

Análise forense de imagens digitais no estudo de caso da ficha criminal de Dilma Rousseff

Wesley Silva dos Reis – wlyreis@gmail.com
Computação Forense e Perícia Digital
Instituto de Pós-Graduação - IPOG
Brasília, DF, 21 de Maio de 2018

Resumo

O presente artigo estuda o uso de técnicas de processamento de imagens aplicadas a perícia forense, com o objetivo de identificar possíveis edições de imagens digitais. Em 05.04.2009, o Jornal Folha de São Paulo divulgou matéria com a imagem de uma suposta ficha criminal da então presidente Dilma Rousseff. O caso, de elevada repercussão nacional, acabou provando-se um episódio contrangedor para o grupo jornalístico que dias depois publicou matéria com retratações aos seus leitores. Este artigo tem por objetivo elucidar, por meio de técnicas de processamento de imagens e perícia forense, a questão sobre a legitimidade da imagem publicada. Utilizando de amostra do arquivo digital disponibilizada na Internet, o estudo terá foco nos seguintes procedimentos de análise da imagem: exame de coerência perceptiva, detecção de clonagens e análise de histograma nos 3 canais de cor R, G e B. Com os resultados obtidos é possível informar categoricamente sinais de falsificação da imagem apresentada. Conclui-se que com a abordagem adequada é possível determinar a ilegitimidade de uma imagem digital identificando sinais de adulteração, ocultação e inclusão de informações indevidas.

Palavras-chave: Perícia. Processamento de imagem. Imagem digital.

1. Introdução

Com o advento da modernização vivenciada nos últimos anos, surgiram no ramo da ciência forense diversas técnicas e ferramentas que revelaram as respostas para questões ora impossíveis de serem respondidas. Porém, esta verdadeira revolução tecnológica também trouxe desafios para a arte forense, principalmente no que tange a análise de imagens digitais.

Contratos, fotos e fichas cadastrais: o universo de documentos com versões digitalizadas é uma realidade cada vez maior nos ambientes corporativos, governamentais e organizacionais. Apesar da solução no dilema de armazenamento de tanta informação, as premissas de segurança continuam necessárias: confidencialidade, disponibilidade e principalmente a autenticidade.

Para Arruda (2016:208) “Com a atual facilidade de acesso a aplicativos especializados em edição de imagens, alguns dos quais disponibilizados de forma gratuita, é cada vez mais comum a existência de imagens adulteradas digitalmente”. A afirmativa do autor pode ser

Dezembro/2018

facilmente confirmada pela verdadeira onda de montagens, notícias e imagens falsas hoje vinculadas na internet, principalmente em períodos eleitorais e em vários lugares do mundo.

O escopo de trabalho deste artigo é a análise forense de amostra da imagem publicada, no ano 2009, de suposta ficha criminal da então presidente Dilma Rousseff no jornal Folha de São Paulo. Não há dúvidas quanto aos prejuízos financeiros e institucionais que uma imagem digital falsa pode causar. O valor de negócio de um jornal está ligado diretamente com a assertividade e veracidade das informações publicadas. O próprio objeto de estudo de este artigo gerou prejuízos incalculáveis ao veículo de comunicação envolvido, pois sua credibilidade foi diretamente afetada. Neste sentido, uma abordagem de análise de imagens digitais fundamentada em princípios técnicos poderia mitigar, ou até coibir, a exposição desnecessária ocorrida no caso, evitando os prejuízos de imagem institucional.

A fundamentação técnica é pilar indispensável para condução dos objetivos deste estudo. Franco et al. (2016:2) descreve a computação forense como “a ramificação da Criminalística, com objetivo de identificar os vestígios cibernéticos” nas práticas de ilícitos no meio digital. O autor assertivamente limita o escopo de trabalho da computação forense a todo vestígio ligado ao universo digital e a perícia em imagens digitais está inserida neste contexto. Em contrapartida, não há dúvidas quanto a vasta área de conhecimento empregada no estudo da perícia em imagens digitais:

Para compreensão das técnicas empregadas nos exames periciais em imagens, é necessário conhecer o processo de formação das imagens digitais, seu armazenamento em dispositivos computacionais e o formalismo matemático que envolve as diversas áreas correlatas. Desse modo, o estudo voltado a análise forense de imagens digitais é interdisciplinar, envolvendo desde conceitos de neurofisiologia e psicologia cognitiva, passando por matemática, física, computação, estatística e eletrônica (ARRUDA, 2016:208).

Com base nesses conceitos do autor é possível compreender que mesmo com a limitação de escopo ao universo cibernético existam variadas técnicas para abordagem em uma análise pericial, todas dependendo da natureza dos vestígios a serem observados. A verdadeira gama de tecnologias disponíveis permite que uma mesma evidência possa ter mais de uma abordagem de análise de diversos níveis de eficácia e áreas de conhecimento. Este artigo propõe uma observação direcionada com a prática do estudo forense, proporcionando uma experiência objetiva e restrita a um caso real de adulteração em imagem digital.

Goldestein e Rocha (2009) realizaram um trabalho comprovando as irregularidades da imagem objeto a ser analisada. O laudo técnico possui abordagem direta nas análises de cópia e colagem, procedência e manipulação tipográfica. Contudo, utilizaremos neste estudo de caso três abordagens distintas: exame de coerência perceptiva, análise de histograma e detecção de clonagens. Apesar da abordagem distinta, o estudo realizado pelos autores servirá de alicerce conceitual para a análise proposta neste artigo de forma a simplificar alguns procedimentos e dar objetividade ao trabalho.

Sendo assim, o presente artigo tem por objetivo evidenciar outras possíveis adulterações com auxílio da literatura da arte pericial em imagens digitais, com uso de abordagens distintas de outros estudos já realizados. Permitindo comprovar a ilegitimidade da prova já apresentada por outros profissionais.

2. Fundamentação Teórica

2.1 Perícia em Imagens Digitais

Arruda (2016:208) ressalta a definição de Perícias em Imagens Digitais como a atividade que geralmente é associada à detecção de montagens e fraudes em fotografias. Em outra definição, Freitas (2006:1) detalha a Perícia Forense Computacional como o uso conjunto de técnicas forenses e conhecimento de TI para obtenção de evidências em análises investigativas. O ponto de convergência entre os autores é o uso de técnicas computacionais para análise de vestígios criminais, guardadas as devidas diferenças de escopo da análise. Portanto, a tecnologia é ponto chave na perícia forense moderna e torna casos como a ficha criminal de Dilma Rousseff cada vez mais comuns.

Fica evidente a necessidade de recursos e técnicas para a análise pericial de uma imagem digital, bem como a correta seleção de quais ferramentas a utilizar. A definição de escopo no exame pode ser um fator chave para o sucesso de uma perícia. Para o estudo de caso proposto definimos como escopo de trabalho o exame de coerência perceptiva, a técnica de detecção de clonagens e a análise de histograma.

