro fotojornalista bem sucedido mundialmente, Mathew Brady, foi também um dos mais talentosos manipuladores de sua época. Na clássica foto do general William Tecumseh Sherman e seus oficiais, Brady adicionou o comandante Francis P. Blair (na extrema direita) à foto.

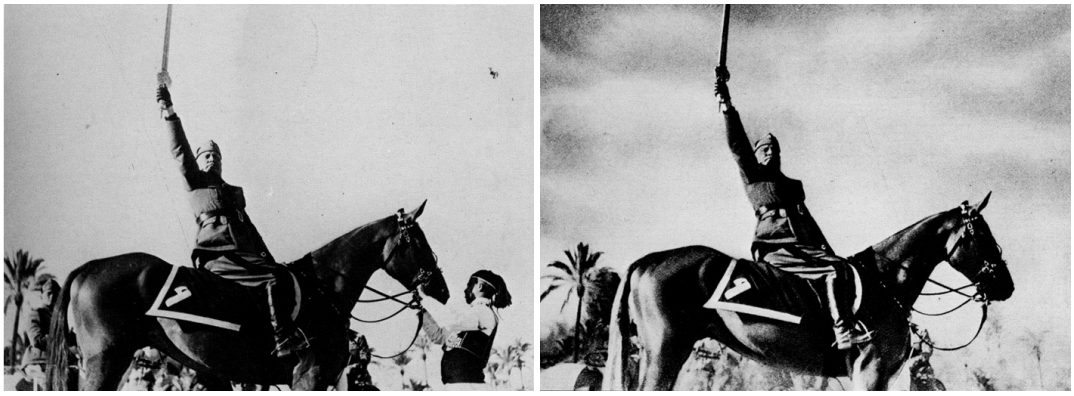
Os regimes ditatoriais também foram grandes utilizadores da arte de adulterar imagens, fosse em prol de construir uma imagem mais heroica dos líderes ditatoriais, ou para remover pessoas que se tornaram contrárias ao regime. O ditador Benito Mussolini, por exemplo, teve seu escudeiro (o qual segurava seu cavalo) removido da foto para dar a esta uma aparência mais heroica e imponente como mostra a Figura 1.3. Já o ditador Mao

[4]Robert Leggat. *A History of Photography From its beginnings till the 1920s*. Publicado em `http://lnx.phototeka.it/documenti/Cenni_storici_fotografia.pdf`. Último acesso: 19/09/2012.



(a) Original (b) Adulterada

Figure 1.2. Manipulação retratando generais da guerra civil americana. O comandante Francis P. Blair (na extrema direita) da foto adulterada não estava presente na foto original.

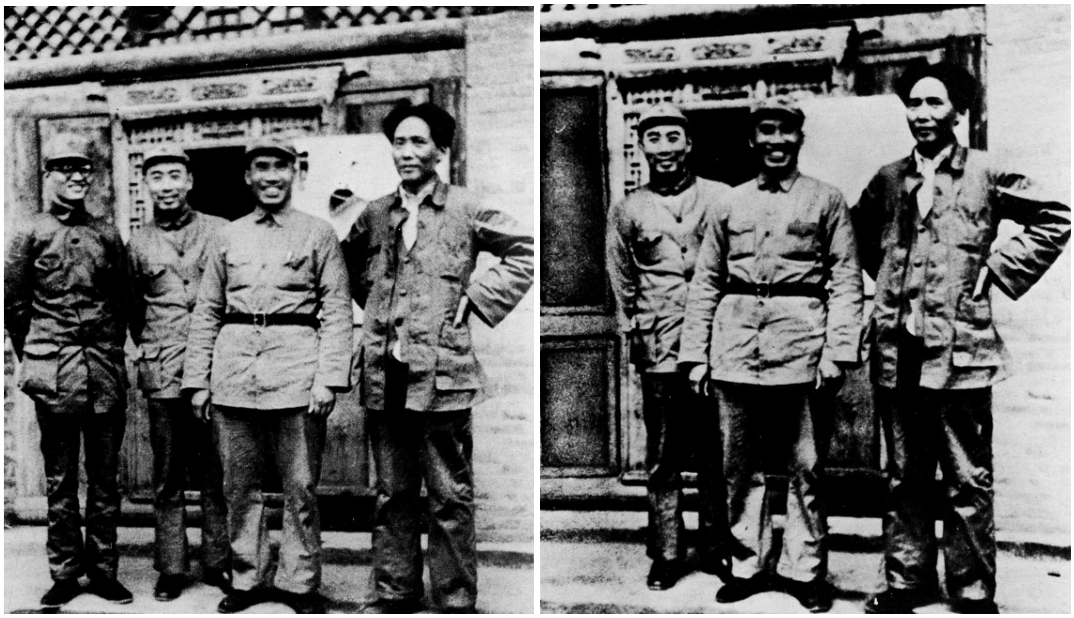


(a) Original (b) Adulterada

Figure 1.3. Assim como outros ditadores, Benito Mussolini também utilizou-se de manipulações de imagens durante seu domínio.

Tse-tung teve seu oficial Po Ku removido de uma foto, como mostra a Figura 1.4, após um desentendimento entre eles.

O processo de adulteração de imagens antes da era digital, era um processo que poderia durar dias, até mesmo meses, e exigia dos manipuladores um grande conhecimento técnico na área [Popescu 2004]. Hoje em dia porém, com o avanço das ferramentas de manipulação de imagens e vídeos (e. g., Adobe Photoshop e Gimp), mesmo usuários sem muito conhecimento podem fazer adulterações realistas em imagens em poucas horas. Observe por exemplo a Figura 1.5, a qual circulou pela internet pouco tempo após o atentado de 11 de setembro de 2001 (indicando que a manipulação não levou mais do que algumas horas para ser feita). Apesar de sugerir que um turista capturou a foto no observatório externo do *World Trade Center* (WTC) no momento do impacto de um dos aviões (a data da foto no canto inferior direito aponta 11 de setembro de 2001, dia exato do atentado), a foto contém alguns elementos divergentes: o observatório externo do WTC se situava na torre sul, sendo que a foto aponta rumo ao norte (na direção do Empire



(a) Original (b) Adulterada

Figure 1.4. Mao Tse-tung também fez uso de manipulações de imagens.

State Building, o qual pode ser observado no fundo da foto). No entanto, a torre sul foi atingida pelo pelo avião sequestrado vindo do sul. Essa simples análise lógica já indica que a imagem é produto de uma falsificação.

Figure 1.5. Suposta imagem retratando o *World Trade Center* segundos antes do atentado de 11 de setembro.

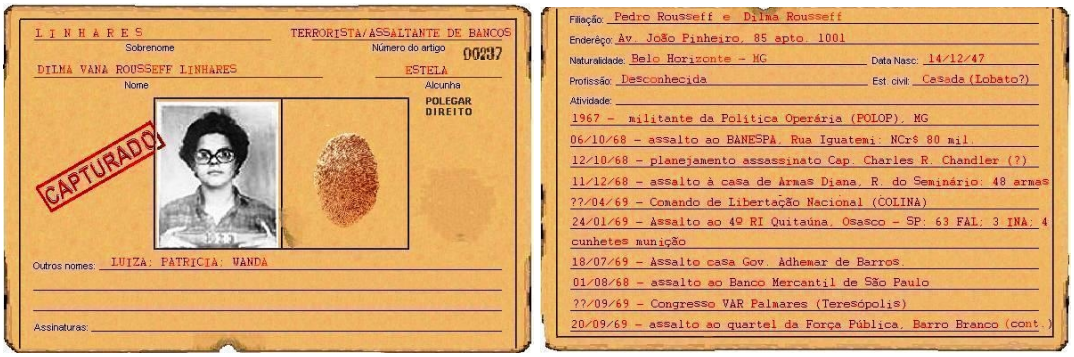
Outro exemplo do uso de adulterações de imagens ocorreu em abril de 2009, quando a imprensa britânica divulgou uma foto da suposta morte do terrorista Ozama Bin Laden como mostra a Figura 1.6. No entanto, devido a baixa qualidade da adulteração, pouco tempo depois foi constatado de que se tratava de uma falsificação.

