O que os olhos não veem
Estudo de um algorítimo para detectar imagens digitais manipuladas

André Guaraldo*
Giuliano Pinheiro†
Oscar Esgalha‡
Anderson Rocha§

Abstract

Imagens digitais fazem parte do cotidiano de muitas pessoas, raras são as que não possuem acesso à essa tecnologia. Devido à essa ubiquidade, cresce, em ritmo acelerado, a qualidade dos softwares de edição de imagens, bem como as técnicas para a manipulação das mesmas. Em uma realidade na qual uma imagem pode servir de prova em um caso jurídico, é importante haver meios para se identificar imagens fraudulentas para garantir a integridade do caso. A evolução das fraudes, impossibilita, muitas vezes, essa identificação simplesmente através da observação, mesmo para olhos treinados. É necessário o desenvolvimento de algorítimos para esse fim. O nosso trabalho implementa e testa um algorítimo para identificar imagens alteradas por resampling (i.e rotação, redimensão) proposto por Popescu [1] e tenta melhorá-lo.

1. Introdução

No passado, quando existiam apenas imagens analógicas, manipular imagens exigia técnicas manuais complexas, muito tempo, cuidado e paciência de quem o fosse fazer. O simples ato de remover uma pessoa de uma foto exigia uma grande quantidade de trabalho e de tempo (muitas horas, às vezes dias) na sala escura. Em vista disso manipulações de imagens eram raras e, muitas vezes, limitada à operações governamentais ou militares. [2]

Nos últimos anos, todavia, computadores e câmeras digitais ficaram cada vez melhores e mais acessíveis, bem como *softwares* de edição de imagens, (*Adobe Photoshop* e *GNU Gimp*[1], por exemplo). [1] Atualmente muitas pessoas possuem acesso à imagens digitais e manipulá-las pode ser feito por qualquer um em poucos minutos. Com um mínimo de técnica em um software de edição, uma pessoa pode alterar significativamente uma imagem, em poucos minutos, de modo que isso não seja perceptível à olho nu.

Figura 1. Fotos originais (esquerda) e imagem manipulada (direita) por Brian Walski.

O uso de tais softwares para fins banais, como correção de iluminação, remoção de olhos vermelhos, entre outros, não interessa à computação forense. Entratanto, a partir do momento em que uma manipulação de imagem tem algum objetivo malicioso, é de grande interesse conseguir confirmar a autenticidade da imagem. A facilidade em manipular imagens, diminuiu a credibilidade da mesma nos tribunais. [3] Em um caso jurídico no qual a evidência mais forte para inocentar ou criminalizar uma pessoa seja uma imagem, é necessário conseguir separar as fraudes de imagens autênticas.

Imagens fraudadas também aparecem na mídia, com o intuito de mostrar uma situação sob outra perspectiva, como aconteceu com o fotógrafo Brian Walski em 2003 no jornal

*Is with the Institute of Computing, University of Campinas (Unicamp). **Contact**: ra101487@students.ic.unicamp.br
†Is with the Institute of Computing, University of Campinas (Unicamp). **Contact**: ra108579@students.ic.unicamp.br
‡Is with the Institute of Computing, University of Campinas (Unicamp). **Contact**: ra108231@students.ic.unicamp.br
§Is with the Institute of Computing, University of Campinas (Unicamp). **Contact**: anderson.rocha@ic.unicamp.br

[1] Adobe Photoshop e GNU Gimp são softwares registrados com suas respectivas licenças por seus respectivos autores


UM JORNAL A SERVIÇO DO BRASIL ★ ★ ★ WWW.FOLHA.COM.BR

FOLHA DE S.PAULO

DIRETOR DE REDAÇÃO: OTAVIO FRIAS FILHO — DOMINGO, 5 DE ABRIL DE 2009 — EDIÇÃO SÃO PAULO, CONCLUÍDA ÀS 21H00 ★ R$ 4,00

história

CAPTURADO

Ficha de Dilma Rousseff no Dops

Grupo de Dilma planejou sequestro de Delfim Netto

Antonio Spinoza, ex-colega de ministra (Casa Civil), diz que o grupo armado que dirigiram teve como alvo o titular da Fazenda em 1969.