2.2 Observação direta

A observação direta é a análise mais elementar quando se procura identificar elementos alterados em uma imagem digital. Conforme Arruda (2016:222) essa técnica é básica e subjetiva, que deve ser utilizada com parcimônia e objetivando identificar elementos da imagem que estejam fora de contexto para posterior análise com técnicas apropriadas. Na literatura nacional o autor é singular em abordar esta análise, que apesar da subjetividade mostra-se um excelente ponto de partida para a perícia em imagens digitais, mas limitada do ponto de vista técnico para se comprovar uma adulteração.

Neste ponto deve-se identificar indícios que sirvam de vetores iniciais para aplicações de técnicas avançadas que possam comprovar a suposta alteração: bordas distorcidas, cores, profundidade e elementos estranhos à imagem em seu contexto geral. Esta abordagem é um alicerce para definição do escopo de trabalho.

2.3 Análise de Coerência Perceptiva

A análise de coerência perceptiva está ligada ao exame sensorial perceptivo da imagem: efeitos de sombra e luz, continuidade lógica, dimensões e inconsistências físicas.

A análise de coerência perceptiva transborda a subjetividade da observação direta enquanto se propõe a evidenciar, por meio de técnicas específicas, as distorções apresentadas como fruto de adulterações proposital na imagem digital periciada. Para isso, a análise de coerência perceptiva faz uso de ciências como a Fotogrametria:

O termo fotogrametria é usado para definir técnicas que permitem obter informações sobre dimensões de objetos ou pessoas em uma imagem bidimensional, eventualmente por meio da aplicação de princípios de perspectiva cônica[...] No

ambiente pericial, a fotogrametria está fortemente presente na estimação de altura de suspeitos e determinação de velocidade de veículos. (ARRUDA, 2016:236-237).

Já Tommaselli (2018:1) determina a Fotogrametria de acordo com sua origem etimológica, trazendo um contexto filosófico em traduzir o termo como “medir graficamente usando a luz”. O ponto de interesse nos dois conceitos é o objetivo principal da abordagem que é obter medidas reais de objetos em uma imagem.

Para se obter informações sobre dimensões de objetos como descrito acima pelo autor é necessária a informação de uma dimensão conhecida na imagem digital analisada que, no caso de estudo, utilizaremos o tamanho padrão da ficha criminal do DEOPS (Departamento de Ordem e Política Social) identificada por Goldestein e Rocha (2009:3) em seu laudo técnico.

2.4 Análise de Histograma nos Canais de Cor RGB

Para compreender melhor o conceito de histograma e canais de cor devemos primeiro realizar uma breve revisão do processo de formação de imagens digitais. Há uma convergência na literatura do tema que define o termo imagem como uma representação ou reprodução de uma determinada cena. Partindo do princípio comum de que o processo de digitalização é a conversão de informações analógicas para o formato digital, podemos concluir que o processo de formação de imagens digitais baseia-se na interpretação de uma determinada cena (informação analógica) e sua posterior conversão/representação em um formato digital pré-definido (dados binários).

Este processo de conversão da informação analógica para digital é realizada por meio de sensores, que por sua vez, são compostos de células sensíveis a luz dispostas em um arranjo definido. Scanners de mesa normalmente utilizam sensores em arranjo de linha, enquanto câmeras digitais utilizam-se de uma disposição dos sensores em uma matriz. “Cada elemento dessa matriz constitui um *pixel*, ou elemento de imagem, e a união desses pontos é o que forma uma imagem digital.” (ARRUDA 2016:210). O autor nesta abordagem é uníssono com outros conceitos de mesmo tema na literatura nacional.

A informação de cor é interpretada pela mente ao captar determinado comprimento de onda de luz no espectro visível ao olho humano. Dado principalmente ao custo financeiro, geralmente as empresas utilizam o recurso de filtros em forma de mosaico, fazendo com que cada sensor receba a informação de apenas uma única cor (vermelho, verde ou azul). Aos sensores, cabe o papel de determinar a intensidade luminosa do sinal não bloqueado pelo filtro. É aqui que entra o conceito de análise de histograma nos canais de cor RGB: uma análise da disposição e intensidade de cada canal de cor em uma determinada imagem.

Uma vez que o histograma é uma distribuição de determinados valores dentro de uma classificação previamente estabelecida, podemos inferir que um histograma dos canais de cor RGB é uma disposição, onde cada uma das cores será representada dada sua intensidade/distribuição de acordo com uma classificação prévia. No caso de imagens digitais é comum a utilização da escala de 0 a 255 (8 bits) para a representação da luminosidade de um determinado pixel, onde zero seria uma intensidade de brilho nulo e 255 a intensidade máxima. Podemos representar a quantidade de vezes em que os pixels de uma imagem, em

um exemplo prático, obtiveram intensidade de valor 255 para a cor vermelha em seu histograma de cor.

Perceba que todas as demais cores observáveis são uma junção de diversas proporções dos canais de cor RGB, de forma que um valor idêntico de intensidade nos três canais de cor: vermelho, verde e azul em um determinado pixel, formaria uma imagem em tons de cinza ou de saturação nula, algo inimaginável em uma representação de uma suposta imagem real capturada digitalmente.

2.5 Detecção de Clonagens

Antes de definirmos o que seria a detecção de clonagens em imagens digitais é necessário compreendermos o conceito de composição, em que Goldestein e Rocha (2010:09) descrevem como a utilização de partes de uma ou mais imagens para editar/compor uma outra imagem final adulterada. Pode-se, por exemplo, inserir a imagem de um carro em uma segunda imagem de uma estrada qualquer. Uma terceira imagem resultado é gerada da estrada com o carro supostamente presente na pista no ato da digitalização da cena.

A clonagem em imagens digitais seria conceitualmente uma ramificação da técnica de manipulação por colagem de uma imagem digital, mas utilizando-se de “pedaços” da própria imagem para ocultar ou modificar alguma informação da imagem original. A vantagem de tal alteração quando utilizada para omitir algum pedaço da imagem é a sua maior dificuldade na percepção em uma análise inicial por observação direta.

A Transformada de Fourier, de Jean Baptiste Joseph Fourier, expressa todo sinal como a soma de frequências em uma função temporal. Freitas et al (2009:6884) determina que este conceito somado as teorias de convolução e correlação foram alicerces para os filtros de eliminação de ruídos e interferências (sinais) em imagens digitais. De forma objetiva o autor descreve o atual estado da arte onde diversos *softwares*, ou programas de computador, realizam de forma automática as operações matemáticas necessárias para os ajustes propostos.

A deconvolução, por exemplo, é normalmente utilizada para remover distorções de imagens com uso de operações aritméticas entre a imagem a ser processada e um valor conhecido da função de espalhamento de pontos ou PSF – *Point Spread Function*. O PSF funciona como um modelo, para que através de operações inversas possamos remover ou atenuar a distorção da imagem processada. Este processo também pode ser utilizado para detecção de clonagens em imagens digitais.