Em um exemplo mais próximo de nossa realidade, ocorrido no Brasil em abril de 2009 envolvendo a atual presidente do Brasil Dilma Rousseff, o jornal Folha de São Paulo

(a) Ozama Bin Laden (b) Suposta morte (c) Base da adulteração

Figure 1.6. Imagens retratando a suposta morte do terrorista Ozama Bin Laden em abril de 2009. Pouco tempo depois foi provado que se tratava de uma falsificação.

publicou um artigo envolvendo uma suposta participação da atual presidente em ações de terrorismo durante o governo militar. A matéria divulgou ainda a imagem de uma ficha criminal que, supostamente, pertencia a Dilma Rousseff como mostra a Figura 1.7. Em uma análise forense detalhada do documento, [Goldenstein and Rocha 2009] provaram que o documento foi produto de uma série de operações de manipulação. Assim, além de afetar a popularidade do jornal, o mesmo foi obrigado a publicar uma retratação formal à atual presidente.



(a) Frente (b) Verso

Figure 1.7. Suposta ficha criminal da atual presidente Dilma Rousseff publicada no jornal Folha de São Paulo em abril de 2009.

Todos os exemplos apresentados ao longo desta Seção ilustram um pouco da presença e da força das adulterações de imagens na vida das pessoas. No entanto, a AFD abrange uma quantidade de problemas muito maior do que apenas as adulterações em imagens. A próxima seção abordará alguns dos principais problemas tratados pela AFD, detalhando-os de maneira simples e concisa.

1.3. Problemas Tratados na AFD

Apesar de ganhar destaque na atualidade por atestar a autenticidade de documentos quanto a falsificações, a AFD é uma área muito mais ampla e abrange diversos outros tipos de problemas. Nesta seção faremos uma breve descrição dos alguns dos tipos de problemas mais tratados na AFD, exibindo alguns dos métodos mais recentes para tratá-los na Seção 1.4.

1.3.1. Atribuição de Fonte de Imagens (Câmeras)

Encontrar a fonte geradora de uma imagem é uma forma de verificar sua integridade e autenticidade. Isso geralmente é feito pela detecção de "marcas" deixadas na imagem pelo dispositivo gerador no momento da captura e geração da imagem, como se fosse uma impressão digital da câmera deixada nas imagens. Estas marcas geralmente são provenientes de características próprias do dispositivo gerador, como defeitos de fabricação, modo de interação entre os componentes da câmera e a luz, algoritmos de geração de imagem implementados nos componentes do dispositivo, entre outros fatores.

A atribuição de fontes de imagens é uma sub-área da AFD que desenvolve métodos para se determinar o dispositivo de origem de uma determinada imagem. Em especial pode-se desejar obter dois tipos de respostas: (i) o modelo do dispositivo que gerou uma imagem (e. g., uma imagem qualquer x foi gerada por uma câmera Nikkon D7000) ou (ii) o modelo específico responsável pela geração de uma determinada imagem (e. g., uma imagem qualquer x foi gerada por uma câmera Nikkon D7000 número de série 1234).

Focando na identificação do dispositivo que gerou uma determinada imagem, é possível garantir, por exemplo, que a informação de que uma foto foi obtida por uma câmera digital apreendida sob possessão de um suspeito poderia classificá-lo não mais como um consumidor mas sim como produtor de, por exemplo, fotos de pornografia infantil, além de garantir também que um documento foi gerado por uma câmera e não é resultado de qualquer manipulação digital.

1.3.2. Caracterização de impressoras

No cenário forense, as ferramentas mais importantes se referem à validação de evidências, ou seja, as técnicas que dão peso a um objeto apresentado como evidência de um crime de forma a permitir seu uso como prova durante o julgamento. Dentre essas ferramentas está a caracterização de dispositivo, que consiste em identificar unicamente um dispositivo (como uma câmera fotográfica ou, no caso, uma impressora) por aquilo que este dispositivo produz (fotos ou documentos impressos).

Imagine o seguinte cenário: uma equipe de investigação apreende um computador e uma impressora na casa de um suspeito que, supostamente, teria impresso um documento falso que permitiria operações ilícitas por outrém. Ao analisar o material apreendido, a equipe não encontra vestígios do documento no disco rígido do computador, nem quaisquer outros dados que liguem o suspeito à fraude, como e-mails. Restam o documento falso e a impressora.

Numa situação como essa, a caracterização da impressora pode extrair a "impressão digital" capaz de dizer se o documento apreendido foi ou não impresso nela.

Mesmo havendo um crescimento acentuado de conteúdo digital, bem como o aparecimento de ferramentas de edição e manipulação de informação poderosas e de fácil uso, o papel não está perto de se tornar obsoleto e muitas falsificações (e.g. dinheiro, documentos pessoais, contratos, cartas diplomáticas etc.) continuam sendo produzidas tendo-o como suporte.

1.3.3. Detecção de Ataque por Spoofing em Sistema de Biometria de Face

Autenticação biométrica ou biometria é uma tecnologia concernida para reconhecer humanos de maneira automática e única, baseado em suas características fisiológicas, comportamentais ou químicas. Exemplos de características incluem impressão digital, geometria da mão, veias da mão, face, íris e retina, assinatura, voz e DNA [Jain and Ross 2008]. Com aumento do volume de informações e pessoas, dos serviços baseados na web e principalmente com o aumento de fraudes e terrorismos, a necessidade por sistemas de gestão de informações em larga-escala e de controle de acesso seguro tornou-se imprescindível para a segurança da sociedade moderna. Nesse cenário, a biometria tem se destacado como uma nova abordagem de autenticação de pessoas capaz de complementar ou substituir o uso de métodos tradicionais de autenticação como senhas, palavras-chaves e cartões inteligentes.

Devido aos recentes avanços na área de reconhecimento de padrão aplicados ao reconhecimento de face, os sistemas de biometria de face tem sido aplicados em diversos problemas incluindo controle de acesso, vigilância e identificação criminal [Jain and Ross 2008, Jain and Klare 2011, Zamani et al. 2011]. No entanto, ao mesmo tempo que avanços significativos são alcançados nesta área do conhecimento, diversas técnicas de tentativas de ataques são desenvolvidas com o objetivo de enganar os sistemas de biometria. Portanto, a segurança de tais sistemas é ainda um problema em aberto, o que motiva o desenvolvimento de métodos que consigam detectar possíveis tentativas de ataques.

Embora um sistema de biometria apresente diversos pontos de vulnerabilidade, uma técnica de ataque relativamente simples de ser realizada é o ataque por *spoofing*. Uma tentativa de ataque por *spoofing* ocorre quando um usuário impostor tenta se passar por um usuário legítimo, falsificando ou mascarando os dados biométricos apresentados ao sensor de aquisição na tentativa de enganar o sistema. Como o sensor de aquisição é parte mais vulnerável (qualquer usuário tem acesso a esta parte do sistema), técnicas de ataques por *spoofing* têm se tornado mais atrativas. Além disso, alguns de nossos dados biométricos como a face estão disponíveis em redes sociais e sites pessoais, além de serem facilmente amostrados com uma câmera digital.

1.3.4. Identificação de Clonagens

Da ficção à realidade, a investigação policial retratada em séries de TV e livros inspira pesquisas. Da realidade à ficção, imagens digitais podem inspirar desconfiança e falta de credibilidade, uma vez que seu conteúdo pode ser facilmente adulterado. Contribuindo com esse ceticismo, a Clonagem (ou Cópia-Colagem) ganha um papel de destaque. Tal forma de manipulação pode ser utilizada na confecção de imagens digitais fraudulentas e com elevado grau de realismo.

O propósito da clonagem é mascarar ou multiplicar elementos presentes em uma cena como, por exemplo, folhagem, objetos e pessoas. Para isso, um segmento da imagem é copiado e uma transformação geométrica é realizada sobre este. Finalmente, o segmento duplicado é movido para outra região da mesma imagem, por vezes ocultando um elemento relevante da cena. A Figura 1.8 retrata o potencial da clonagem.

(a) (b)

Figure 1.8. Exemplo de cópia-colagem. (a) é imagem original e (b) é a imagem manipulada.

