Análise forense de documentos digitais: além da visão humana

Digital document forensics: beyond the human vision

Ewerton Almeida Silva[1], Anderson Rocha[2]

Silva EA, Rocha A. Análise forense de documentos digitais: além da visão humana. Saúde, Ética & Justiça. 2011;16(1):9-17.

RESUMO: As ferramentas de *hardware* e *software* atuais promovem, cada vez mais, a criação de falsificações com alto grau de realismo. Adulterações fraudulentas em documentos digitais podem ser facilmente executadas visando enganar seus observadores. Neste artigo, exploramos o campo de pesquisas denominado *Análise Forense de Documentos*, enfatizando os aspectos ético-legais acerca da adulteração em imagens digitais. Examinamos, também, alguns dos mais interessantes casos de falsificação já registrados em contextos diversos, tais como na política, em pesquisas científicas e na Medicina Forense. Finalmente, mostramos algumas abordagens da literatura que podem ser aplicadas na tarefa de discernir entre um documento digital autêntico e uma falsificação.

DESCRITORES: Documentos; Processamento de imagem assistida por computador/ética; Má conduta científica/ética; Medicina legal. Fotografia/recursos humanos.

Mestrando em Ciência da Computação, Universidade Estadual de Campinas (UNICAMP).
Professor Doutor, Instituto de Computação, Universidade Estadual de Campinas (UNICAMP).
Endereço para correspondência: e-mail: ewerton.silva@students.ic.unicamp.br, anderson.rocha@ic.unicamp.br

INTRODUÇÃO

A capacidade inventiva e a habilidade de transformar ideias em situações concretas são características humanas que não devem ser subestimadas. Neste contexto, o computador, que ganhou popularidade e se tornou mais acessível e poderoso, é uma ferramenta quase indispensável na tradução dessas ideias em artefatos da realidade. Contudo, ao mesmo tempo em que a capacidade de criar parece não ter limites, a habilidade de distinguir o que é realidade e o que não é parece seguir o caminho inverso.

A tecnologia atual permite produzir falsificações em documentos digitais com muita facilidade, mesmo para usuários com reduzida experiência no assunto. Isso se deve, principalmente, ao pouco trabalho requerido para efetuar manipulações indevidas utilizando ferramentas de *software* como Adobe Photoshop®, GIMP, Corel Draw® entre outras. Além disso, a expansão das tecnologias de captura de dados, tais como câmeras, *scanners* e filmadoras, permitiu às pessoas, bem intencionadas ou não, adquirirem maior interação com imagens e vídeos digitais, tornando seu manuseio uma tarefa ordinária.

Segundo Rocha e Goldenstein[16], de maneira geral, alterações em imagens e vídeos digitais podem ser analisadas em dois âmbitos distintos. De um lado existem as modificações cujo intuito é melhorar a qualidade visual e estética do documento, proporcionando uma visualização agradável de seu conteúdo. Neste caso, destaca-se o emprego de operações de pós-processamento que são efetuadas de maneira global no vídeo ou na imagem, tais como ajuste de brilho e contraste, realce de nitidez, suavização, rotação e redimensionamento. Por exemplo, em uma foto de família, um indivíduo poderia ajustar o brilho da cena ou ampliá-la como um todo de maneira a adequá-la para ser colocada em uma moldura. Por outro lado, existem alterações cujo objetivo é iludir os observadores do documento digital quanto ao seu verdadeiro conteúdo.

Sem necessidade de muita sofisticação, é possível usar as operações de pós-processamento supracitadas como um instrumento malicioso na criação de imagens e vídeos que correspondam a situações inverossímeis. Se um indivíduo mal-intencionado desenvolvesse, por exemplo, uma composição de imagens na qual um suspeito aparecesse na cena de um crime, a fotografia em questão poderia ser considerada como prova cabal, numa corte de justiça, de que tal suspeito teve participação no ato criminoso.

A falsificação de imagens tem sido presente em diversos meios tais como ciência, jornalismo, política, *marketing* etc. No que diz respeito à ciência, Richardson et al.[13] destacam que é simples alterar uma imagem médica com propósitos obscuros. Além disso, adulterações ilícitas comprometem a interpretação de evidências e laudos médicos: a imagem de um corpo pode ser digitalmente modificada com a finalidade de dificultar sua análise ou de exercer alguma influência no resultado dos exames.

