AUTENTICIDADE DE FOTOGRAFIAS DIGITAIS

Everaldo Henrique Diniz

Bacharel em Engenharia Eletrônica pela Universidade de Brasília (UnB).
Especialista em Ciências Forenses IFAR/LS
E-mail: diniz.everaldo@gmail.com

Palavras-chave: Autenticidade de Fotografias, Forense Digital, Análise de Fotografias Digitais.

INTRODUÇÃO

Nas últimas décadas, houve enorme crescimento da utilização de imagens digitais devido à evolução das câmeras e à presença delas nos celulares. Simultaneamente, também se observou o incremento do uso de *softwares* de edição de imagem em virtude da popularização e barateamento de programas de edição, como o *photoshop*. A partir dessa popularização da tecnologia digital, tornou-se cada vez mais comum a manipulação de fotografias digitais, dificultando o atesto de sua autenticidade (SWAMINATHAN; WU; LIU, 2008). Adulterações em imagens, na maioria das vezes, são feitas com o intuito de melhorar sua qualidade visual e estética. Contudo, há intervenções feitas com o fito de iludir os destinatários do documento digital em relação ao seu verdadeiro conteúdo (SILVA; ROCHA, 2011). Essas alterações nas fotografias costumam ser feitas por meio da mescla, que consiste na mistura de duas imagens, ou da clonagem, a qual consiste na utilização de pedaços da mesma imagem para esconder ou aumentar a quantidade de objetos (ROCHA et al., 2011). As implicações da adulteração de fotos ultrapassam o mero dissabor com a potencial imprecisão do documento, podendo inclusive dar origem ou embasar contestações judiciais. Dessa forma, mostra-se importante a conceituação de documento: objeto corporal resultado da atividade humana capaz de conservar vestígios e que, por meio da apreensão de sinais gráficos, luz ou som, pode representar, de forma permanente, um fato existente fora de seu conteúdo ao observador. Igualmente relevante é a análise do vocábulo sob o

prisma jurídico, no qual representará prova documental, ou seja, a afirmação de um fato escrita ou gravada, como em um contrato ou em uma fotografia (NEVES, 2016). A fotografia digital se enquadra, desse modo, como espécie de prova documental, conforme disposição do §1º do art. 422 do Novo Código de Processo Civil, Lei 13.105 (BRASIL, 2015). Tal dispositivo, juntamente com o art. 225 do Código Civil, Lei 10.406 (BRASIL, 2002), determina que a fotografia faz prova daquilo que reproduz, mas, caso seja contestada, deve-se apresentar sua autenticação eletrônica ou, não sendo possível, deve ser realizada sua perícia (ARAUJO, 2010). É importante ainda destacar que, excetuado o artigo 241-C do Estatuto da Criança e Adolescente (ECA), Lei 8.069 (BRASIL, 1990), que proíbe a adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual relacionada à simulação de criança ou adolescente em cenas de sexo, não há regulamentação da manipulação fotográfica. Observe-se que, ainda assim, a conduta pode ser enquadrada em outros crimes, como a injúria e a difamação (AUAD, 2013). Apesar da inexistência de tipificação específica da conduta de adulteração de imagens, é inegável que ela pode impactar fortemente a sociedade, a exemplo do que aconteceu em abril de 2009, quando foi forjada ficha criminal de Dilma Rousseff, até então Ministra da Casa Civil (SILVA; ROCHA, 2011). Existe a necessidade de diferentes técnicas para identificar cada estilo de alteração gráfica, uma vez que adulterações de alta qualidade não são detectáveis a olho nu (FARID, 2008).

OBJETIVO

Devido ao número crescente de fotografias digitais adulteradas, este estudo tem por objetivo levantar técnicas capazes de contribuir amplamente no campo da ciência forense detectando fraudes em fotografias digitais.

METODOLOGIA

Foi realizada pesquisa no banco de dados do Google Acadêmico utilizando com as palavras-chave: “autenticidade fotográfica”, “fraudes fotográficas”, “perícia digital” e “perícias fotográficas”. Entre os trabalhos encontrados, foram escolhidos os mais relevantes, recentes e que abordam diferentes técnicas de reconhecimento de fraudes fotográficas.