As modificações adicionais aplicadas aos segmentos clonados incluem rotação, escala, espelhamento (horizontal e vertical) e suavização completa da região ou apenas das bordas desta. A imagem como um todo também pode ser comprimida em JPEG, que é um formato de compressão com perdas, ou ser alvo de uma operação de inserção de ruídos Gaussianos. Em ambos os casos, as operações contribuem para eliminar vestígios visuais da adulteração mas, ao mesmo tempo, acrescentam um desafio extra à tarefa de detecção via mecanismos computacionais. A explicação é simples: ao se efetuar essas operações, os segmentos clonados terão seus valores, posições e quantidades de *pixels* modificados, o que tornará a correspondência entre essa região e a original (copiada) um processo mais complicado.

1.3.5. Detecção de Composições (*Splicing*)

Em AFD, o termo *splicing* define o conjunto de operações utilizados para se compor uma nova imagem à partir de partes de outras imagens já existentes. A imagem que serve de base para a composição, também conhecida como *host*, é aquela que receberá os objetos provenientes de outras imagens. Os objetos, ou partes, adicionadas à base são conhecidos como *aliens* e podem ser provenientes de diversas imagens diferentes.

Quando dizemos que uma imagem foi produzida à partir de uma composição, não nos referimos ao simples processo de cópia e colagem entre partes de imagens diferentes. As composições podem envolver um conjunto complexo de operações, como visto na Figura 1.9, a fim de enganar, de maneira eficaz, o observador. Além das operações mais básicas como rotação e redimensionamento dos seguimentos adicionados, algumas operações mais complexas envolvidas no processo de composição são definidas por [Carvalho et al. 2012]:

- **ajuste fino de bordas (*feather edges*):** este tipo de operação é realizada nas fronteiras dos objetos adicionados à base visando adequá-los às regiões da imagem onde estes são adicionados.

- **casamento de padrões de iluminação (*light matching*):** realiza o ajuste de iluminação entre a base e as partes adicionadas, de modo a homogeneizar o aspecto da iluminação da imagem.
- **realce de nitidez (*sharpening*):** este tipo de operação é empregada para realçar os objetos adicionados à imagem, de forma a deixá-los mais, ou menos, visíveis.

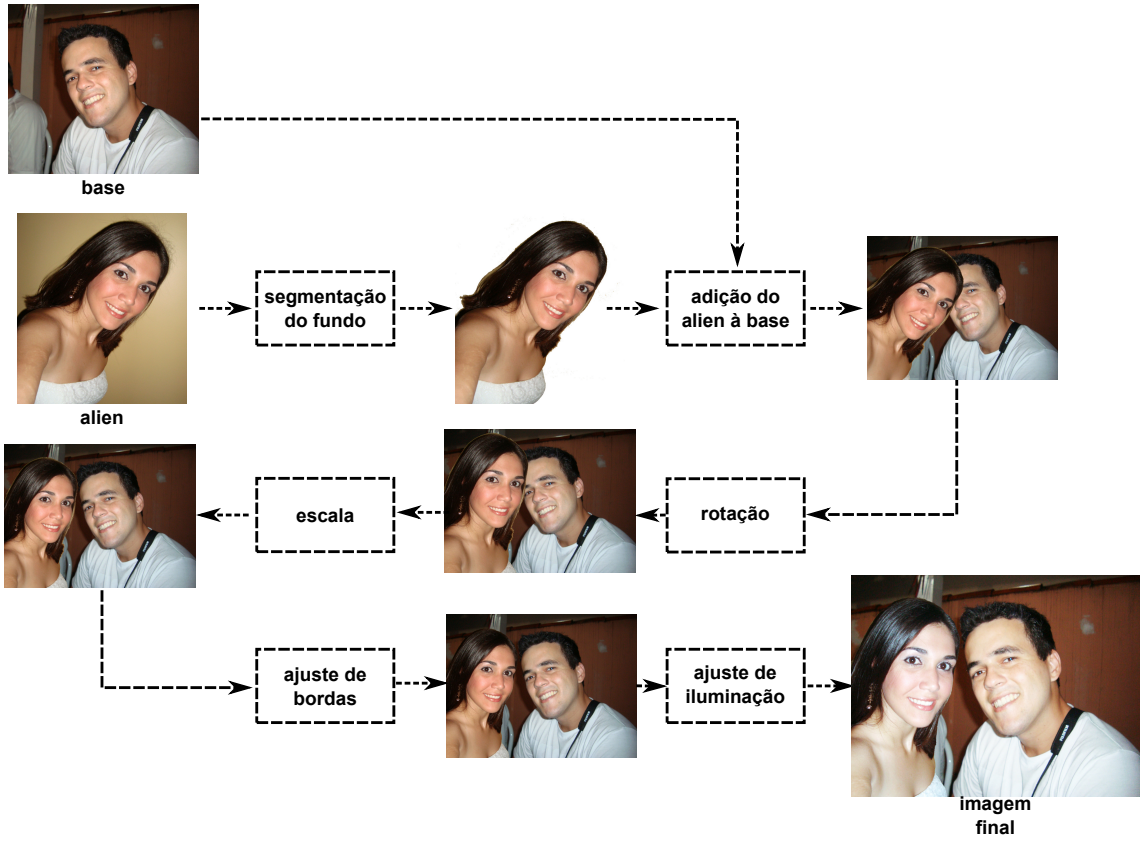


Figure 1.9. Processo de composição de imagem envolvendo um conjunto complexo de operações.

No entanto, mesmo utilizando operações sofisticadas na geração de composições, na maioria das vezes, a imagem gerada preserva algumas pequenas inconsistências, as quais podem ser exploradas para a detecção de tais composições.

1.4. Métodos Forenses para Resolução de Problemas

Na seção anterior, foram apresentados alguns dos principais tipos de problemas encontrados na AFD. A seguir, serão apresentadas algumas das mais recentes abordagens utilizadas na solução de cada um dos problemas acima citados.

1.4.1. Identificando Dispositivos Específicos

Em particular, a tarefa de se encontrar o dispositivo específico utilizado na captura de uma imagem (e não só sua marca ou modelo) é a mais estudada. Algumas propostas na literatura são voltadas para a identificação da origem de uma imagem por meio do padrão de ruído deixado na imagem pelo dispositivo [Lukas et al. 2006, Li 2010,

Goljan et al. 2008], artefatos gerados por imperfeições dos sensores de captura de um dispositivo [Kurosawa et al. 1999, Geradts et al. 2001], e presença de partículas de poeira no sensor [Dirik et al. 2008].

Pesquisas na área de atribuição de fonte geralmente são realizadas considerando um cenário fechado (*closed-set*), no qual os pesquisadores assumem que uma imagem sob investigação foi gerada por uma entre n câmeras disponíveis durante a etapa de treinamento. Na prática, uma imagem a ser avaliada pode ter sido gerada por uma câmera totalmente desconhecida que não faz parte de nosso grupo de câmeras suspeitas, o que torna importante a identificação deste fato. Portanto, é importante modelar o problema de atribuição de fontes considerando um cenário aberto (*open-set*), no qual tem-se acesso somente a um conjunto limitado de câmeras suspeitas. Assim sendo, [Costa et al. 2012] propõe uma abordagem para resolver o problema de atribuição de fonte em cenário aberto, que consiste em três etapas:

A. Definição de regiões de interesse (ROIs). De acordo com [Li and Sata 2011], diferentes regiões da imagem podem ter diferentes informações sobre o padrão de ruído da câmera. Assim, [Costa et al. 2012] consideram várias regiões de uma imagem. Para cada imagem, foram extraídas nove regiões de interesse (*Regions of Interest* – ROI) de tamanho 512×512 *pixels*, considerando regiões centrais e os cantos da imagem, de forma que a escolha dessas regiões de interesse permita trabalhar com imagens de diferentes resoluções. As regiões selecionadas são apresentadas na Figura 1.10.

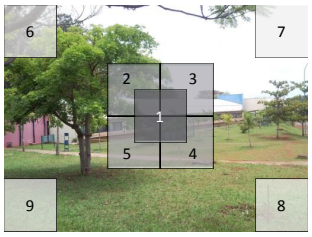


Figure 1.10. Regiões de interesse (ROIs) de dimensão 512×512 *pixels*.