Técnicas baseadas em correlação de fase estimam os deslocamentos espaciais analisando picos em $v(x, y)$, a inversa da transformada de Fourier $\psi(Wx, Wy)$. Um pico é esperado na origem [...] Quaisquer picos em outras posições são pistas para alinhamentos secundários que podem representar uma região duplicada. (GOLDESTEIN e ROCHA, 2010:295).

Apesar dos autores se referirem a uma técnica distinta de detecção de clonagens podemos utilizar o mesmo conceito. Se utilizarmos um trecho suspeito de duplicação na imagem como valor de função de espalhamento e aplicarmos um filtro de deconvolução, teoricamente existirá mais de um pico de sinal observável na evidência digital resultado do

processamento, bem como uma degradação evidente no restante da imagem.

2.6 Cadeia de Custódia

Em um processo de perícia forense a evidência digital é um artefato digital com informação de valor, capaz de validar ou não uma hipótese dada uma linha de investigação. O processo de transição deste artefato desde sua aquisição até a análise pericial em um ambiente controlado é chamado de cadeia de custódia.

No estudo de caso proposto a cadeia de custódia é totalmente prejudicada: conforme informações do próprio jornal a suposta imagem foi recebida por e-mail do editorial, não se podendo afirmar quais possíveis alterações foram realizadas na imagem no processo de sua aquisição na biblioteca nacional até sua publicação. Não obstante, em carta de resposta da então ministra e presidente Dilma Rousseff, a foto objeto de fraude teria sua origem em um portal da internet: www.ternuma.com.br “Terrorismo nunca mais” em Novembro de 2008. Fica evidente que o trabalho de aquisição do exato artefato digital publicado é definitivamente impossível de ser realizado de acordo com a literatura forense ortodoxa.

Há, portanto, duas abordagens possíveis para o caso. A utilização de uma amostra disponibilizada na internet: metodologia de Goldestein e Rocha (2009) em seu laudo, de forma a se aproximar o máximo possível da imagem original por meio de critérios técnicos definidos. Ou a sua coleta direta da página da matéria publicada pelo grupo Folha de São Paulo. A segunda hipótese é descartável devido a qualidade da imagem disponibilizada na página da notícia uma vez que o grupo utiliza de amostra de dimensões incompatíveis, que certamente divergem da publicada originalmente no periódico.

3. Estudo de Caso

3.1 Evidência Digital

Utilizando a abordagem de coleta aproximada, utilizamos ferramentas de pesquisa na internet de forma a localizar a imagem que mais se assemelha a aquela publicada pela Folha em 05 de abril de 2009. Com base na medida padrão das fichas de papel utilizadas pelo Departamento de Ordem Política e Social DEOPS é possível calcular as supostas características da imagem resultante do suposto processamento digital de captura.

O Arquivo Público de São Paulo abriga, desde 1991, a documentação do Departamento de Ordem Política e Social (DEOPS). Todos os dados policiais estão organizados em fichas de papel cartão com dimensões uniformes de 6 x 4 polegadas. [...]com estas dimensões padronizadas capturadas a uma taxa de 96 pontos por polegada (DPI), teriam 576 pixels de largura[...] (GOLDESTEIN e ROCHA, 2009:3).

Com base nos estudos levantados por Goldestein e Rocha (2009) em seu laudo, selecionamos a imagem abaixo como a mais adequada para a análise proposta.

ESPECIALIZE

Análise forense de imagens digitais no estudo de caso da ficha criminal de Dilma Rousseff

Dezembro/2018

LINHARES **TERRORISTA/ASSALTANTE DE BANCOS**
Sobrenome Número do artigo **00297**
DILMA VANA ROUSSEFF LINHARES **ESTELA**
Nome Alcunha
POLEGAR DIREITO
CAPTURADO
Outros nomes: **LUIZA; PATRICIA; WANDA**
Assinaturas: _____
Filiação: **Pedro Rousseff e Dilma Rousseff**
Endereço: **Av. João Pinheiro, 85 apto. 1001**
Naturalidade: **Belo Horizonte - MG** Data Nasc: **14/12/47**
Profissão: **Desconhecida** Est. civil: **Casada (Lobato?)**
Atividade:
1967 - militante da Política Operária (POLOP), MG
06/10/68 - assalto ao BANESPA, Rua Iguatemi: NCr\$ 80 mil.
12/10/68 - planejamento assassinato Cap. Charles R. Chandler (?)
11/12/68 - assalto à casa de Armas Diana, R. do Seminário: 48 armas
??/04/69 - Comando de Libertação Nacional (COLINA)
24/01/69 - Assalto ao 4º RI Quitaúna, Osasco - SP: 63 FAL; 3 INA; 4
cunhetes munição
18/07/69 - Assalto casa Gov. Adhemar de Barros.
01/08/68 - assalto ao Banco Mercantil de São Paulo
??/09/69 - Congresso VAR Palmares (Teresópolis)
20/09/69 - assalto ao quartel da Força Pública, Barro Branco (cont..)

Figura 1 – Ficha de Dilma
Fonte: MDIG – Metamorfose Digital

Nome	ficha_dilma.jpg
Fonte	http://www.mdig.com.br/imagens/curiosidade/ficha_dilma.jpg
Hash MD5	E1D47C7CD0CE72C8B0B5E8D73E10E134
Tamanho	596 x 784 pixels
Resolução	96 x 96 pontos por polegada (DPI)

Tabela 1 – Dados diversos do arquivo digital ficha_dilma.jpg

Fonte: Elaborada pelo autor

Haveria a possibilidade de realizar a análise comparativa realizada pelos autores, mas o objetivo deste artigo não é replicar outros experimentos realizados, e sim, de forma objetiva e alternativa localizar novas evidências de fraude na evidência digital.

3.2 Ferramenta de análise

Para a análise da evidência digital colhida é necessário um ambiente controlado e uma ferramenta adequada para estudo, testes e avaliações necessárias dos indícios forenses a serem observados. Dado ao objetivo acadêmico deste estudo utilizaremos o software ImageJ.

Programa de código aberto o ImageJ foi desenvolvido por Wayne Rasband em 1987 em um projeto idealizado pelos Institutos Nacionais da Saúde dos Estados Unidos da América, onde o programa passou a ser utilizado para análises científicas diversas principalmente no campo da microscopia.

A grande vantagem da ferramenta digital é sua escalabilidade, com o uso de plug-ins que permitem agregar novos algoritmos matemáticos, e assim, estendendo a capacidade e variedade de técnicas de análise de uma imagem.