Farid[4] destaca algumas implicações no uso de adulterações em imagens científicas. Segundo o autor, estima-se que aproximadamente 20% das publicações aceitas em alguns periódicos científicos contém manipulações de imagem inapropriadas, sendo que 1% destas contém alterações de caráter fraudulento. Em virtude desses dados alarmantes, editores têm procurado elevar seus critérios de aceitação para assegurar a credibilidade dos trabalhos que publicam. Todavia, ainda que as políticas dos periódicos e conferências sejam aprimoradas e que estas sejam seguidas por uma maior consciência por parte dos autores dos trabalhos, faz-se imprescindível a utilização de técnicas computacionais que indiquem a existência de falsificações em documentos digitais.

Ter o conhecimento necessário para diferenciar um documento digital autêntico de uma falsificação é de grande importância. Ao atentar para o fato de que muitas adulterações são difíceis de serem desvendadas a olho nu, Farid[5] evidencia os principais objetivos da área de pesquisa conhecida como *Análise Forense de Documentos* (AFD): o desenvolvimento e o aprimoramento de métodos computacionais que revelem e apontem possíveis manipulações em documentos digitais tais como imagens e vídeos.

Um dos grandes desafios da AFD é a detecção de operações de *composição*[1] e *clonagem*[2]. Tais operações são simples de efetuar e geram resultados satisfatórios visualmente. Além disso, se efetuadas por profissionais,

1. A composição consiste na combinação de elementos de dois ou mais documentos digitais diferentes em um único documento. Por exemplo, uma composição de imagens pode agregar, em uma única cena, duas pessoas que nunca estiveram no mesmo local num mesmo momento.
2. A clonagem caracteriza-se pela ocultação de elementos presentes em um documento digital por segmentos do mesmo documento. Um exemplo típico de clonagem em imagens consiste em mascarar partes de um objeto da cena com regiões que se assemelham a texturas, como folhagem e areia.

tais operações podem ser difíceis de revelar, mesmo empregando-se métodos computacionais sofisticados. Neste contexto, o surgimento de abordagens contra-forenses mais competentes e difíceis de destrinchar é uma conseqüência direta do progresso no desenvolvimento de técnicas forenses computacionais. Dado que este ponto também engloba circunstâncias legais, ampliaremos seu debate nas seções posteriores.

Neste trabalho, enfatizamos os aspectos ético-legais acerca da adulteração de imagens. Apresentamos, na Seção 2¸ alguns dos casos dignos de nota já registrados nos meios de comunicação e suas implicações; em particular, destacamos alguns casos relacionados à Medicina Legal. Na Seção 3, discutimos algumas abordagens da literatura que visam discernir entre fabricações e documentos autênticos, e apresentamos os desafios em aberto. Por fim, na Seção 4, discutimos algumas conclusões.

HISTÓRICO E FATOS

Uma das primeiras manipulações de imagem de que se tem notícia é datada de 1857, pouco depois do aparecimento da fotografia (em 1814, por Nicéphore Niepce), quando o francês Oscar G. Reijland produziu uma composição analógica conhecida como *The two ways of life* a partir de 30 fotografias[16]. O regime soviético comandado por Stalin e Lênin também contribuiu com bons exemplos de adulterações em fotografias. De acordo com Popescu[12], com o propósito de preservar a imagem dos ditadores, antigos aliados eram eliminados de registros fotográficos a fim de evidenciar que tais alianças nunca ocorreram.

Todas essas manipulações (analógicas) passavam por procedimentos demorados e requeriam alto grau de habilidade e conhecimento técnico, além de equipamentos sofisticados para sua execução, estando, por isso, fora do alcance do cidadão comum[12].

Recentemente, com a difusão do computador e de equipamentos para aquisição de imagens e vídeos, tornou-se menos custoso e demorado criar tais falsificações. Utilizando ferramentas de *software* adequadas como, por exemplo, o Adobe Photoshop®, é possível reproduzir com facilidade muitas das operações que, no passado, levavam horas ou mesmo dias para serem realizadas manualmente e de forma precisa. Tal facilidade tem levado diversos pesquisadores, tais como Sencar e Memon[20], a atentar para o fato de que a sociedade tem, continuamente, se aproximando de uma situação na qual não é possível garantir a autenticidade e integridade de uma imagem ou vídeo digital. Por conseguinte, percebe-se uma diminuição da credibilidade de documentos digitais quando considerados como evidências numa corte de justiça, como registros médicos, ou mesmo como documentos financeiros.

Farid[6], por sua vez, ressalta que não é mais possível acreditar cegamente no conteúdo de imagens, devido ao surgimento da tecnologia digital. O autor destaca que a adulteração de imagens tem sido empregada com frequência por tablóides, pela indústria da moda, campanhas políticas ou, ainda, resultados de pesquisas científicas. Nos últimos anos, o campo da *Análise Forense Digital* tem auxiliado a determinar a autenticidade desses documentos digitais fornecendo técnicas para identificar anomalias estatísticas introduzidas no nível dos menores elementos de uma imagem, os *pixels*.