B. Definição de características. Para cada região, o padrão de referência é calculado conforme apresentado em [Lukas et al. 2006], utilizando o filtro para extração de ruído no domínio da Transformada Discreta de Wavelet (DWT) proposto em [Mihcak et al. 1999], considerando os canais de cores R (vermelho), G (verde), B (azul) e o canal Y (luminância, do espaço de cor YCbCr [Wang and Weng 2000]), que pode ser considerada como uma combinação dos canais R, G e B.

Para cada ROI, o ruído residual de cada canal de cor é extraído utilizando um filtro baseado na DWT. Em seguida, calcula-se a média entre os ruídos de mesmo canal de várias imagens, gerando o padrão de ruído para cada canal de cor que representa a câmera sob investigação. Com isso, são obtidos 36 padrões de ruído para representar uma câmera. Para cada imagem, calcula-se seu ruído residual e em seguida é gerado um vetor de características considerando a correlação entre cada ROI de uma imagem e o padrão de referência correspondente para cada câmera. Com essas correlações, uma

imagem é representada por 36 características, considerando uma câmera, rotulando imagens geradas pela câmera sob investigação como a classe positiva e as câmeras restantes disponíveis como classe negativa. Observe que algumas dessas imagens serão consideradas como sendo pertencentes à classe negativa desconhecida, ou seja, são imagens geradas por câmeras às quais não se tem acesso na etapa de treinamento.

C. Atribuição de fonte em um cenário aberto. Primeiramente, é necessário encontrar um classificador para treinar um conjunto de amostras considerando a classe de interesse e outras classes as quais se tem acesso. O classificador escolhido na abordagem de [Costa et al. 2012] baseia no clássico algoritmo de Máquina de Vetores de Suporte (*Support Vector Machine* – SVM) [Bishop 2006] que transporta as amostras para um espaço de alta dimensão de forma que seja possível encontrar um hiperplano que faça a separação entre os dados da classe de interesse e das demais classes conhecidas.

Após o cálculo do hiperplano na etapa de treinamento, propõe-se um meio de classificar corretamente as classes desconhecidas por meio da movimentação do hiperplano de decisão por um valor ε se aproximando da classe positiva ou se afastando da(s) classe(s) negativa(s). A lógica é que, movendo o hiperplano é possível ser mais restritos para as amostras que se tem conhecimento como amostras positivas e, portanto, classificar qualquer outra amostra "muito diferente" como negativa (especialização), ou pode-se ser pouco rigorosos sobre o que conhecimento em relação às amostras positivas e aceitar pontos mais distantes do hiperplano como possíveis amostras positivas (generalização). Essa movimentação de plano tem como objetivo minimizar o erro de classificação na etapa de treinamento. Assim sendo, uma amostra na etapa de teste será considerada como amostra da classe de interesse se esta estiver acima do hiperplano de classificação após sua movimentação.

Para os experimentos, os autores utilizaram um conjunto de dados com 8500 imagens provenientes de 35 câmeras diferentes [5] obtendo um acerto médio de, aproximadamente, 98%, considerando um cenário onde tem-se acesso a 15 das 35 câmeras no treinamento, mas uma imagem a ser avaliada pode ter sido gerada por qualquer uma das 35 câmeras.

1.4.2. Separando Impressoras por Características de Textura

Quando um documento é impresso num processo de eletrofotografia (utilizado por impressoras *laser*), ele passa por estágios (indicados em ordem por A, B, C, D, E e F na Figura 1.11) e peças mecânicas que deixam marcas intrínsecas de cada aparelho no documento final. São essas qualidades "invisíveis" e "acidentais" que são buscadas pelos métodos de atribuição forense.

Um dos trabalhos propostos na área [Mikkilineni et al. 2004] apresenta um método de caracterização baseado em textura da área impressa. No trabalho, um banco de impressoras é usado para imprimir um conjunto de documentos que é, sem seguida, escaneado a 2400 dpi. De cada documento são extraídas as letras 'e'[6] e a partir da área

[5] O conjunto de dados é público e se encontra disponível para *download* em `http://www.recod.ic.unicamp.br/~filipe/image-source-attribution.zip`

[6] A justificativa da escolha é que essa letra é a mais comum dentre as palavras.

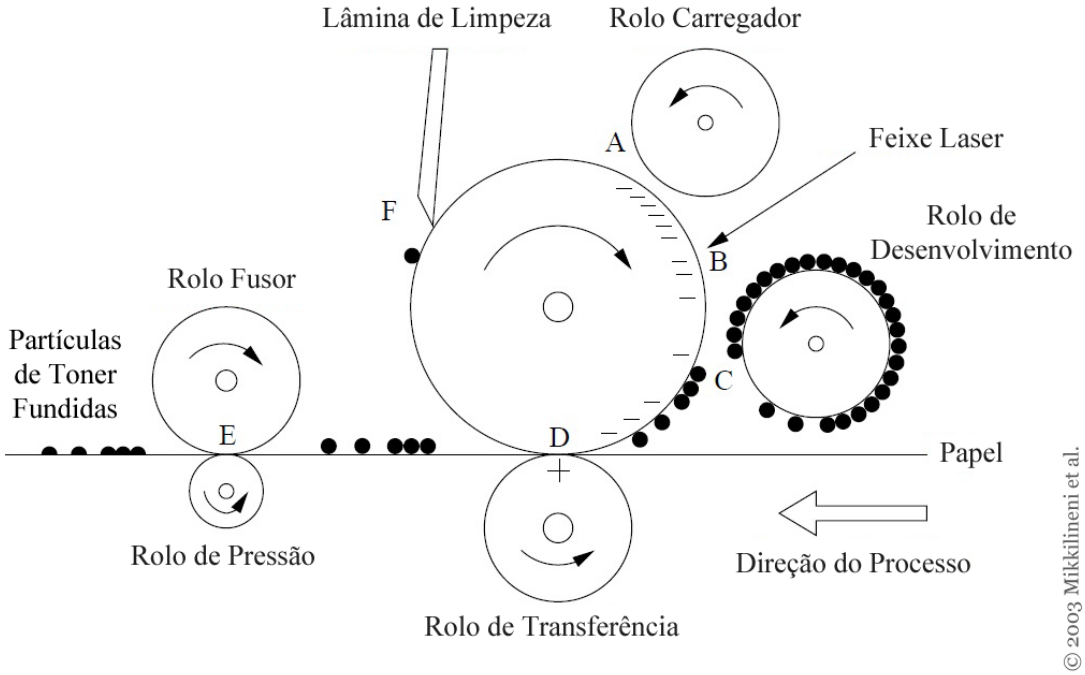


Figure 1.11. Processo de impressão impressão a *laser*: (A) carga, (B) exposição, (C) desenvolvimento, (D) transferência, (E) fusão e (F) limpeza.

impressa de cada letra é construída uma Matriz de Co-Ocorrência de Tons de Cinza (*Grayscale Co-Occurrence Matrix*, GLCM).

De posse da GLCM da área impressa, os autores calculam 22 características estatísticas, dentre elas, médias, variâncias, energia, entropias e correlações. Os vetores descritores treinam um classificador k-NN[7], que classifica os descritores dos caracteres de um documento desconhecido. O resultado é uma função mapeamento $c(\phi)$, que diz quantos caracteres são atribuídos à impressora ϕ. A classe final é o voto majoritário dessa funcão, ou seja, a classe de maior quantidade de mapeamentos. Sendo $c(\phi_1)$ e $c(\phi_2)$ as duas maiores classes, a razão entre $c(\phi_1)$ e $c(\phi_2)$ é dita *confidência* do resultado e é diretamente proporcional ao valor obtido.

Os autores reportam boa confidência nos resultados, indicando que apenas uma impressora fora confundida com frequência. Não satisfeitos, dizem suspeitar de possível redundância nas características escolhidas e que por experimentos de escolha manual de 4 delas para a classificação, viram que seria possível a redução do conjunto a um espaço de menor dimensão com características ótimas.

1.4.3. Método anti-spoofing para vídeos digitais

Considerando um sistema de biometria de face, um usuário impostor que queira se passar por um usuário legítimo pode fazê-lo de três maneiras, apresentando ao sistema: (1) uma fotografia de um usuário legítimo; (2) um vídeo de um usuário legítimo ou (3) um modelo

[7] k-NN: *k-Nearest Neighbor Classifier*. Um modelo de classificação onde a classe do elemento desconhecido é decidida observado-se a classe da maioria dos k vizinhos mais próximos.