A ação chegou a ter data e local definidos. Um napa da emboscada consta de processo no STM. Dilma, hoje aliada de Delfim, negou de forma "peremptória". "Ele fantasiou. Não me lembro disso." Pág. A8

Brasil gasta com 'spread' 2,5 vezes o orçamento da Saúde

Estudo calcula que pessoas físicas e jurídicas pagaram R$ 134,5 bi em 2008

Em 2008, os brasileiros gastaram R$ 134,5 bilhões em "spread" bancário —diferença entre a taxa paga pelo banco e a que é aplicada em empréstimos a consumidores. O valor é duas vezes e meia o orçamento do Ministério da Saúde no período.

Segundo estudo feito pela Fecomercio-SP (Federação do Comércio do Estado de SP), as pessoas físicas foram responsáveis por R$ 85,4 bilhões do total, e as empresas, por R$ 49,1 bilhões. O "spread" bancário no Brasil é o mais alto do mundo.

No cálculo do "spread" estão impostos, risco de inadimplência, custos e lucro. Considerando empréstimo pessoal de R$ 1.000 a ser quitado em um ano, dos R$ 604 que o cliente de banco pagava de juros em 2008, R$ 475 equivaliam ao "spread".

O governo Luiz Inácio Lula da Silva criou um grupo que reúne técnicos do Ministério da Fazenda e do Banco Central para estudar maneiras de reduzir a margem bancária. Para especialistas, a diminuição vai demandar tempo. Pags. B3 e B5

Otan anuncia plano de enviar 5 mil militares ao Afeganistão

MARCELO NINIO

Líderes europeus vão en-

Figura 2. Falsa ficha criminal da então chefe de estado Dilma Rousseff no jornal Folha de São Paulo.

Los Angeles Times. [2] Como pode ser observado na **Figura 1**, na montagem à direita o soldado britânico parece estar orientando um iraquiano com uma criança no colo, mas, como pode ser visto nas imagens originais, à esquerda, esse momento nunca aconteceu. Assim que a fraude foi descoberta, o fotógrafo foi demitido.

Outro exemplo, é o caso da ficha criminal de Dilma Rousseff, que no dia 5 de abril de 2009 saiu no jornal Folha de São Paulo (ver Figura 2). Segundo a ficha, a então chefe de estado, teve participação ativa na resistência durante o regime militar, planejando roubos e sequestros. Foi afirmado que o documento vinha do arquivo público de São Paulo, portanto, que era autentico. Entretanto, uma análise forense realizada na imagem revelou que a imagem da ficha não provinha de um scanner, além de possuir outras características típicas de imagens criadas em computador, counclui-se que a ficha era falsa. [4]

Além de imagens serem fraudadas para alimentar o sensacionalismo da mídia, é comum, em época de eleições principalmente, surgirem imagens fraudadas com políticos em situações não louváveis ou se encontrando com pessoas odiadas pelo público, com o intuito de denegrir a imagem do candidato. Inúmeros são os casos, já foi visto Bill Clinton cumprimentando Saddam Hussein [3], Sarah Palin segurando um fuzil em frente à uma piscina [2], George W Bush e Luís Inácio Lula da Silva lendo livros de cabeça para baixo, entre outros.

Neste documento será estudado um método para conseguir separar imagens suspeitas de fraudes, de imagens autênticas e, no caso da imagem suspeita, apontar as regiões da imagem que provavelmente foram adulteradas. O método, originalmente proposto por Popescu [1], identifica imagens alteradas através de uma técnica conhecida como *resampling*, na qual uma imagem ou um pedaço de imagem é rotacionado, redimensionado ou realocado de posição. Utilizando essa técnica, é possível remover ou multiplicar objetos de uma foto.

2. Estado da Arte

Recentemente, muito esforço vem sendo colocado para resolver o problema de identificação de imagens digitais fraudulentas. Cada método foca em diferentes características que podem ser avaliadas para se tentar verificar a autenticidade de uma imagem. Algumas técnicas, tentam separar imagens naturais de imagens geradas por computador, uma delas propõe fazer isso analisando características físicas da imagem, que se mostrou melhor do que analisar se a imagem possui características de desenhos. [5]

O método proposto por Fridrich et al. [3] detecta imagens alteradas por cópia e colagem, e revela onde estão as regiões copiadas. A técnica simples, porém robusta, consiste em ir comparando blocos de pixels da imagem de dois modos diferentes, no primeiro, comparando se os blocos são exatamente iguais, no segundo utilizando a transformada discreta do cosseno para fazer comparações aproximadas, e assim, tolerar possíveis ruídos ou alterações na imagem. Apesar da precisão, o custo da técnica aumenta muito para imagens com grande grande quantidade de pixels.