RESULTADOS E DISCUSSÃO

Uma primeira forma de garantir que um arquivo digital não foi alterado é a criação de uma assinatura digital do arquivo, a chamada HASH. Qualquer modificação feita no arquivo depois da criação da HASH irá substituí-la, permitindo a detecção da fraude. Portanto, trata-se de uma boa técnica para se utilizar na cadeia de custódia de documentos digitais (SAMPAIO, 2007). Já para o início de uma investigação a respeito da autenticidade de uma fotografia digital, é conveniente a utilização da análise do Exif (*Exchangeable image file format*), que é anexado à imagem pela própria câmera. Este arquivo apresenta informações importantes para a perícia, como o fabricante, o modelo da câmera, a localização na hora da fotografia (via GPS) e a utilização ou não de *flash*. Contudo, a análise do Exif se mostra inviável em alguns casos, tendo em vista que diversos programas de transferência o descartam para reduzir o tamanho do arquivo. Em relação à detecção de mesclagem, uma das técnicas mais utilizada é a análise de luz e sombra. Como na mesclagem são utilizadas duas imagens diferentes para criar uma nova, é improvável que ambas apresentem fontes luminosas nas mesmas posições. Assim, foram desenvolvidos algoritmos que calculam a origem da luz em diferentes objetos. Caso haja diferença, será esta a prova de que houve alteração (ROCHA et al., 2011). Ainda no caso da mesclagem, para que as duas imagens se encaixem de maneira que pareçam pertencer à mesma foto, são feitos o redimensionamento e a rotação das imagens (POPESCU; FARID, 2005). Estas operações geram uma correlação entre os pixels da parte adulterada identificável por meio do algoritmo matemático de maximização da expectativa (EM), tornando possível encontrar evidências de adulteração (ARAUJO, 2010). Quanto à clonagem, uma forma de detectá-la em uma imagem é por meio da pesquisa exaustiva, na qual é procurada, parte a parte da imagem, uma cópia dela. Não obstante, outra forma mais eficiente é a técnica de utilização de uma janela que percorre toda a imagem calculando a transformada discreta de cosseno. Por meio desta técnica, fica viável, de forma mais célere, detectar inclusive cópias não exatas (ROCHA et al., 2011). As câmeras digitais comuns utilizam a matriz de Bayer ao fazerem o registro das cores, ou seja, só é feita a captura do valor da luminescência de uma cor por pixel. Como as fotografias possuem três cores por pixel (vermelho, verde e azul), as

outras cores são obtidas por interpolação, o que gera uma correlação entre pixels vizinhos. Portanto, ao se fazer qualquer mudança na fotografia original perde-se essa correlação entre os pixels, o que é um forte indício de adulteração (SWAMINATHAN; WU; LIU, 2008). Há ainda outro método, que utiliza os olhos da pessoa fotografada. Apesar das íris dos olhos serem circulares, quando uma pessoa aparece na foto deslocada do centro óptico, seus olhos ficam ligeiramente elípticos. Portanto, se uma pessoa apresenta os olhos com o formato diferente do esperado para a posição em que ela se encontra, pode-se concluir que essa pessoa foi colocada ali a partir de outra foto ou que a mudaram de posição. Esse procedimento também pode ser utilizado para outros objetos com o formato conhecido (FARID, 2008). Igualmente por meio dos olhos, é possível analisar a iluminação que forma pontos brancos nos olhos e, dependendo da posição desse ponto, estimar a posição da fonte de luz. Assim, examinando-se todos os olhos de uma fotografia, e identificando-se alguma diferença de iluminação ambiente entre eles, haverá prova de adulteração (FARID, 2008). Outro método utilizado pela perícia de imagens é a utilização de algoritmo que detecte a dupla compressão em JPEG, uma vez que fotos não adulteradas normalmente passam apenas uma vez pelo processo de compressão (ARAUJO, 2010). Existe também a possibilidade de se verificar a autenticidade de uma imagem a partir das peculiaridades das lentes das câmeras. As lentes possuem diferentes índices de refração para diversos comprimentos de ondas luminosas, o que é chamado de aberração cromática. Essa aberração cromática é proporcional à distância do centro óptico, sendo viável estimar tal aberração. Ao se mudarem as posições de objetos na imagem ou acrescentarem objetos, as aberrações cromáticas das partes alteradas fogem do padrão do resto da foto (JOHNSON; FARID, 2006). Outro procedimento muito utilizado é o da análise dos ruídos das fotografias. As fotografias digitais possuem ruído espalhado uniformemente, porém na falsificação é comum a adição de ruídos para esconder imperfeições e, com isso, tornando o padrão de ruído inconsistente, denunciando a região fraudada (ARAUJO, 2010). Por fim, foi desenvolvida outra forma de garantir a autenticidade da fotografia, que é a inserção de uma assinatura especial que não se modifica mesmo com a compressão JPEG (LIN; CHANG, 2001).