O impacto social decorrente da alteração indevida de imagens é, por vezes, relacionado à ocultação e invenção de informações e fatos. Um exemplo pertinente é datado de abril de 2009, quando a imagem de uma suposta ficha criminal da então ministra da Casa Civil do Brasil Dilma Rousseff foi estampada num conhecido periódico brasileiro. A ficha relatava a participação da ministra, à época, em assaltos e planejamentos de sequestros durante o Regime Militar Brasileiro. Uma análise técnica, contudo, revelou que o documento era uma fabricação[15]. A Figura 1 ilustra a análise de variabilidade entre as letras provenientes da suposta ficha criminal e de um padrão de referência obtido de outras fichas reais datadas do período em questão (1965-1970) e disponíveis no Arquivo Público de São Paulo (APM-SP). A baixa similaridade entre as letras do padrão e do documento inspecionado forneceu pistas de que este último se tratava de uma fabricação.

Em um exemplo mais recente[2], em setembro de 2010, o periódico egípcio *Al-Ahram*, um dos jornais de maior circulação daquele país, publicou uma imagem na qual o presidente egípcio, Hosni Mubarak caminhava num tapete vermelho à frente dos líderes dos Estados Unidos, Palestina, Israel e Jordânia. Na fotografia original, em contraste, Hosni Mubarak situava-se atrás dos demais representantes de Estado. Com a manipulação, o jornal intencionou ampliar a importância do presidente egípcio nas negociações de paz no Oriente Médio, colocando-o em posição de liderança no grupo como mostra a Figura 2.

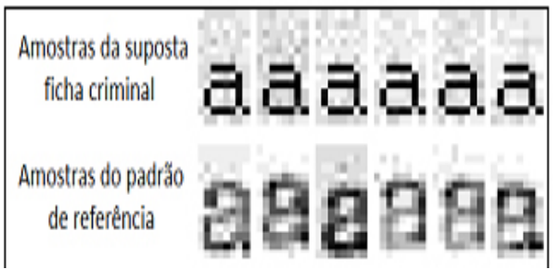

Figura 1. Análise da variabilidade entre amostras de letras "a" provenientes da suposta ficha criminal e do padrão de referência produzido a partir de fichas reais da mesma época. Para que a ficha fosse procedente do Arquivo Público de São Paulo, como alegado, ela deveria ter sido digitalizada com auxílio de um scanner que, invariavelmente, capturaria pequenas distorções nas letras decorrentes, principalmente, do envelhecimento e padrões de datilografia, como ilustram as amostras do padrão de referência em detrimento das amostras da suposta ficha criminal[15]. A análise efetuada conclui que, muito provavelmente, as amostras da suposta ficha criminal não foram datilografadas e sim inseridas computacionalmente com o auxílio de algum software de edição de imagens. Imagem adaptada de Rocha e Goldenstein[15]

Figura 2. Imagem original na qual o presidente do Egito, Hosni Mubarak, situa-se atrás dos demais líderes de Estado (esquerda) e a imagem adulterada (direita). Originais publicados em BBC[2] e GettyImages (Disponível em: http://www.gettyimages.com)

Falsificações nos meios de informação, tais como a efetuada pelo jornal egípcio, visam influenciar os leitores de maneira a formar falsas opiniões sobre determinados fatos e assuntos. O trabalho de Sacchi et al.[19] fortalece a hipótese de que imagens digitalmente manipuladas podem afetar as lembranças dos cidadãos. Os autores realizaram experimentos com vários participantes, que foram requisitados a descrever alguns eventos públicos com base em falsas fotografias. Dentre as cenas retratadas estava o protesto pacífico contra a guerra no Iraque ocorrido na cidade de Roma em 2003. Segundo os autores, participantes que visualizaram fotografias do evento que o retratavam como sendo violento e negativo tenderam a recordar supostos confrontos e lesões aos manifestantes, que, na verdade, nunca ocorreram. Este fato demonstra a suscetibilidade da mente humana à distorção de idéias e opiniões, principalmente mediante fotografias e estímulos visuais.