3.3 Observação direta e o levantamento de hipóteses

Conforme já explicitado, o estudo de caso proposto já foi objeto de avaliação de diversos outros trabalhos. Apesar da mesma conclusão apresentada por todos: a evidência digital é falsa, o trabalho do perito é analisar a maior quantidade possível de dados que o permita concluir de forma objetiva quanto a legitimidade da prova.

Seguindo a estratégia de análise definida no escopo do trabalho é neste momento em que realizamos a observação direta da imagem, com objetivo de elencar hipóteses de adulteração que deverão ser comprovadas nas abordagens posteriores.

Em uma primeira avaliação rasa da imagem podemos observar um alinhamento improvável de linhas e bordas da ficha policial.

ESPECIALIZE

Análise forense de imagens digitais no estudo de caso da ficha criminal de Dilma Rousseff

Dezembro/2018

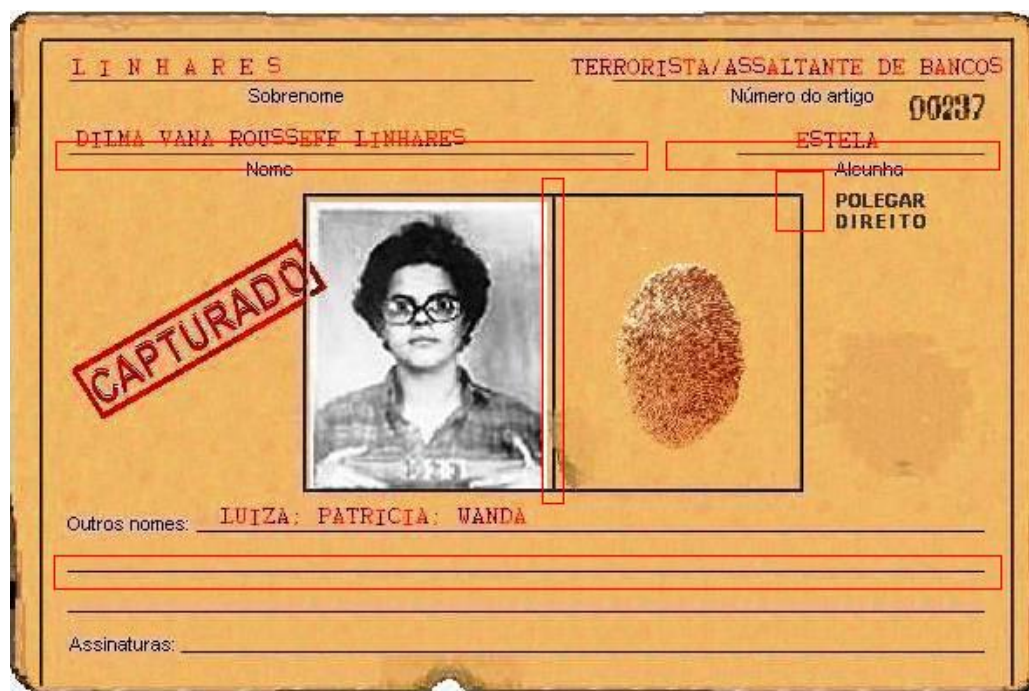


Figura 2 – Linhas perfeitas

Fonte: Elaborada pelo autor

Há um alinhamento (destacado pelos retângulos vermelhos) quase impossível de se reproduzir em um suposto documento confeccionado por impressoras tipográficas da época. Não obstante, o próprio espaçamento entre as linhas dificilmente seria capturado por um scanner padrão com tamanha precisão, mesmo se tivessem sido impressas com alinhamento cirúrgico entre elas. Ressalta-se ainda, a formação de junções entre as linhas perfeitamente alinhadas em ângulos de 90°.

Para abordagem técnica dessas observações utilizaremos a análise de coerência perceptiva, utilizando de recursos do ImageJ, para tentar evidenciar por meio da fotogrametria o suposto alinhamento perfeito das linhas apresentadas.

Em seguida, observamos com mais detalhes a foto da ficha policial:



Figura 3 – Foto da ficha criminal

Fonte: Elaborada pelo autor

Além do alinhamento quase sobre humano em uma foto que teoricamente foi colada à mão, o que chama atenção aqui é a coloração e estado da foto: assim como a ficha supostamente sofreu desgastes com ação do tempo a foto teoricamente deveria ter sofrido envelhecimento semelhante. Todavia, o que observamos é uma imagem “perfeitamente preto e branco”. Não há qualquer evidência visível de borrões, manchas e desgastes que são abundantes no resto da ficha criminal. Para abordagem desta observação utilizaremos a análise de histograma com objetivo de identificar algum vestígio na área em questão.

Finalmente, observamos os campos semelhantes na ficha criminal que denotam aspectos suspeitos em elementos determinados que compõem a evidência digital, surgindo a hipótese de clonagem.



Figura 4 – Letras de carimbo idênticas
Fonte: Elaborada pelo autor

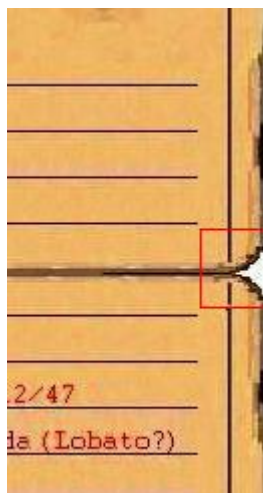


Figura 5 – Bordas semelhantemente desgastadas
Fonte: Elaborada pelo autor

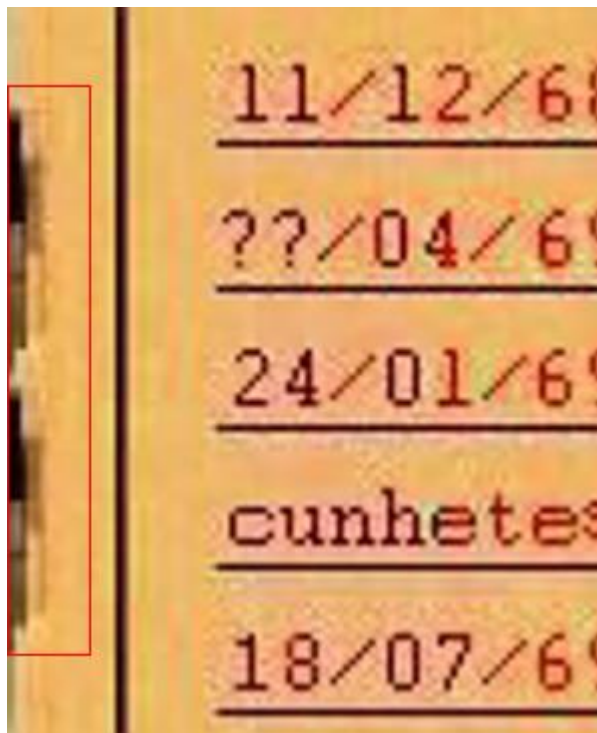


Figura 6 – Desgastes semelhantes na lateral

Fonte: Elaborada pelo autor

Em uma época onde a impressão de papéis e a inserção de dados nos mesmos era realizada de forma mecânica (impressoras tipográficas e máquinas de escrever) não é razoável identificarmos elementos iguais. Além das letras que deveriam possuir borrões e distorções mínimas, ainda podemos identificar padrões aparentemente idênticos de desgastes do papel. Conforme já abordado nos conceitos teóricos no início deste artigo, a clonagem é uma das fraudes mais utilizadas e mais simples de serem realizadas em imagens digitais. Para abordagem dessas observações utilizaremos o método de detecção de clonagens.