3D da face de um usuário legítimo. Se um impostor tiver êxito no ataque utilizando qualquer uma destas abordagens, a unicidade da característica biométrica é violada, tornando o sistema vulnerável.

Com o objetivo de detectar tentativas de ataques por vídeos digitais realizado em um sistema de biometria de face com uma única câmera, [Pinto et al. 2012] propuseram um método *anti-spoofing* baseados no fato de que durante o processo de visualização dos vídeos em qualquer dispositivos de exibição são adicionados alguns artefatos como *moiring*, *flickering* e distorções. Além disso, uma amostra biométrica capturada a partir de um vídeo contém muito mais ruído do que as amostras biométricas capturadas diretamente de uma pessoa, pois ocorrência de ruídos durante o processo de amostragem e quantização de uma imagem ou vídeo digital é inevitável.

Para capturar estes artefatos, os autores propõem uma análise espectral do sinal de ruído contido no vídeo, supondo que o sistema biométrico gere um vídeo da amostra biométrica. Para isolar o sinal de ruído de um vídeo V, uma cópia deste vídeo é submetido a um processo e filtragem usando um filtro passa-baixa a fim de eliminar o ruído. Então, é realizado uma subtração entre o vídeo original e o filtrado, gerando um novo vídeo contendo somente o sinal de ruído, chamado de vídeo de ruído residual, como mostra a Equação 1.

$$V_{rudo}^{(t)} = V^{(t)} - f(V_{copia}^{(t)}) \qquad \forall\, t \in T = \{1,2,\ldots,t\}, \tag{1}$$

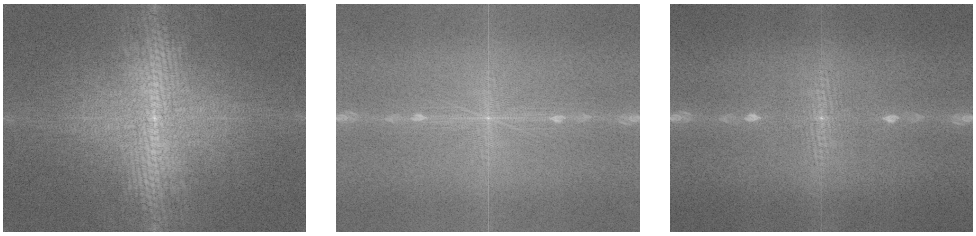
onde $V^{(t)} \in \mathbb{N}^2$ é o t-ésimo quadro de V e f é uma operação de filtragem.

A análise espectral do padrão de ruído e dos possíveis artefatos contidos no vídeo é realizada aplicando uma Transformada Discreta de Fourier 2D em cada quadro do vídeo de ruído residual e calculando seus respectivos espectros de Fourier em escala logarítmica, usando as Equações 2 e 3, respectivamente. O novo vídeo é chamado de vídeo de espectros. Pode-se notar que o logaritmo do espectro de Fourier mostrado na Figura 1.12(b-c) contém as componentes de mais alta frequência concentradas nos eixos da abscissa e da ordenada, cuja origem encontra-se no centro do quadro, diferentemente do logaritmo do espectro de Fourier mostrado na Figura 1.12(a). Isto se repete praticamente em todos os quadros. Este é um fato importante, pois a ocorrência, ou não, destes componentes nos eixos permite decidir se o dado biométrico é real ou falsificado. Para que essa decisão seja tomada de maneira automática, é projetada uma caracterização espaço-temporal usando o conceito de ritmos visuais [Chung et al. 1999, Guimaraes et al. 2001]: as informações mais relevantes de cada quadro do vídeo são amostrados e concatenados, formando uma única imagem denominada de ritmo visual.

$$\mathscr{F}(\upsilon,\nu) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} V_{(noise)}(x,y)e^{-j2\pi[(\upsilon x/M)+(\nu y/N)]} \tag{2}$$

$$\begin{aligned} |\mathscr{F}(\upsilon,\nu)| &= \sqrt{\mathscr{R}(\upsilon,\nu)^2 + \mathscr{I}(\upsilon,\nu)^2} \\ \mathscr{S}(\upsilon,\nu) &= \log(1+|\mathscr{F}(\upsilon,\nu)|) \end{aligned} \tag{3}$$

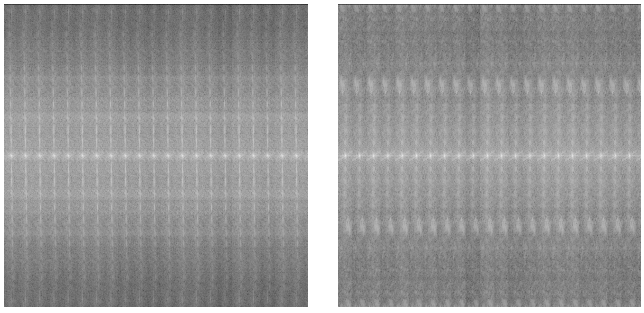
Como as informações mais relevantes para o problema encontram-se nas linhas e colunas centrais dos quadros que formam o vídeo de espectros, os autores constroem dois



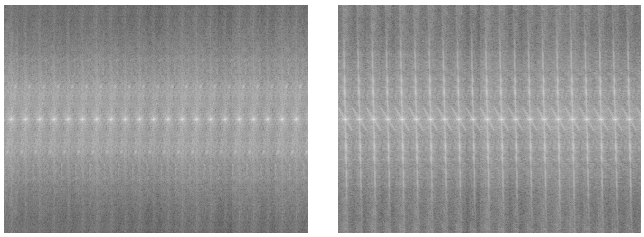
(a) (b) (c)

Figure 1.12. Exemplo de um quadro do vídeo de espectro gerado a partir de (a) um acesso válido e (b)-(c) uma tentativa de ataque considerando o filtro Gaussiano e Mediana, respectivamente.

tipos de ritmos visuais para cada vídeo: (1) ritmo visual horizontal formado pelas linhas centrais horizontais e (2) ritmo visual vertical formado pelas linhas centrais verticais. A figura 1.13 ilustra os ritmos visuais gerados, considerando um acesso válido (1.13(a) e 1.13(c)) uma tentativa de ataque (1.13(b) e 1.13(d)).



(a) Acesso válido (b) Tentativa de ataque



(c) Acesso válido (d) Tentativa de ataque

Figure 1.13. Exemplos de ritmos visuais construídos a partir (a)-(b) das linhas centrais horizontais rotacionadas de 90^o e (c)-(d) das linhas centrais verticais.

Com o propósito de resumir as informações contidas nos ritmos visuais, os autores as consideram como mapas de texturas e utilizam o descritor de textura Matriz de Co-ocorrência de Tons de Cinza (*Gray-Level Co-occurrence Matrices — GLCM*) [Haralick et al. 1973], o qual provê uma distribuição espacial e as variações de brilho de regiões da imagem, para extrair suas informações. Finalmente, é utilizado as técnicas de classificação Máquina de Vetores de Suporte (*Support Vector Machine — SVM*) [Boser et al. 1992] e Mínimos Quadrados Parciais (*Partial Least Square — PLS*) [Wold 1985] para classificar os padrões extraídos pelos descritores de textura. Os experimentos realizados para avaliação da técnica utilizaram um *Dataset* publicamente

disponível [8], contendo 700 vídeos (100 de acessos válidos e 600 de tentativa de ataques), no qual os autores obtiveram excelentes resultados.

1.4.4. Identificando Clonagens por meio de um algoritmo randomizado

A identificação de clonagem é um tema bastante explorado na literatura. As abordagens atuais adotam estratégias diversas para melhorar os resultados de detecção considerando que, possivelmente, operações específicas tenham sido usadas sobre os segmentos duplicados ou sobre a imagem completa. Assim, por exemplo, para melhorar os resultados da detecção em um cenário envolvendo compressão JPEG, a abordagem de [Popescu and Farid 2004] sugere percorrer a imagem coletando blocos de *pixels* com sobreposição. Uma matriz desses blocos é formada e a Análise de Componentes Principais (*Principal Component Analysis* – PCA) é aplicada sobre esta. Posteriormente, a matriz é ordenada lexicograficamente, visando encontrar com mais agilidade os blocos de *pixel* similares. Com PCA, as pequenas variações nos segmentos causadas pela compressão são descartadas e torna-se possível recuperar a correspondência existente entre aqueles.

