ANÁLISE E INVESTIGAÇÃO FORENSE EM FOTOGRAFIAS DIGITAIS
Relato de pesquisa: andamento

Tiago Torresani[1];Ana Elisa Schimdt[2];

RESUMO

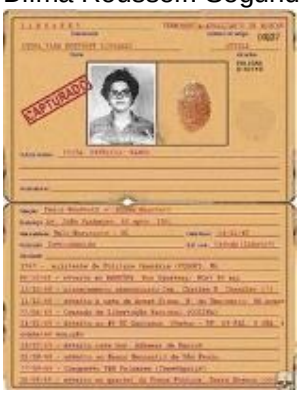
Este artigo apresenta o estado de andamento do projeto de pesquisa que tem como objetivo estudar técnicas de ProcessamentoDigital de Imagem e de Computação Forense que possam auxiliar a desvendar se uma determinada imagem digital foi alterada, e em caso de alteração o que foi alterado exatamente. Para isto, está sendo feita a pesquisa de bibliotecas de processamento de imagem, verificando suas funcionalidades e buscando dentre estas as que permitam implementar tais análises forense. Busca-se chegar ao final do projeto permitindo a identificação de alterações na imagem de fotografias digitais, podendo dizer se uma fotografia foi modificada digitalmente.

Palavras-chave:Computação forense.Processamento digital de imagem. Adulteração fotografia digitai.

INTRODUÇÃO

É fato que a adulteração de fotografias não é datada de hoje, visto que Hitler, Mussolini e tantos outros nomes históricos já tiveram suas fotografias manipuladas [Rocha et al. 2011].A cada dia tem ficado mais rápido e fácil a manipulação digital de uma imagem. Softwares como Photoshop(Adobe Inc, 2015) e GIMP(GIMP Team, 2015) acabam facilitando a manipulação de maneira muito ágil, permitindo alteração de suas características, muitas vezes de formas imperceptíveis a olho nu, ou seja, sendo necessário aajuda de softwares específicos de análise de imagens para descobrir tal alteração, conforme mostra a Figura 1.

Figura 1 – Ficha criminal de Dilma Rousseff: Segundo pesquisas, a ficha é falsa.



Fonte: CSI: Análise Forense de Documentos Digitais (GOLDENSTEIN et al. 2010)

Visto o poder de influência que uma foto pode causar [Sacchi et al. 2007], é necessário um esforço cada vez maior da comunidade forense para descobrir métodos que possam detectar ameaças de falsificação e manipulação de fotografias digitais. Focado em ajudar tanto a comunidade acadêmicacomo também a comunidade forense, este projeto tem como objetivoestudar técnicas de Processamento Digital de Imagem (PDI)(Solomon et al. 2011), bem como

1EstudantedeGraduaçãoemSistemaspara Internet,InstitutoFederalCatarinense – Campus Camboriú.E-mail:ttorresane@gmail.com.
2Doutoraem Informática, PUC-Rio;Professorado Instituto Federal Catarinense – Campus Camboriú.E-mail:anaelisa@ifc-camboriu.edu.br

bibliotecasde processamento, que possam auxiliar na detecção de adulterações em fotografias digitais.Ao final deste projeto, pretende-se propor um sistema computacional que possadetectar se uma imagem foi modificada digitalmente, seja ela somente melhorada (brilho, nitidez, saturação), ou modificada totalmente (cópia-cola de elementos, técnicas de iluminação, e outras).

O escopodeste projetorestringe-se a descoberta e utilização de bibliotecas de PDIjá existentes que sejam capazes de interagir com técnicas de Computação Forense(Farmer et al. 2004), auxiliando assimna elaboração de métodos para detectar alterações em fotografias digitais. Busca-se também elaborar uma proposta de software de análise de imagens que utilize as técnicas estudadas durante o projeto.