3.4 Análise de coerência perceptiva

Neste procedimento analisamos a hipótese de inserção de linhas e contornos na ficha criminal com uso de editor de imagens.

O ImageJ permite a medida de comprimentos e áreas da imagem dada a informação inicial de uma distância conhecida, este processo é baseado nas técnicas de fotogrametria já descritas anteriormente.

Utilizamos o acionamento da opção *Set Scale e Measure* da ferramenta e atribuímos a largura da ficha a dimensão conhecida: 4 polegadas ou 10,16 centímetros.

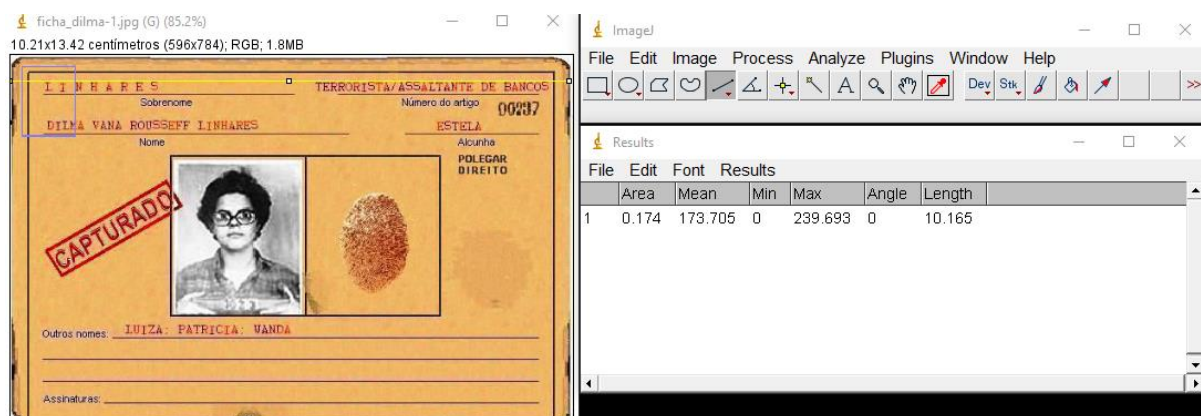


Figura 07 – Configurando escala de medida conhecida na largura da imagem

Fonte: Elaborada pelo autor

Em seguida selecionamos alguns elementos suspeitos da imagem e capturamos suas medidas:

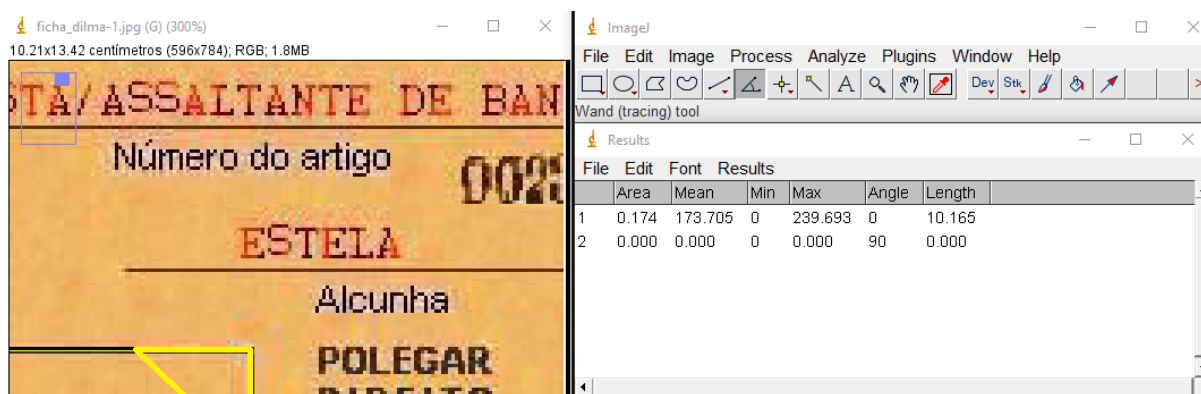


Figura 08 – Medida de ângulo formado por linhas da ficha criminal

Fonte: Elaborada pelo autor

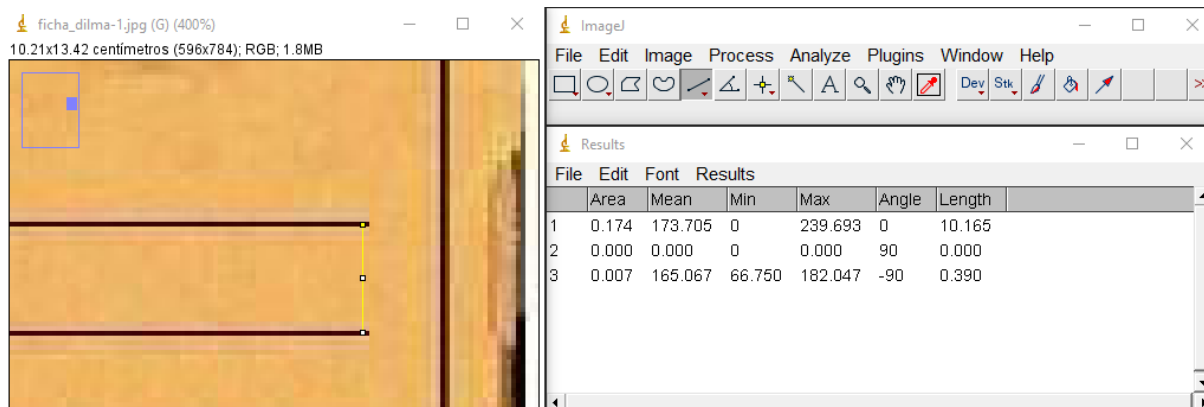


Figura 09 – Distância de linhas consecutivas na ficha (A)