Lint et al. [6] propõe uma técnica que compara blocos de pixels em bordas na imagem, tentando identificar uma função resposta da câmera e verificando se os resultados das comparações batem. A função resposta de uma câmera consiste em uma função matemática que faz uma aproximação de cores em bordas com contrastes (por exemplo, na borda da imagem entre uma árvore e um céu de fundo), tal aproximação é necessária devido à limitação da resolução de uma câmera digital. Comparando-se as funções usadas para gerar as cores nas bordas, ao se encontrar alguma região que parece usar uma função muito diferente pode-se suspeitar de uma montagem. Essa técnica não é muito eficiente em imagens nas quais as bordas não tenham alto contraste.

Para o caso em que o problema é saber se uma determinada imagem veio de uma determinada câmera e não sofreu nenhum tipo de operação, Swaminathan et al. [7] propõe uma solução que avalia uma foto que com certeza foi obtida pela câmera e dessa foto extrai informações de processamento de imagem, única daquela câmera, a digital (*fingerprint*) da câmera e repete o processo na imagem dada. Caso as digitais não estejam batendo, suspeita-se de uma fraude.

Popescu [1], em sua tese de doutorado, propõe diversos métodos estatísticos para se identificar se uma imagem é verdadeira. Dentre eles está o método para identificar manipulações por *resampling* no qual este trabalho se baseia. Dentre as outras técnicas abordadas pelo autor, está a detecção de dupla compressão JPEG, que pode identificar se houve uma colagem de duas ou mais imagens JPEGs dife-

rentes, a detecção de regiões duplicadas da imagem (cópia-colagem) e a verificação da interpolação de cores da imagem. Quanto á última, a maioria das câmeras digitais não capturam todos os três canais de cores ao mesmo tempo (vermelho, verde e azul), mas apenas uma cor para cada pixel e depois, através de interpolação dos valores, as cores finais são calculadas. O método proposto consiste em tentar estimar como as cores foram interpoladas e tentar achar aberrações na imagem, isto é, regiões que apresentam outro comportamento de interpolação, que pode significar uma montagem.

3. Solução Proposta

Falar sobre a solução proposta...

4. Experimentos e Discussão

Resultados

5. Conclusões e Trabalho Futuro

Os finalmentes

Referências

[1] Alin C. Popescu. *Statistical Tools for Digital Image Forensics*. PhD thesis, DARTMOUTH COLLEGE, 2004. 1, 2

[2] Siome Goldenstein Anderson Rocha. *Atualizações em Informática (JAI)*, chapter CSI: Análise Forense de Documentos Digitais, pages 263–317. Sociedade Brasileira de Computação (SBC), 2010. 1, 2

[3] A Jessica Fridrich, B David Soukal, and A Jan Lukáš. Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*, 2003. 1, 2

[4] T. Boult A. Rocha, W. Scheirer and S. Goldenstein. Vision of the unseen: Current trends and challenges in digital image and video forensics. *ACM Computing surveys*, 2011. to appear. 2

[5] Tian-Tsong Ng, Shih-Fu Chang, Jessie Hsu, Lexing Xie, and Mao-Pei Tsui. Physics-motivated features for distinguishing photographic images and computer graphics. In *Proceedings of the 13th annual ACM international conference on Multimedia*, MULTIMEDIA '05, pages 239–248, New York, NY, USA, 2005. ACM. 2

[6] Zhouchen Lint, Rongrong Wang, Xiaoou Tang, and Heung-Yeung Shum. Detecting doctored images using camera response normality and consistency. *Computer Vision and Pattern Recognition, IEEE Computer Society Conference on*, 1:1087–1092, 2005. 2

[7] A. Swaminathan, M. Wu, and K.J.R. Liu. Digital image forensics via intrinsic fingerprints. *Information Forensics and Security, IEEE Transactions on*, 3(1):101–117, 2008. 2