A estratégia de [Silva 2012] é baseada nos algoritmos *PatchMatch* [Barnes et al. 2009] e *PatchMatch Generalizado* [Barnes et al. 2010]. Tratam-se de algoritmos randomizados que se propõem a encontrar correspondências aproximadas de *patches* (blocos de *pixels* de tamanho definido, e.g., 7×7) em uma ou mais imagens por meio das etapas de Propagação e Busca Aleatória de correspondências. Uma correspondência (ou pareamento) para um *patch* consiste em um *patch* similar a este dentro da imagem.

O *PatchMatch Generalizado* pode ser considerado uma extensão do *PatchMatch*, uma vez que se propõe a encontrar, para cada *patch* da imagem, um conjunto de K correspondências deste. As informações sobre pareamento são armazenadas em uma estrutura denominada Campo de Vizinhos mais Próximos (*Nearest Neighbor Field* – NNF), que é uma matriz com as mesmas dimensões da imagem em análise. Cada posição (x,y) do NNF é tomada como o centro de um *patch* da imagem. Além disso, o *patch* (x,y) aponta para um Max-Heap que armazena as suas correspondências. A organização desta estrutura se dá com base na distância de similaridade entre (x,y) e seus pareamentos (*patches* com menor similaridade a (x,y) estarão dispostos mais próximos da raiz do max-heap). Originalmente, o *PatchMatch Generalizado* adota uma métrica de distância baseada na Soma das Diferenças Quadradas (*Sum of Squared Differences* – SSD) entre os *patches*, mas é facilmente adaptável para o emprego de distâncias entre descritores de imagens, tais como SIFT [Lowe 1999] e SURF [Bay et al. 2006].

A abordagem de detecção de clonagens proposta por [Silva 2012] consiste em aplicar o *PatchMatch Generalizado* em uma imagem suspeita, a fim de encontrar um conjunto K de correspondências para cada um dos *patches* desta. Os pareamentos encontrados são considerados candidatos a fazerem parte da região duplicada, caso ela exista. Logo, são examinados cada um dos conjuntos de *patches* candidatos, a partir da verificação da vizinhança em que estes se encontram.

[8] http://www.ic.unicamp.br/∼rocha/pub/communications.html

O autor adota uma métrica de similaridade baseada na comparação de histogramas de intensidade/cor, uma vez que a SSD não é robusta a pequenas variações nas regiões duplicadas. Primeiramente, caso a imagem suspeita não possua informação de cor, o procedimento para cálculo da distância consiste na extração dos histogramas de intensidade de ambos os *patches* sendo inspecionados. Em seguida, calcula-se a Soma das Diferenças Absolutas (*Sum of Absolute Differences* – SAD) entre os *bins* de mesma posição. O valor desta soma indica a distância de similaridade entre os dois *patches*. Analogamente, no espaço RGB (Vermelho – *Red*, Verde – *Green* e Azul – *Blue*) calculam-se os histogramas de cada canal e um *patch* passa a ser descrito por 3 histogramas. Em seguida, efetuam-se os cálculos de SAD para os histogramas que representam a mesma componente e aplicam-se os valores encontrados na equação 4, sendo I o valor da distância de similaridade. O método é descrito a seguir e esquematizado na Figura 1.14.

$$I = 0.299R + 0.587G + 0.114B \tag{4}$$

1. Encontrar K correspondências para cada *patch* da imagem usando o*PatchMatch Generalizado*. A inicialização do NNF é aleatória;

2. Percorrer o NNF final obtido em *scan order*;

3. Examinar o Max-Heap (lista de pareamentos) de cada *patch* (x,y);

4. Caso uma correspondência (x_i,y_i), sendo $i \leq K$, de (x,y) se encontre a uma distância física deste inferior a um limiar T preestabelecido, interrompe-se a análise e passa-se para a correspondência seguinte;

5. Comparar a região ao redor do *patch* (x,y) com a região ao redor de cada uma de suas correspondências (x_i,y_i). Esta região abrange o *patch* e um acréscimo de dois *pixels* nas quatro direções. Caso um *patch* não possa crescer em quaisquer direções (e.g., borda da imagem), a mesma restrição se aplicará ao outro *patch* em comparação;

6. Caso a distância de similaridade entre ambas as regiões (ao redor de (x,y) e (x_i,y_i)) for menor do que um limiar D, ambas são assinaladas como regiões duplicadas;

7. Se uma região já foi marcada, não ocorre uma nova inspeção desta.

Nos experimentos realizados, o método contempla, além de clonagens sem transformações adicionais, operações de espelhamento horizontal e vertical e rotações de 90, 180 e 270 graus porventura aplicadas nos segmentos duplicados.

A Figura 1.15 mostra um exemplo de clonagem e o resultado de detecção encontrado pelo algoritmo proposto por [Silva 2012].

1.4.5. Detectando Composições Utilizando o Reflexo da Luz nos Olhos das Pessoas

Métodos utilizados para detecção de composições podem fazer uso de diversos tipos de inconsistências deixados na imagem ao longo do processo de composição. Entre elas, as

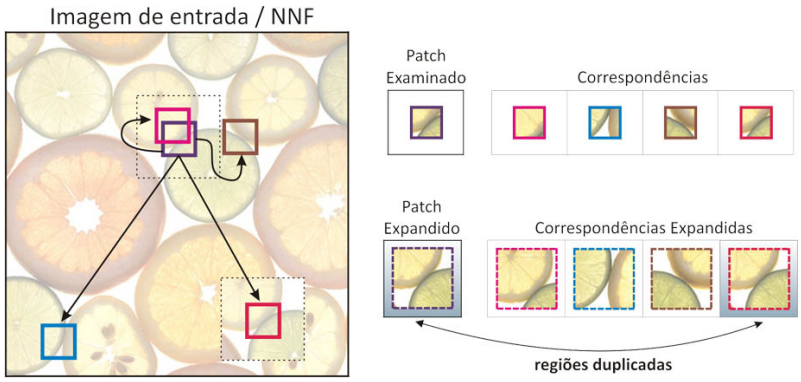
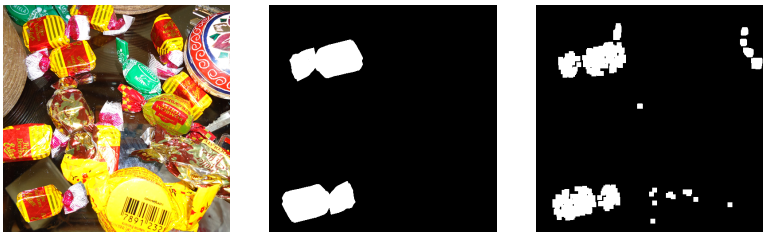


Figure 1.14. Esquematização do método proposto por [Silva 2012] para detecção de clonagens. O método examina todos os conjuntos de correspondências do NNF obtido, visando descobrir aquelas situadas em vizinhanças similares. Na Figura, a vizinhança do *patch* de borda roxa sendo avaliado é similar à vizinhança do *patch* de borda vermelha, o que indica uma duplicação.



(a) (b) (c)

Figure 1.15. Resultado de uma detecção positiva utilizando o algoritmo proposto por [Silva 2012]. (a) é a clonagem, (b) é o mapa de referência que mostra as regiões efetivamente duplicadas (em branco) e (c) é o resultado da detecção usando o método apresentado.

inconsistências de iluminação são fortemente utilizadas, uma vez que um ajuste perfeito na iluminação de uma composição é de difícil obtenção.

Em seu método para detecção de composições, em imagens envolvendo duas ou mais pessoas, os autores [Saboia et al. 2011] baseiam-se em uma extensão do artigo proposto por [Johnson and Farid 2007]. O trabalho utiliza o reflexo da luz nos olhos das pessoas para estimar: (i) a posição da fonte de luz do ambiente onde a imagem foi obtida e (ii) a posição da câmera que capturou a imagem.