CONCLUSÃO

Com as facilidades presentes nos novos *softwares,* a tendência é de que as fraudes em fotografias digitais continuem a aumentar. Contudo, existem múltiplas técnicas que, juntas, proporcionam relevante conjunto de ferramentas para desmascarar as manipulações gráficas.

REFERÊNCIAS

SWAMINATHAN, A.; WU, Min; LIU, K.j.r.. Digital image forensics via intrinsic fingerprints. **Ieee Transactions On Information Forensics And Security,** [s.l.], v. 3, n. 1, p.101-117, mar. 2008. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/tifs.2007.916010.

SILVA, Ewerton Almeida; ROCHA, Anderson. Análise forense de documentos digitais: além da visão humana. **Saúde, Ética & Justiça,** v. 16, n. 1, p.9-17, 7 jun. 2011. Universidade de Sao Paulo Sistema Integrado de Bibliotecas - SIBiUSP. http://dx.doi.org/10.11606/issn.2317-2770.v16i1p9-17.

ROCHA, Anderson et al. Vision of the unseen. **Acm Computing Surveys,** v. 43, n. 4, p.1-42, 1 out. 2011. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/1978802.1978805.

BRASIL. Lei Nº 13.105. Brasília, 16 mar. 2015.

BRASIL. Lei Nº 10.406. Brasília, 10 jan. 2002.

BRASIL. Lei Nº 8.069. Brasília, 13 jul. 1990.

ARAUJO, Juliana Cristina Busnardo Augusto de. **Fotografia digital como prova no processo:** Aspectos tecnológicos. 2010. Disponível em: <http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=8787&revista_caderno=21>. Acesso em: 11 jan. 2017.

AUAD, Guilherme Cal. TÉCNICAS DE PERÍCIA FORENSE EM FOTOGRAFIAS DIGITAIS. Brasília, out. 2013.

FARID, Hany. Digital Image Forensics. **Scientific American,** [s.l.], v. 298, n. 6, p.66-71, jun. 2008. Springer Nature. http://dx.doi.org/10.1038/scientificamerican0608-66.

SAMPAIO, Marcelo. A FOTOGRAFIA DIGITAL E SEU VALOR LEGAL NA PERÍCIA OFICIAL. **Prova Material: REVISTA CIENTÍFICA DO DEPARTAMENTO DE POLÍCIA TÉCNICA DA SECRETARIA DA SEGURANÇA PÚBLICA DO ESTADO DA BAHIA,** Bahia, v. 8, n. 4, p.19-22, dez. 2007.

POPESCU, A.c.; FARID, H.. Exposing digital forgeries by detecting traces of resampling. **Ieee Transactions On Signal Processing,** [s.l.], v. 53, n. 2, p.758-767, fev. 2005. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/tsp.2004.839932.

JOHNSON, Micah K.; FARID, Hany. Exposing digital forgeries through chromatic aberration. **Proceeding Of The 8th Workshop On Multimedia And Security - Mm&sec; '06,** [s.l.], p.48-55, set. 2006. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/1161366.1161376.

LIN, Ching-yung; CHANG, Shih-fu. A robust image authentication method distinguishing JPEG compression from malicious manipulation. **Ieee Transactions On Circuits And Systems For Video Technology,** [s.l.], v. 11, n. 2, p.153-168, 2001. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/76.905982.