PROCEDIMENTOSMETODOLÓGICOS

Para alcançar os objetivos do projeto e facilitar seu gerenciamento, foram identificadas fases que englobam as ações necessárias para obterem-se os resultados almejados. A descrição de cada fase e respectivas ações, em conformidade com os objetivos, é apresentada a seguir:

1. Estudos e levantamento bibliográfico sobre características forenses de imagens digitais e técnicas de PDI relevantes a análise forense;
2. Levantamento e análise de softwares existentes na área de análise forense de imagens fotográficas digitais;
3. Levantamento, estudo e teste de bibliotecas de processamento de imagem;
4. Proposta de um protótipo para análise forense de fotografias digitais;
5. Validação da proposta do protótipo;
6. Elaboração de relatórios e documentos de divulgação da pesquisa.

ESTADO ATUAL DA PESQUISA

Cabe ressaltar que este projeto iniciou-se em Março/2015, tendo duração prevista para 01 ano, e portanto encontra-se nas suas fases iniciais de andamento. Dentre as etapas de desenvolvimento do projeto, elencadas na seção anterior, as seguintes atividades já foram cumpridas ou estão atualmente em andamento:

1. Estudos e levantamento bibliográfico sobre características forenses de imagens digitais e técnicas de PDI relevantes a análise forense;
2. Levantamento e análise de softwares existentes na área de análise forense de imagens fotográficas digitais;
3. Levantamento, estudo e teste de bibliotecas de processamento de imagem.

As etapas 1 e 2 encontram-se com 90% das suas atividades de estudo e análise concluídos. Já a etapa 3 está sendo atualmente desenvolvida, com 30% das suas atividades já concluídas.

As informações levantadas e analisadas nestas etapas iniciais são detalhadas nas próximas seções.

FUNDAMENTAÇÃO TEÓRICA

A área de Computação Forense(Farmer et al. 2004)é relativamente nova dentre as áreas da computação eintersecciona-se, em muitos momentos, com a área de PDI.Novos desafios surgem na busca de técnicas de PDI que possam contribuirpara desvendar fotografias e arquivos alterados digitalmente com a intenção de alterar provas forenses, “incluir” e “excluir” pessoas de imagens ou até mesmo esconder fatos.

São várias as técnicas de falsificação existentes, porém entre elas algumas se destacam, como por exemplo as técnicas de *splicing* e de *cloning*(Goldenstein et al. 2010). A primeira tem por objetivo utilizar pedaços de duas ou mais imagens para compor uma única, incluindo assim pessoas em fotografias ou até mesmo alterando a sua composição, conforme mostra Figura 2. Já a técnica de *cloning*, é basicamente a cópia e cola de partes de uma única fotografia, com o objetivo de esconder objetos, pessoas, ou características presentes na imagem.

Figura 2 – Técnica de *splicing* para criar composição de Marilyn Monroe e Abraham Lincoln

Fonte: Detecting Photographic Composites of People (FARID, 2008)

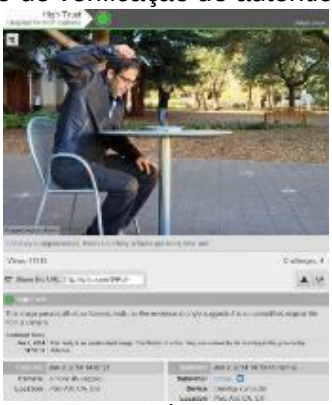
SOLUÇÕES EXISTENTES

Buscando uma solução para os problemas encontrados quanto a necessidade de detecção de adulterações em fotografias digitais, foram encontrados os seguintes softwares especializados em técnicas forenses:

Izitru [http://www.izitru.com]: No Izitru o usuário efetua o *upload* de uma imagem tendo ela sido editada ou não e após algumas análises automatizadas feitas por uma API hospedada em nuvem, o aplicativo retorna ao usuário o resultado informando se a imagem é legítima, se foi alterada, ou se o site não conseguiu

chegar a um parecer. A Figura 3 mostra um exemplo de verificação utilizando o Izitru.