Fonte: Elaborada pelo autor

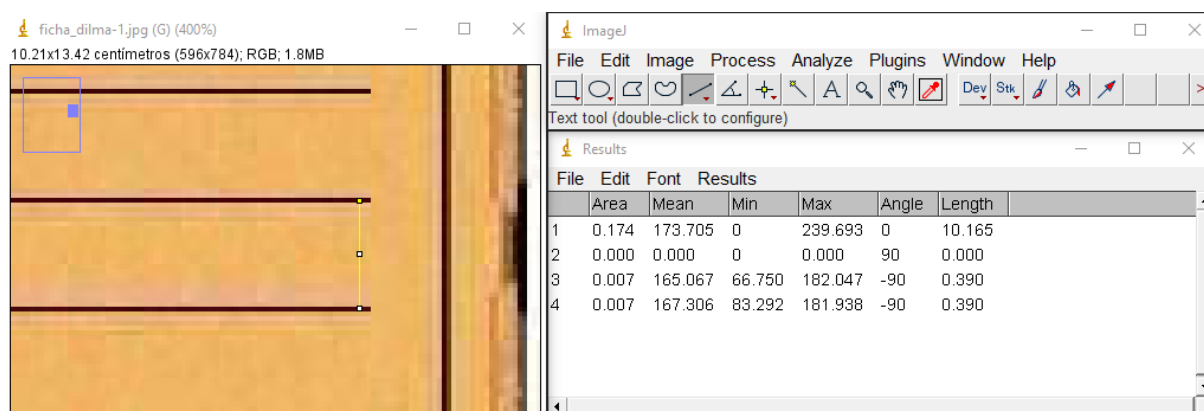


Figura 10 – Distância de linhas consecutivas na ficha (B)

Fonte: Elaborada pelo autor

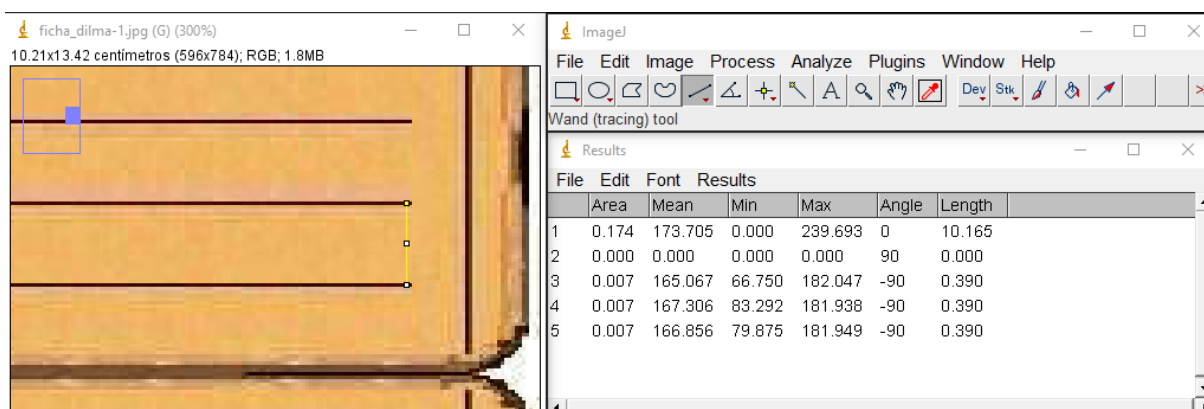


Figura 11 – Distância de linhas consecutivas na ficha (C)

Fonte: Elaborada pelo autor

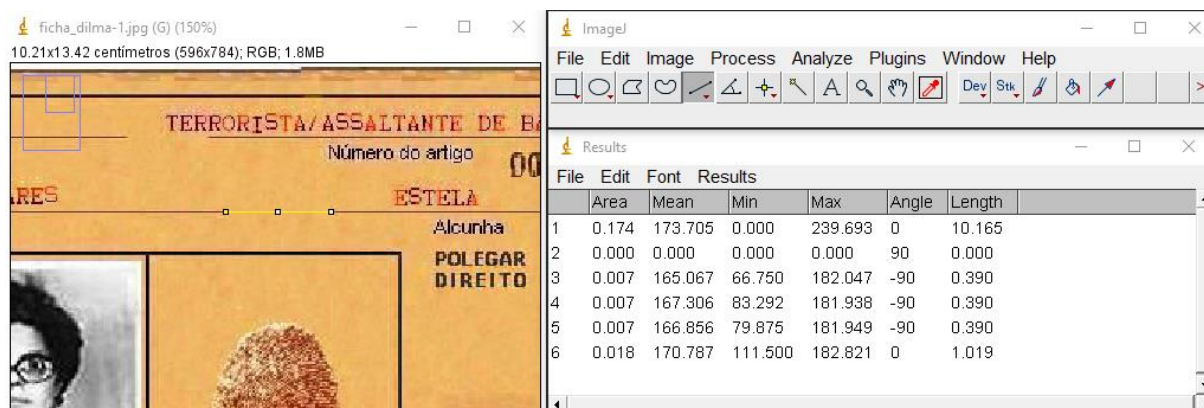


Figura 12 – Alinhamento perfeito de linhas consecutivas

Fonte: Elaborada pelo autor

Resultados:

- Ângulo perfeito de 90° no vértice formado na área alocada para a digital;
- Distanciamento idêntico (0.39 centímetros) de 3 linhas consecutivas da ficha criminal;
- Alinhamento perfeito (ângulo nulo) de linhas consecutivas.

3.5 Análise de histograma nos canais de cor RGB

Nesta análise consideramos a hipótese de inserção direta da foto na imagem da ficha criminal. Na observação direta foi levantada a suspeita de que o referido trecho da imagem não possui qualquer imperfeição: rasgos, desgastes e o conhecido amarelado comum em fotos antigas.

Na primeira fase, isolamos a área de interesse da análise:



Figura 13 – Foto de Dilma
Fonte: Elaborada pelo autor

ESPECIALIZE

Análise forense de imagens digitais no estudo de caso da ficha criminal de Dilma Rousseff

Dezembro/2018

Em abordagem inicial colhemos amostras de pixels da foto e observamos os valores de intensidade nos 3 canais de cor: vermelho, verde e azul. As áreas selecionadas estão marcadas com as setas vermelhas.

Na Figura 14 temos o valor idêntico de intensidade 241 para os 3 canais de cor.