O método originalmente proposto por [Johnson and Farid 2007], é provido de três estágios, os quais podem ser observados na Figura 1.16. O estágio um, é responsável por estimar a direção da fontes de luz (l_i) para cada um dos olhos de cada uma das pessoas presentes na fotografia. Assim, dadas P pessoas em uma imagem, este estágio encontrará $2P \times l_i$. A seguir, o estágio dois (caracterização) utiliza as $2P \times l_i$ para estimar a posição da fonte de luz da cena ($\dot{X}$) onde foi capturada a imagem. Uma vez calculada ($\dot{X}$), para cada l_i, onde $i \leq 2P$, é calculado o erro angular (θ_i) entre l_i e $\dot{X}$. No terceiro e último estágio, também chamado estágio de decisão, é calculado o erro angular médio (θ_m) utilizando os $2P \times \theta_i$. Esse θ_m é utilizado em um teste de hipótese clássico com 1% de significância para decidir se uma imagem sob investigação é uma composição.

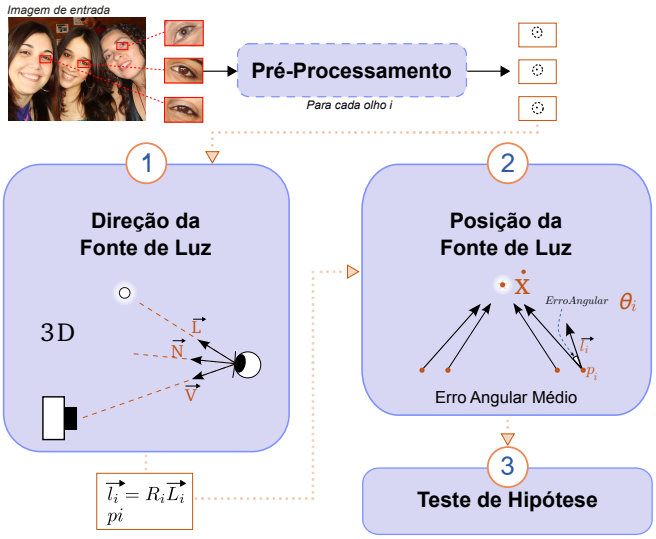


Figure 1.16. Diagrama mostrando os três estágios do método original proposto por [Johnson and Farid 2007]. Imagem retirada de [Saboia et al. 2011].

Na abordagem desenvolvida por [Saboia et al. 2011], os autores focaram em uma melhor caracterização do problema, levando em consideração não apenas a posição da fonte de luz mas também, a posição da câmera. Utilizando um *pipeline* similar ao descrito acima para calcular as posições do observador de cada olho e da cena, os autores caracterizaram cada imagem utilizando quatro características: (i) o erro angular médio relativo à direção fontes de luz, (ii) seu respectivo desvio padrão, (iii) o erro angular médio relativo à direção da câmera e (iv) seu respectivo desvio padrão.

Uma vez que a posição da fonte de luz e do observador são obtidas através de métodos não determinísticos, a cada nova estimativa de tais posições é produzida uma pequena variação em relação a uma estimativa anterior. Essa diferença também foi utilizada como forma de caracterizar as imagens. Assim, cada imagem possui diferentes estimativas das quatro características acima descritas (os autores reportaram experimentos utilizando cinco estimativas por imagem), possibilitando a substituição do teste de hipótese clássico da etapa de classificação por uma combinação de classificadores, em que cada um dos vetores de características era classificado por um classificador independente (e. g., SVM [Bishop 2006]).

A Figura 1.17 mostra um exemplo de composição e o resultado de detecção encontrado pelo algoritmo proposto por [Saboia et al. 2011].

1.5. Conclusões

Apesar do constante desenvolvimento dos métodos de computação forense aplicados no cenário forense atual, a necessidade de se estudar e propor novas soluções se faz crescer a cada dia, uma vez que para cada novo método forense desenvolvido, diversos métodos contra-forense são elaborados. Neste trabalho apresentamos uma visão geral da computação forense no panorama mundial atual, bem como alguns dos principais tipos de problemas e suas respectivas soluções dentro Análise Forense de Documentos Digitais.

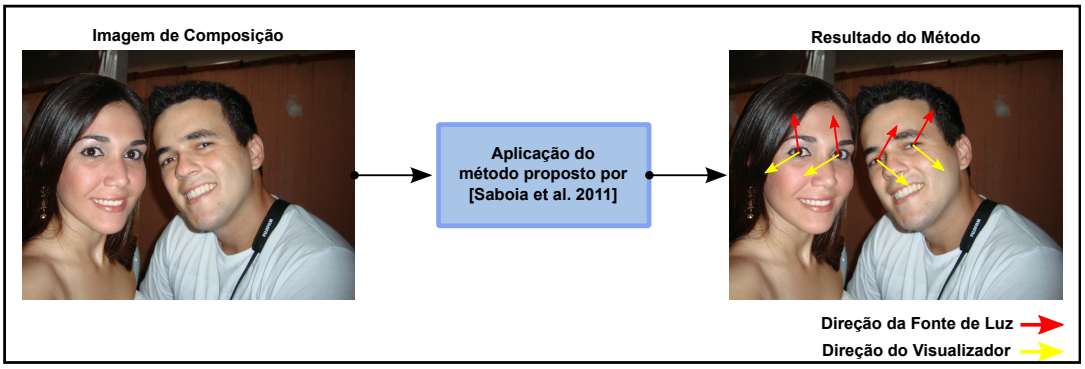


Figure 1.17. Aplicação do método proposto por [Saboia et al. 2011] em uma imagem produzida por composição. É interessante notar que, assim como pressupõe o método, as direções estimadas para o visualizador e para a fonte de luz de cada uma das pessoas apontam em direções opostas.

Baseado no método apresentado para separação de impressoras por características de textura, fica exposta a boa confidência nos resultados, indicando que apenas uma impressora fora confundida com frequência. Os autores reportam ainda uma possível redução do conjunto a um espaço de menor dimensão com características ótimas.

Identificar a origem de uma imagem é uma forma de garantir que esta não sofreu qualquer tipo de manipulação digital. Para isso, a abordagem apresentada neste trabalho utiliza informações do padrão de ruído do sensor. A abordagem considera um cenário mais realístico, denominado cenário aberto, onde uma imagem sob investigação pode ter sido gerada por qualquer dispositivo, e não somente pelos dispositivos disponíveis no momento do treinamento. Com a abordagem proposta, é possível analisar imagens de diferentes resoluções. Além disso, é possível identificar a fonte de imagens considerando métodos de caracterização complementares, tirando vantagem de todos os potenciais métodos de classificação de padrões por aprendizado de máquina.

No que diz respeito à importância de se detectar tentativas de ataque por *spoofing* em sistemas biométricos baseados em características faciais, o desenvolvimento de métodos anti-spoofing em vídeo, como o apresentado neste trabalho, é de importância vital uma vez que métodos anti-spoofing para ataque por meio de fotografia podem não ser adequados para detectar ataques por vídeo. Utilizando o espectro de Fourier da assinatura de ruído do vídeo e os ritmos visuais como mapas de texturas, o método foi capaz de capturar informações discriminativas para distinguir dados biométricos reais de falsificados. No entanto, o método apresentado ainda não foi testado em um cenário considerando tentativas de ataques mais sofisticadas, como o uso de vídeos de alta qualidade e também o uso de dispositivos como *tablets* (os quais são cada vez mais comum com a popularização desse tipo de tecnologia) para a exibição dos mesmos, tornando impossível afirmar se o método é eficaz neste tipo de cenário.

A abordagem para detecção de clonagens apresentada pode ser considerada uma estratégia que diverge bastante do foco atual da literatura, uma vez que se apoia em um mecanismo baseado em aleatoriedade. Os resultados alcançados, apesar de modestos, demonstram que a estratégia tem potencial e que pode ser expandida para contemplar outras operações, tais como escala e rotações em graus diversificados. Neste contexto,

a ideia da utilização de histogramas de intensidade/cor, que são invariantes às operações contempladas, pode ser modificada a fim de que o se possa tratar a similaridade entre *patches* (sob transformações geométricas bruscas) de maneira mais apropriada.