Figura 3 – Exemplo de verificação de autenticidade do site Izitru



Fonte: Izitru.com

FIAS [http://www.forensicav.ro/software.htm]:O Forensic Image Analysis System é uma ferramenta de análise forense para imagens que efetua análises buscando saber a origem da imagem, bem como se a mesma foi alterada. Segundo o autor, Catalin Grigoras Ph. D., a ferramentautiliza técnicas de computação forense a fim de verificar a autenticidade de imagens, dentre elas, verificações de dados e informações contidos no arquivo, com o propósito de conseguir informações de onde e com qual equipamento aquela imagem foi feita. Um exemplo de detecção de alteração por *cloning* através do FIAS é mostrado na Figura 4.

Figura 4 - Exemplo de funcionamento da técnica Clone Detection do FIAS.

Fonte: http://www.forensicav.ro/

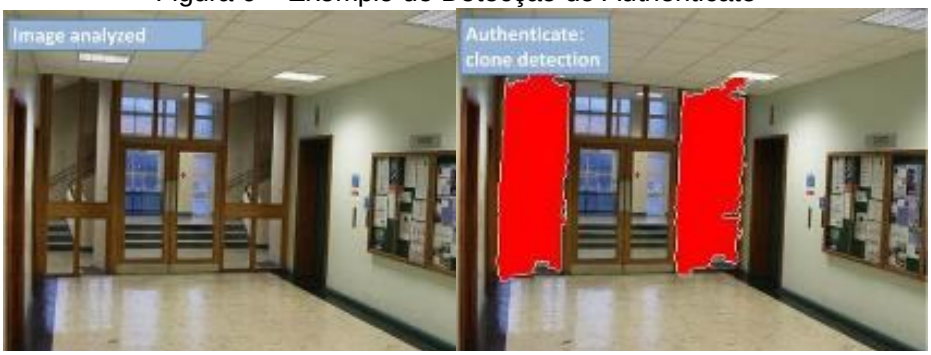
Verifeyed [http://verifeyed.com/]:desenvolvido pela*startup* de mesmo nome,é capaz de detectar a veracidade de imagens e também arquivos PDF, além de dizer exatamente qual a alteração realizada na foto. Não conseguiu-se contato com a empresa para verificar a existência de uma versão de testes até o momento. A Figura 5 mostra um exemplo de detecção de adulteração utilizando o Verifeyed.

Figura 5 – Exemplo de verificação do Verifeyed

Fonte: Verifeyed.com

Authenticate [http://ampedsoftware.com/authenticate]: foi desenvolvido por uma empresa italiana, a Amped Software, e é especializado em detectar falsificações em imagens, identificando se a imagem foi alterada, e o que exatamente. Para verificar a autenticidade sãos realizados múltiplos testes de uma única vez, e além disso, o mesmo possui integração com diversas ferramentas entre elas Google Maps e MS Excel. Um exemplo do uso do Authenticate é mostrado na Figura 6.

Figura 6 – Exemplo de Detecção do Authenticate



Fonte: http://ampedsoftware.com/authenticate

TÉCNICAS DE DETECÇÃO DE ADULTERAÇÃO

Até o presente momento, foram encontradas diversas técnicas de PDI que podem auxiliar na identificação de adulterações; dentre elas duas se destacam: oMétodo de Fridrich [Fridrich et al. 2003],é capaz de encontrar partes de uma imagem que foram duplicadas (*cloning*);enquanto o Método de Johnson e Farid(Farid et al. 2007)é capaz de detectar erros na iluminação de uma imagem, descobrindo assim se foi utilizada alguma técnica de *slicing* na mesma. Estamos estudando estasduas técnicas para que possamos implementá-las em nosso protótipo a ser desenvolvido na linguagem de programação Python (Python Software Foundation, 2015)e utilizando aas funcionalidades disponíveis na biblioteca gráfica OpenCV (Marengoni e Stringhini, 2009).