No âmbito científico, fraudes em imagens digitais também têm sido usadas para encobrir ou ampliar resultados de pesquisas. Um dos casos mais divulgados se deu em 2005, quando o professor Woo-Suk Hwang, da *Seoul National University*, e equipe publicaram o que aparentava ser um enorme avanço nos estudos referentes a células-tronco. No artigo, publicado pela *Science*, Hwang afirmava ter clonado, com sucesso, células-tronco embrionárias a partir de material genético extraído de pessoas com enfermidades. Investigações revelaram que dentre as onze colônias de células-tronco que Hwang afirmara ter gerado, apenas duas eram autênticas. As demais haviam sido geradas digitalmente por meio de adulterações em fotografias envolvendo as duas únicas colônias verdadeiras[4,17,22]. A Figura 3 mostra uma das diversas evidências de fraude descobertas no trabalho de Hwang et al.[7].

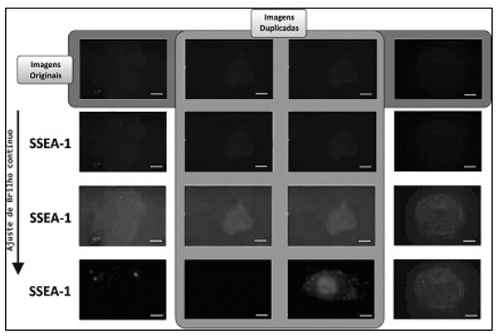

Figura 3. Evidência de fraude no trabalho de Hwang et al.[7]. Uma operação de ajuste de brilho revelou que as duas imagens centrais (em destaque) mostradas no trabalho são idênticas, a menos de pequenas variações nos *pixels* ocasionadas, possivelmente, pela compressão diferenciada das duas imagens. Imagem adaptada de Baron[1]

Outro caso que recebeu visibilidade por parte da mídia e da comunidade acadêmica se deu em 2007, quando a revista científica americana *Science* se retratou, novamente, por um trabalho publicado anteriormente pelo periódico. Coincidentemente, tal trabalho[3] também apresentava resultados com

grandes implicações nas pesquisas em células-tronco. No referido trabalho, o professor R. Michael Roberts e colegas da *Missoury University* indicavam a possibilidade de diferenciar células de embriões de ratos nas células que formariam a placenta e naquelas que fariam parte do feto em estágios precoces da divisão celular. No entanto, investigações apontaram que algumas imagens essenciais do trabalho haviam sido alteradas indevidamente[21].

O uso incorreto de operações de manipulação de imagens digitais em trabalhos científicos pode levar à abertura de processos contra as entidades e pessoas envolvidas nas pesquisas. Um estudo realizado em 2010 e publicado no *Journal of Medical Ethics* mostrou que, aproximadamente, 25% dos trabalhos divulgados e retratados em periódicos médicos continham fabricações e falsificações de dados. Segundo o estudo, a maior parte dos artigos contendo dados manipulados foi publicada em revistas científicas de alto prestígio. Este fato aponta que, possivelmente, algumas das razões para a criação de tais embustes é a pressão da academia e dos órgãos de fomento por publicações em periódicos com elevada influência, além das promessas de cargos melhores, maiores investimentos nas pesquisas, ou mesmo o cancelamento destes[10].

Rossner e Yamada[18] apresentam e debatem algumas diretrizes para alterações em imagens adotadas por periódicos importantes no campo da Biologia. Os autores mostram exemplos de adulteração de imagem baseados em casos reais (Figuras 4 e 5) referentes à pesquisas nessa área do conhecimento.

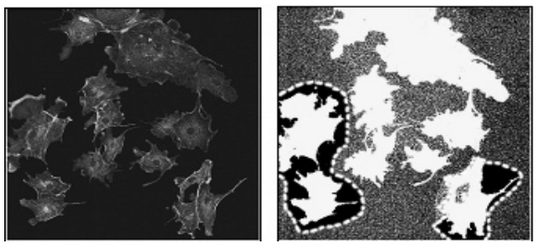

Figura 4. Exemplo de manipulação baseado em um caso real, na qual vários campos microscópicos foram combinados em uma única imagem, à esquerda. Esta falsa representação dos dados pode ser revelada com o auxílio de uma operação de ajuste de contraste, que torna visíveis as regiões inseridas e os seus recortes (áreas escuras da imagem à direita). Imagens extraídas de Rossner e Yamada[18]

Ainda no contexto científico, Richardson et al.[13] salientam que imagens médicas radiológicas são potenciais alvos de manipulações ilegais. Em termos práticos, uma radiografia pode ser digitalmente modificada de modo a destacar e minimizar determinados artefatos de interesse ou, ainda, removê-los totalmente da imagem. Com isso, indivíduos mal-intencionados poderiam amplificar resultados de pesquisas científicas, tornando-os mais convincentes.