A detecção de composições utilizando abordagens baseadas em inconsistências de iluminação é uma grande arma a ser utilizada no cenário forense atual mas, em sua maioria, possui uma grave limitação sendo apenas possível de ser aplicada a imagens de um cenário específico. O método apresentado neste trabalho, por exemplo, é aplicável apenas em imagens contendo duas ou mais pessoas, sendo necessário que os olhos das pessoas estejam bem visíveis na imagem. Isso deixa em aberto um grande parenteses envolvendo esse tipo de método: a necessidade de se desenvolver métodos baseados em inconsistências de iluminação que possam ser aplicados em imagens sem restrições de cenário.

Agradecimentos

Agradecemos à Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Microsoft Research, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes) e Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo financiamento dessa pesquisa.

References

[Barnes et al. 2009] Barnes, C., Shechtman, E., Finkelstein, A., and Goldman, D. B. (2009). Patchmatch: A randomized correspondence algorithm for structural image editing. *ACM ToG*, pages 24:1–24:11.

[Barnes et al. 2010] Barnes, C., Shechtman, E., Finkelstein, A., and Goldman, D. B. (2010). The generalized patchmatch correspondence algorithm. In *ECCV*, pages 29–43.

[Bay et al. 2006] Bay, H., Tuytelaars, T., and Van Gool, L. (2006). Surf: Speeded up robust features. In *ECCV*, pages 404–417.

[Bishop 2006] Bishop, C. M. (2006). *Pattern Recognition and Machine Learning, 1st edition*. Springer.

[Boser et al. 1992] Boser, B. E., Guyon, I. M., and Vapnik, V. N. (1992). A Training Algorithm for Optimal Margin Classifiers. In *Workshop on Computational Learning Theory*, pages 144–152.

[Carvalho et al. 2012] Carvalho, T., Silva, E., Costa, F. O., Ferreira, A., and Rocha, A. (2012). Além do óbvio: a análise forense de imagens e a investigação do conteúdo implícito e explícito de fotografias digitais . In *XII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*.

[Chung et al. 1999] Chung, M.-G., Lee, J., Kim, H., Song, S. M.-H., and Kim, W.-M. (1999). Automatic Video Segmentation based on Spatio-Temporal Features. *Korea Telecom*, 1(4):4–14.

[Costa et al. 2012] Costa, F. O., Eckmann, M., Scheirer, W. J., and Rocha, A. (2012). Open set source camera attribution. In *SIBGRAPI*, pages 71–78.

[Dirik et al. 2008] Dirik, A. E., Sencar, H. T., and Memon, N. (2008). Digital single lens reflex camera identification from traces of sensor dust. *IEEE T.IFS*, 3(3):539–552.

[Farid 2009] Farid, H. (2009). *Deception: Methods, Motives, Contexts and Consequences*, chapter Digital Doctoring: Can We Trust Photographs?, pages 95–108.

[Geradts et al. 2001] Geradts, Z. J., Bijhold, J., Kieft, M., Kurosawa, K., Kuroki, K., and Saitoh, N. (2001). Methods for identification of images acquired with digital cameras. *Enabling Technologies for Law Enforcement and Security*, 4232:505–512.

[Goldenstein and Rocha 2009] Goldenstein, S. and Rocha, A. (2009). High-profile forensic analysis of image. In *3rd International Conference on Imaging for Crime Detection and Prevention*.

[Goljan et al. 2008] Goljan, M., Fridrich, J., and LukÃ¡š, J. (2008). Camera identification from printed images. In *SPIE Conference on Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, volume 6819.

[Guimaraes et al. 2001] Guimaraes, S. J. F., Couprie, M., Leite, N. J., and Araujo, A. A. (2001). A Method for Cut Detection Based on Visual Rhythm. In *Brazilian Symposium on Computer Graphics and Image Processing*, pages 297–304.

[Haralick et al. 1973] Haralick, R., Shanmugam, K., and Dinstein, I. (1973). Texture Features for Image Classification. *IEEE Trans. on Systems, Man, and Cybernetics*, 3(6).

[Jain and Klare 2011] Jain, A. and Klare, B. (2011). Matching Forensic Sketches and Mug Shots to Apprehend Criminals. *Computer*, 44(5):94–96.

[Jain and Ross 2008] Jain, A. K. and Ross, A. (2008). *Handbook of Biometrics*, chapter Introduction to Biometrics, pages 1–22. Springer.

[Johnson and Farid 2007] Johnson, M. and Farid, H. (2007). Exposing Digital Forgeries Through Specular Highlights on the Eye. In *Information Hiding*, pages 311–325.

[Kurosawa et al. 1999] Kurosawa, K., Kuroki, K., and Saitoh, N. (1999). CCD fingerprint method – identification of a video camera from videotaped images. In *IEEE ICIP*, pages 537–540.

[Li 2010] Li, C.-T. (2010). Source camera identification using enhanced sensor pattern noise. *IEEE T.IFS*, 5(2):280–287.

[Li and Sata 2011] Li, C.-T. and Sata, R. (2011). On the location-dependent quality of the sensor pattern noise and its implication in multimedia forensics. In *ICDP*, pages 1–6.

[Lowe 1999] Lowe, D. G. (1999). Object recognition from local scale-invariant features. In *ICCV*, page 1150.

[Lukas et al. 2006] Lukas, J., Fridrich, J., and Goljan, M. (2006). Digital Camera Identification from Sensor Pattern Noise. *IEEE T.IFS*, 2:205–214.

[Mihcak et al. 1999] Mihcak, M. K., Kozintsev, I., Ramchandran, K., and Moulin, P. (1999). Low-complexity image denoising based on statistical modeling of wavelet coefficients. *IEEE Signal Processing Letters*, 6(12):300–303.

[Mikkilineni et al. 2004] Mikkilineni, A. K., Pei-Ju Chiang, P.-J., Ali, G. N., Chiu, G. T.-C., Allebach, J. P., and Delp, E. J. (2004). Printer identification based on textural features. In *Intl. Conference on Digital Printing Technologies*, pages 306–311.

[Pinto et al. 2012] Pinto, A., Pedrini, H., Schwartz, W. R., and Rocha, A. (2012). Video-Based Face Spoofing Detection through Visual Rhythm Analysis. In *Brazilian Symposium on Computer Graphics and Image Processing*.

[Popescu 2004] Popescu, A. (2004). *Statistical Tools for Digital Image Forensics*. PhD thesis, Department of Computer Science, Dartmouth College.

[Popescu and Farid 2004] Popescu, A. C. and Farid, H. (2004). Exposing digital forgeries by detecting duplicated image regions. Technical Report TR 2004-515, Dept. of Computer Science – Dartmouth College, Hanover, USA.

[Rocha and Goldenstein 2010] Rocha, A. and Goldenstein, S. (2010). CSI: Análise Forense de Documentos Digitais. *Atualizações em Informática (JAI)*, pages 263–317.

[Rocha et al. 2011] Rocha, A., Scheirer, W., Boult, T. E., and Goldenstein, S. (2011). Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics. *ACM Computing Surveys*, 43:1–42.

[Saboia et al. 2011] Saboia, P., Carvalho, T., and Rocha, A. (2011). Eye Specular Highlights Telltales for Digital Forensics: a Machine Learing Approach. In *IEEE ICIP*, pages 1937–1940.

[Silva 2012] Silva, E. A. (2012). Identificação de Manipulações de Cópia-Colagem em Imagens Digitais. Master's thesis, Instituto de ComputaÃ§Ã£o - Universidade Estadual de Campinas.

[Wang and Weng 2000] Wang, X. and Weng, Z. (2000). Scene abrupt change detection. In *Canadian Conference on Electrical and Computing Engineering*, pages 880–883.

[Wold 1985] Wold, H. (1985). Partial Least Squares. In Kotz, S. and Johnson, N., editors, *Encyclopedia of Statistical Sciences*, volume 6, pages 581–591. Wiley, New York.

[Zamani et al. 2011] Zamani, N., Darus, M., Abdullah, S., and Nordin, M. (2011). Multiple-frames Super-resolution for Closed Circuit Television Forensics. In *Intl. Conference on Pattern Analysis and Intelligent Robotics*, volume 1, pages 36–40.