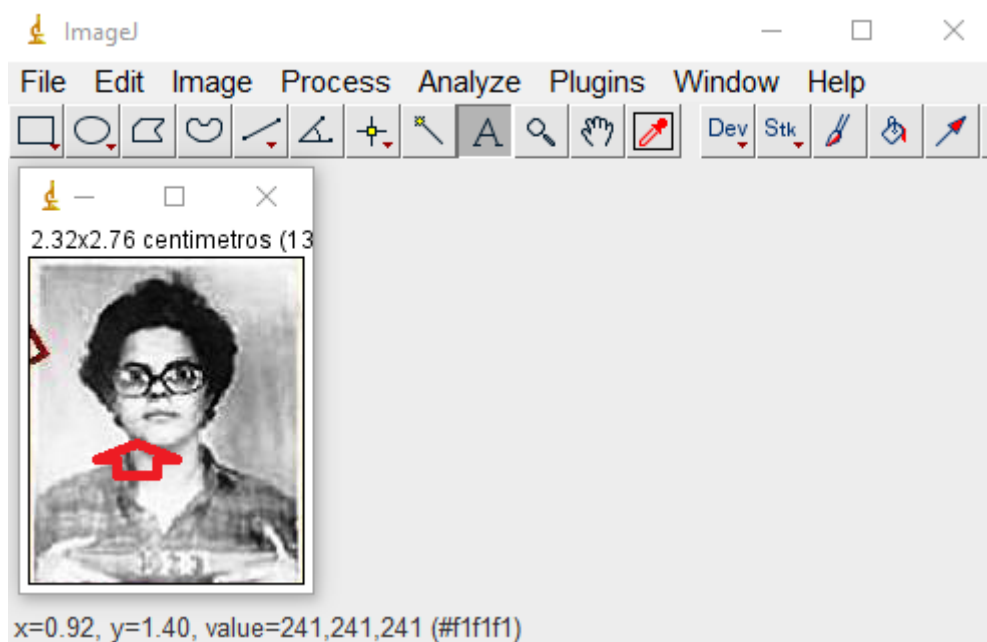


Figura 14 – Foto de Dilma – amostra canais de cor pixel do queixo

Fonte: Elaborada pelo autor

Na Figura 15 temos o valor idêntico de 175 para os 3 canais de cor.

ESPECIALIZE

Análise forense de imagens digitais no estudo de caso da ficha criminal de Dilma Rousseff

Dezembro/2018

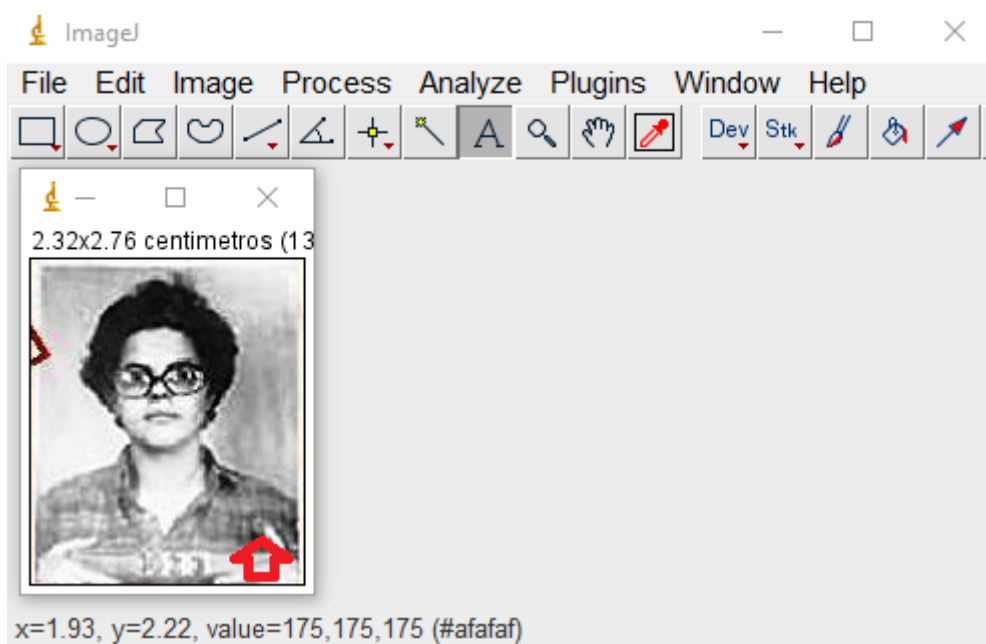


Figura 15 – Foto de Dilma – amostra canais de cor pixel da roupa

Fonte: Elaborada pelo autor

Dezembro/2018

Na Figura 16 temos valores diferentes (251, 239 e 251) para os 3 canais de cor.

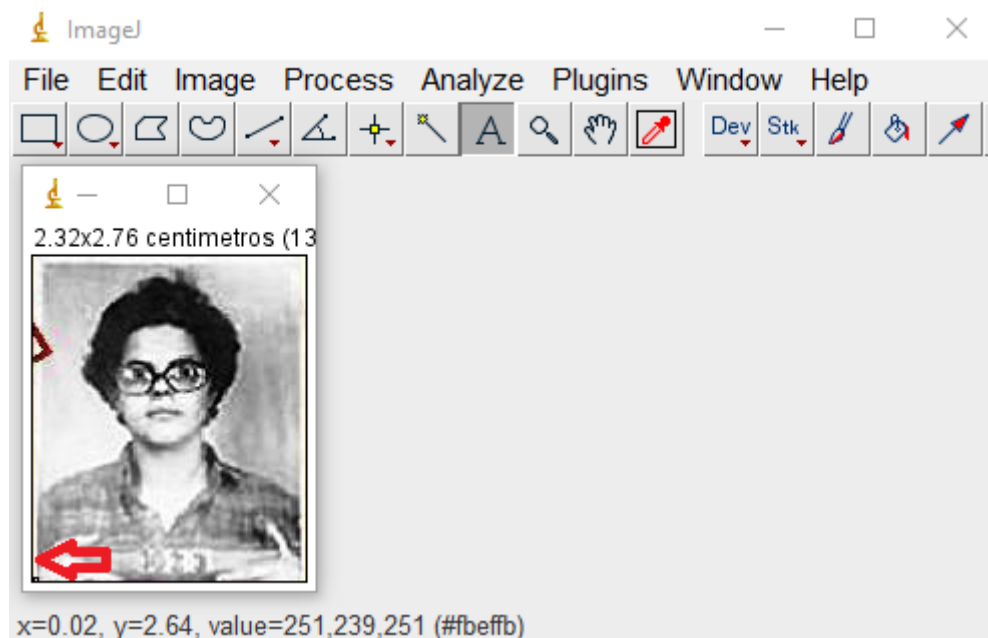


Figura 16 – Foto de Dilma – amostra canais de cor pixel da borda inferior esquerda
Fonte: Elaborada pelo autor

Na Figura 17 temos valores diferentes (104, 014 e 006) para os 3 canais de cor.