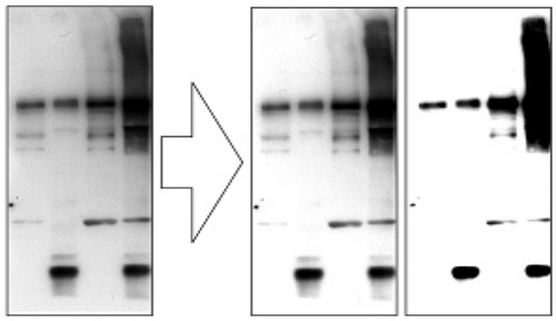

Figura 5. Exemplos de manipulações baseados em um caso real. A imagem à esquerda sofre contínuo ajuste de contraste, resultando nas imagens do centro e da direita. A imagem do meio pode ser considerada aceitável, uma vez que não oculta nenhum elemento da imagem original, ao passo que a imagem da direita provê uma interpretação errônea dos dados (artefatos importantes foram removidos). Imagem adaptada de Rossner e Yamada[18]

Outro caso grave plausível envolveria a apresentação de uma evidência legal, por parte de um médico, de que seu paciente não possuía uma dada enfermidade no momento da radiografia, abstendo-se de suas responsabilidades. A Figura 6 mostra um exemplo de manipulação fraudulenta em uma imagem radiológica, no qual os sinais (metástases) de uma enfermidade foram movidos de lugar e/ou eliminados por meio de da operação de clonagem (cópia-colagem). A Figura 7 apresenta um exemplo de radiografia no qual um tumor foi completamente eliminado empregando-se operações análogas às efetuadas na Figura 6.

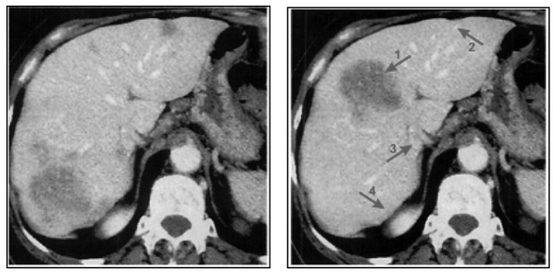

Figura 6. Imagens radiológicas do cérebro humano original (esquerda) e manipulada (direita) na qual as metástases (regiões escuras) indicadas pelas setas foram trocadas de posição (1) ou removidas (2, 3 e 4). Imagem adaptada de Richardson et al.[13]

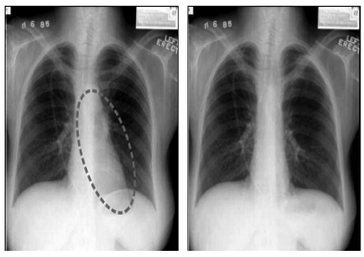

Figura 7. Possível manipulação em uma radiografia. O tumor pulmonar é completamente removido da imagem original (à esquerda) por meio da operação de clonagem (cópia-colagem), e o resultado é mostrado na imagem da direita. Imagem adaptada de Farid[4]

Na Seção 3, a seguir, descrevemos com mais detalhes alguns métodos para a identificação de manipulações em imagens digitais, tais como as apresentadas anteriormente.

DESVENDANDO MANIPULAÇÕES

A facilidade cada vez maior de efetuar modificações em imagens digitais é um dos fatores que guiam as pesquisas em *Análise Forense de Documentos*. Nos últimos anos, esta área de pesquisa tem atraído interesse da mídia, periódicos científicos, órgãos de governo e, mesmo, dos indivíduos que protagonizam falsificações. Neste último caso, o objetivo dos falsificadores é desenvolver manipulações de imagens não detectáveis por meio dos métodos da AFD.

A cópia-colagem é uma operação de manipulação de imagem simples de realizar. Por meio dela, pode-se ocultar, duplicar ou mesmo mover um objeto de posição na cena usando os elementos desta. Revelar este tipo de edição, entretanto, pode ser complicado, uma vez que ela é usualmente complementada com operações de suavização de bordas, rotação e redimensionamento nas regiões duplicadas.

Ferramentas para edição de imagens tais como Photoshop® e GIMP favorecem a execução das operações supracitadas de maneira rápida e precisa, tal como por meio da ferramenta de carimbo (*Clone Stamp*). Adicionalmente, elas fornecem métodos aprimorados de cópia-colagem que tornam as manipulações muito mais reais. Bons exemplos disso são as ferramentas *Content-Aware Fill* e *Spot Healing Brush*, integrantes do Photoshop CS5®, que são usadas para preenchimento automático de regiões da imagem. O preenchimento leva em conta o conteúdo ao redor das áreas em questão. A Figura 8 ilustra o resultado da aplicação dessas funcionalidades.