CONSIDERAÇÕESFINAIS

Por se tratar de um projeto pesquisa na área de computação forense, área relativamente nova, ainda existem poucasbibliografias disponíveis para pesquisa física, sendo necessário efetuar grande parte do levantamento bibliográfico através de materiais digitais, como artigos e teses, onde a complexidade apresentada é bem maior do que em livros e tutoriais.Sendo assim, cabe ressaltar que grande parte das bibliografias pesquisadasapresentamconteúdos acadêmicos muito avançados e complexos, como por exemplo as funções matemáticas utilizadas em filtros de imagens, conhecimento do qual deveremos nos apropriar para dar continuidade ao projeto.

Além do comentado acima, mesmo utilizando-se das funcionalidades já existentes nabiblioteca OpenCV, será necessário desenvolvimento de código nativo para implementar corretamente as técnicas de detecção de adulterações escolhidas.

REFERÊNCIAS

ADOBE INC. **Adobe Photoshop CC.** 2015. Disponível em: http://www.adobe.com/br/products/photoshop.html. Acessado em: 22 jun. 2015.

FARID, Hany; KIMO, Micah J. **Detecting Photographic Composites of People**. 2008. Disponível em: http://www.mit.edu/~kimo/publications/composite/iwdw07.pdf. Acessado em: 26 jun. 2015.

FARID, Hany; KIMO, Micah J. **Exposing Digital Forgeries Through Specular Highlights on the Eye.** 2007. Disponível em: http://www.mit.edu/~kimo/publications/specularity/ih07.pdf. Acessado em: 22. jun. 2015.

FARMER, Dan; VENEMA, Wietse. **Forensic Discovery.** Upper Saddle River, New Jersey, USA: Pearson Education, 2004. p. 193.

FORENSICAV. **Advanced Media Forensics Solutions.** 2015. Disponível em: http://www.forensicav.ro/. Acessado em: 22. jun. 2015.

FRIDRICH, Jessica; SOUKAL, David; LUKÁS, Jan. **Detection of Copy-Move Forgery in Digital Images.** 2003. Disponível em: http://www.ws.binghamton.edu/fridrich/research/copymove.pdf. Acessado em: 29 jun. 2015.

FOURANDSIX TECHNOLOGIES INC.**IZITRU**. 2015. Disponível em: http://www.izitru.com/. Acessado em: 22 jun. 2015.

GIMP TEAM. **GIMP – Feature Overview.** 2015. Disponível em: http://www.gimp.org/features/. Acessado em: 22 jun. 2015.

GOLDENSTEIN, Siome; ROCHA, Anderson. CSI: Análise Forense de Documentos Digitais. In: MEIRA, Wagner; CARVALHO, André. **Atualizações em Informática 2010.** Rio de Janeiro: Editora Puc-Rio, 2010. p.263-317.

MARENGONI, Maurício; STRINGHINI, Denise. **Tutorial: Introdução à visão computacional usando OpenCV.** 2009. Disponível em: http://seer.ufrgs.br/rita/article/viewFile/rita_v16_n1_p125/7289. Acessado em: 21 maio 2015

PYTHON SOFTWARE FOUNDATION. **The Python Tutorial.** 2015. Disponível em: https://docs.python.org/3/tutorial/index.html. Acessado em: 29 jun. 2015.

ROCHA, Anderson; SCHEIRER, Walter; BOULT, Terrance; GOLDENSTEIN, Siome. (2011). **Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics**. 2010. ACM Computer Survey, 43(4):1–42.

SACCHI, Dario L. M.; AGNOLI, Franca; LOFTUS, Elizabeth F. **Changing History: Doctored Photographs Affect Memory for Past Public Events.** 2007.Applied Cognitive Psychology, 21(8):1005–1022.

SOLOMON, Chris; BRECKON, Toby. **Fundamentals of Digital Image Processing: A Practical Approach with Examples in Matlab.** Chichester, UK: Wiley-Blackwell. 2011. p. 344.

VERIFEYED. **Verifeyed - Image, video and PDF Forensics, authentication, manipulation Detection and digital security.**2015. Disponível em: http://verifeyed.com/. Acessado em: 22 jun. 2015.