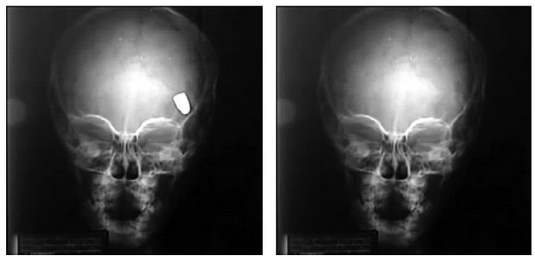

Figura 8. Remoção de uma evidência (bala) de uma radiografia por meio de cópia-colagem. A região da imagem original (à esquerda) contendo a bala é mascarada com o auxílio das ferramentas *Content-Aware Fil* e *Spot Healing Brush* do Photoshop® CS5, e o resultado é apresentado na imagem da direita. Imagem original (esquerda) Disponível em: http://folhadeagenda.blogspot.com

Diversos trabalhos têm buscado aperfeiçoar a identificação de cópia-colagem para os mais variados casos, porém, atenção especial tem sido dada às operações de rotação, principalmente pela característica desafiadora deste problema. Rotações são frequentemente empregadas para conferir à manipulação um aspecto visual mais convincente. Em particular, os métodos de Pan e Lyu[11] e Wang et al.[23] representam grandes avanços no reconhecimento das regiões duplicadas quando elas estão rotacionadas em diferentes graus. A Figura 9 apresenta um exemplo de clonagem no qual o segmento duplicado foi levemente rotacionado.

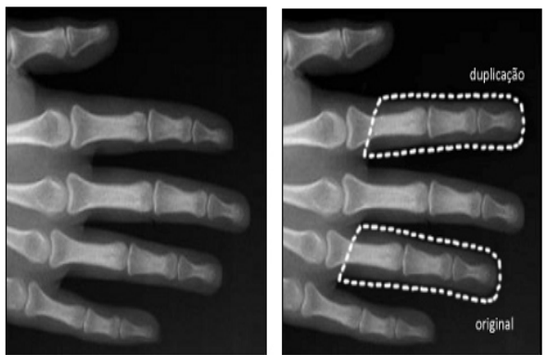

Figura 9. Exemplo de cópia-colagem seguida de uma operação de rotação. O dedo anular mostrado na imagem original (à esquerda) é copiado, levemente rotacionado e, por fim, colado no lugar do dedo indicador, como mostra a imagem da direita. Neste exemplo, a ferramenta *Spot Healing Brush* do Photoshop® CS5 também foi empregada para ajustar as bordas do segmento duplicado, assim como a ferramenta *Clone Stamp.* Imagem original (esquerda) Disponível em: http://dedalus.odo.br/dsp_notc.asp?cod=134

Outros grandes desafios referem-se à detecção de cópia-colagem em imagens comprimidas em JPEG, que é um tipo de compressão com per-

das que modifica o valor dos *pixels* da imagem, e nas situações em que tal manipulação é realizada por meio de métodos de preenchimento automático de regiões, tal como *Content-Aware Fill*. O problema principal das abordagens forenses existentes é que, muitas vezes, as falsificações utilizadas nos experimentos são bem simples, envolvendo duplicações de blocos de *pixels* relativamente grandes. Logo, para falsificações mais bem elaboradas e realísticas que utilizam variadas operações de edição de imagens, os métodos forenses tendem a apresentar resultados pouco satisfatórios.

Outra forma ordinária de manipular imagens é a partir da composição de elementos de duas ou mais imagens distintas numa única cena. Similarmente à cópia-colagem, este tipo de manipulação pode ser executado sem muito esforço por meio de ferramentas de *software* para edição de imagens. O Photoshop®, por exemplo, fornece ferramentas sofisticadas para seleção de objetos, tais como *Magnetic Lasso*, *Quick Selection* e *Magic Wand*, e permite o trabalho com várias camadas de imagens simultaneamente.

Recentemente, métodos avançados para seleção de objetos em imagens têm surgido na literatura. Tais abordagens visam elevar a precisão na localização das bordas dos objetos a partir de pequenas marcações grosseiras feitas pelos usuários ao redor e dentro dos objetos de interesse. *Lazy Snapping*[8] e *Paint Selection*[9] são exemplos desses métodos.

Para lidar com tais falsificações e manipulações, pesquisadores na área de *Análise Forense de Documentos* têm desenvolvido métodos computacionais cada vez mais sofisticadas. Algumas abordagens para revelar composições de imagens analisam a compatibilidade da função de resposta da câmera (*Camera Response Function*) em diversos pontos (bordas dos objetos) da cena, a iluminação nesta ou, ainda, buscam por artefatos de reamostragem dentro da imagem. Em Medicina Legal, tais abordagens poderiam ser utilizadas previamente à execução de atividades periciais, tal como a identificação humana, para garantir a autenticidade das imagens disponíveis. Entretanto, nem sempre há necessidade do uso dessas técnicas. Como ilustra a Figura 4, um simples ajuste de brilho foi suficiente para mostrar, visualmente, artefatos suspeitos de tal manipulação.

O trabalho de Rocha[14] representa um grande passo no desenvolvimento de técnicas para resolver o problema da detecção de composições. O autor descreve um método para diferenciar imagens naturais de imagens geradas em computador que apresenta bons resultados. Isto é conseguido por meio de: (i) uma forma de caracterização e descrição de imagens baseado na introdução de "perturbações" controladas em determinadas regiões daquelas e (ii) um classificador de padrões que se encarrega de diferenciar imagens naturais e sintéticas, a partir das informações de cada imagem fornecidas pela etapa de descrição. Acreditamos que tal método tem potencial aplicação no que se refere às composições de imagens, uma vez que seria possível utilizar aquele descritor em conjunto com um classificador de padrões para categorizar uma imagem em uma de duas classes: autêntica ou resultante de composição.

Rocha[14] também propõe a criação do *Stegi@Work*, um *framework* distribuído para detecção de mensagens escondidas em imagens. Essas mensagens são inseridas de modo a permanecerem secretas e não identificáveis visualmente pelos observadores da imagem. O propósito principal é transmitir uma informação importante através de um meio pouco suspeito. Dado que a inserção não altera significativamente a imagem (é bastante improvável que um indivíduo possa perceber o efeito visual da inserção da mensagem), faz-se necessário o uso de métodos computacionais para revelar a presença de tais informações secretas. As implicações são elevadas, e órgãos do governo (principalmente da área de segurança) e a imprensa têm se interessado por este tema.

O modelo arquitetural do *Stegi@Work* pode ser aplicado à resolução dos desafios da AFD referentes à cópia-colagem e à construção de composições. Neste contexto, o *framework* teria o propósito de vasculhar grandes volumes de imagens digitais em busca de rastros que apontem a presença de edições inapropriadas, provendo dados e evidências de diferentes métodos forenses. A grande vantagem de um *framework* desse tipo é a descentralização das tarefas, que propicia difundir os dados de entrada (e.g., imagens e vídeos) e analisá-los em diferentes estações de trabalho. Isto aceleraria a obtenção dos resultados, que poderiam ser baseados em diversos métodos da literatura, por vezes combinados.

CONCLUSÕES

A *Análise Forense de Documentos* despertou, nos últimos anos, como uma das mais desafiadoras e promissoras áreas de pesquisa dentro da computação devido, principalmente, à necessidade crescente de se autenticar documentos digitais. Neste trabalho, apresentamos diversos casos legais nos quais manipulações impróprias em imagens geraram implicações éticas profundas. No meio

científico, publicações impactantes nos dão falsas esperanças com dados e imagens falsificados. Na mídia, fabricações procuram alterar nossas opiniões e a forma como visualizamos uma situação em particular, iludindo-nos. Em Medicina Legal, alterações fraudulentas em imagens (evidências) podem mudar todo o panorama de um processo judicial, favorecendo incorretamente determinados indivíduos.

Há muito ainda o que fazer na AFD. Métodos forenses surgem e, pouco tempo depois, já se tornam obsoletos com as atualizações das ferramentas de edição de imagens. Também não se pode desmerecer a capacidade humana para criar falsificações cada vez mais realísticas e difíceis de serem descobertas. Assim, apresentamos alguns métodos para criar e desvendar manipulações em imagens digitais, os desafios em aberto e abordagens potencialmente eficientes para a detecção de composições. Além disso, identificamos como necessária a construção de um *framework* distribuído para melhorar e acelerar as tomadas de decisão sobre documentos digitais em casos legais.

Finalmente, voltamos à questão ética para ressaltar que apenas mediante um esforço combinado entre pesquisadores, publicitários, peritos e pessoas ligadas aos governos e à imprensa, além do próprio usuário comum de ferramentas de edição de imagens, será possível diminuir o número de casos de fraudes nos diversos meios de informação. Os casos de falsificações na ciência ensinaram que o prestígio de um autor deve ser levado em conta, mas seus trabalhos devem ser analisados com o mesmo cuidado despedido em um trabalho de um autor ainda desconhecido. Afinal, o que está em jogo não é apenas uma carreira de sucesso, mas o avanço da ciência como um todo e a melhoria da vida dos cidadãos.

Silva EA, Rocha A. Digital document forensics: beyond the human vision. Saúde, Ética & Justiça. 2011;16(1):1-8.

ABSTRACT: With the current hardware and software technology, document falsification with increasingly high degree of realism has been promoted. Fraudulent forgery in digital documents can be easily performed in order to deceive the observer. This article addresses the Digital Document Forensics research field, emphasizing ethical and legal implications of adulteration in digital images. It also presents some of the most interesting cases of forgery in different contexts such as in politics, scientific research and Forensic Medicine. Finally, it sheds light on some literature approaches which can be used to discern between genuine and fake digital documents.

KEY WORDS: Documents; Image processing, computer-assisted/ethics; Scientific misconduct/ethics; Forensic medicine; Photography/manpower.

REFERÊNCIAS

1. Baron C. Weird science: faux findings. Boston: Thompson Course Technology; 2008. cap.6, p.157-184: Adobe photoshop forensics: sleuths, truths and fauxtography.
2. BBC Mid-East. Egyptian newspaper under fire over altered photo [citado em set. 2010]. Available from: www.bbc.co.uk/news/world-middle-east-11313738.
3. Deb K,Sivaguru M, Yong HY, Roberts RM. *Cdx2* gene expression and Trophectoderm lineage specification in mouse embryos. Science. 2006;311(5763):992-6.
4. Farid H. Exposing digital forgeries in scientific images. ACM Multimedia and Security Workshop; 2006. p.29-36.
5. Farid H. Digital image forensics. Scientific Am (SCIAM). 2008;298(6):66-71.
6. Farid H. Image forgery detection: a survey. IEEE Signal Processing Magazine. 2009;26(2):16-25.
7. Hwang W, et al. Patient-specific embryonic stem cells derived from human SCNT blastocysts. Science. 2005;311(5729):1777-83.
8. Li Y, Sun J, Tang C, Shum H. Lazy Snapping. ACM Transact Graph (ToG). 2004; 23(3):303-308.
9. Liu J, Sun J, Shum H. Paint selection. ACM Trans Graph (ToG). 2009;28(3):1-7.
10. MedicineNet. U.S. Scientists Commit Most Research Fraud [cited 2010 Nov.]. Available from: http:www.medicinenet.com/script/main/art.asp?articlekey=122237.
11. Pan X, Lyu S. Detecting image region duplication using SIFT features. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2010. p.1706-9.
12. Popescu AC. Statistical tools for digital image forensics [tese]. Hannover, NH: Department of Computer Science, Dartmouth College; 2004.
13. Richardson ML, Frank MS, Stern EJ. Digital

image manipulation: What constitutes acceptable alteration of a radiologic image? Am J Roentgenol. 1995;164(1):228-9.

14. Rocha A. Classifiers and machine learning techniques for image processing and computer vision [tese]. Campinas: Instituto de Computação, Universidade Estadual de Campinas (UNICAMP); 2009.
15. Rocha A, Goldenstein S. High-profile forensic analysis of images. In: International Conference on Imaging for Crime Detection and Prevention (ICDP); 2009. p.1-6.
16. Rocha A, Goldenstein S. CSI: análise forense de documentos digitais. Belo Horizonte: Sociedade Brasileira de Computação (SBC); 2010. cap. 6, p.263-317: Atualizações em informática.
17. Rocha A, Scheirer W, Boult TE, Goldenstein S. Vision of the unseen: current trends and challenges in digital image and video forensics. ACM Computing Surveys (CSUR). 2011 [prelo].
18. Rossner M, Yamada KM. Hwang case review committee misses the mark. J Cell Biol. 2004;166(1):11-5.
19. Sacchi DL, Agnoli F, Loftus EF. Changing history: doctored photographs affect memory for past public events. Appl Cognit Psychol. 2007;21(8):249-73.
20. Sencar T, Memon N. Overview of state-of-the-art in digital image forensics. World Scientific Press; 2008. cap. 15, p.325-348: Algorithms, architecture and information systems security.
21. USAToday. 'Science' retracts research for doctored photos [cited 2007 July]. Available from: www.usatoday.com/tech/science/genetics/2007-07-27-science-retracted-article_N.htm.
22. Veja Online. Este homem é um farsante [citado em jul. 2006]. Disponível em: http://veja.abril.com.br/110106/p_082.html.
23. Wang J, Liu G, Li H, Dai Y, Wang Z. Detection of image region duplication forgery using model with circle block. IEEE Intl. Conference on Multimedia Information Networking and Security (MINES). 2009;1:25-9.

Recebido em: 04/02/2011
Aprovado em: 02/03/2011