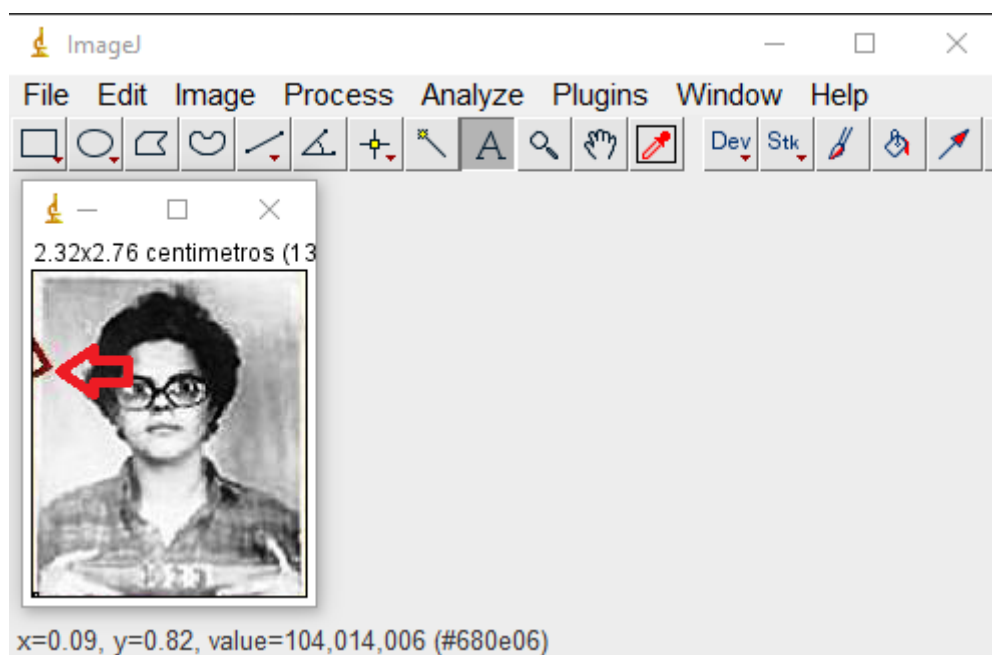


Figura 17 – Foto de Dilma – amostra canais de cor pixel da área de carimbo
Fonte: Elaborada pelo autor

Observamos que na área interior da foto há valores idênticos nos 3 canais de cor para cada pixel observado, enquanto nas áreas externas (borda) e na área invadida pelo carimbo possuímos intensidades divergentes nos canais.

Sendo assim, como análise final extraímos o histograma dos 3 canais de cor da área interna da foto (excluindo bordas e a área do carimbo) e obtivemos os seguintes resultados:

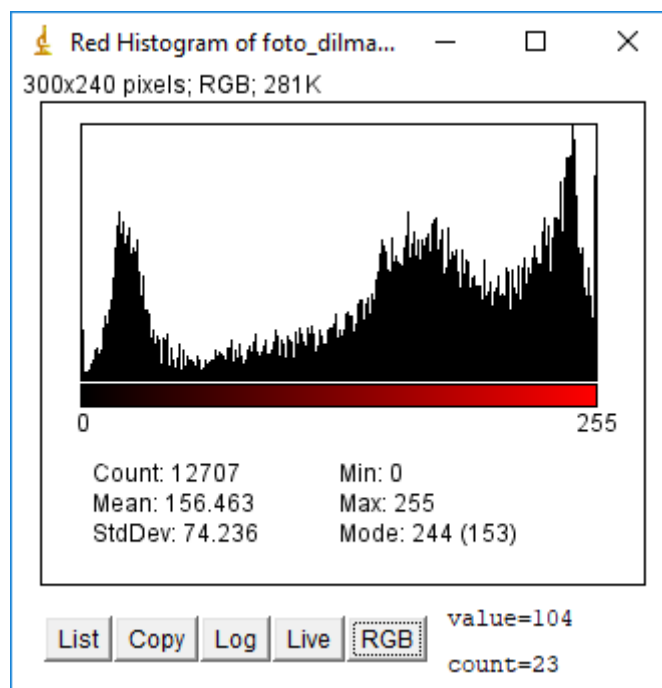


Figura 18 – Foto de Dilma – Histograma do canal de cor vermelho
Fonte: Elaborada pelo autor

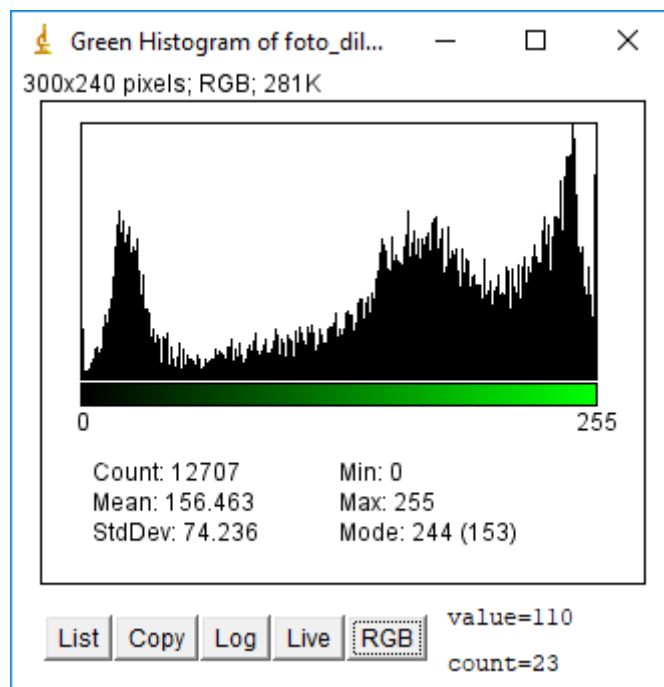


Figura 19 – Foto de Dilma – Histograma do canal de cor verde
Fonte: Elaborada pelo autor

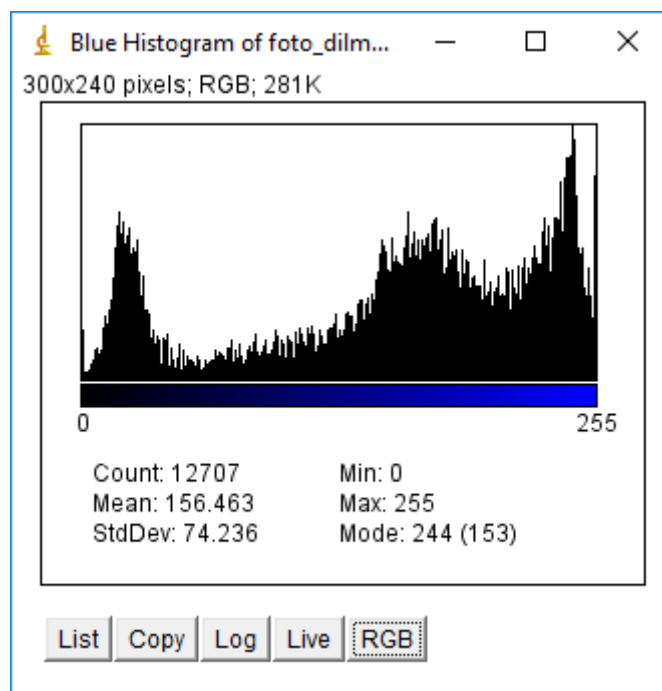


Figura 20 – Foto de Dilma – Histograma do canal de cor azul
Fonte: Elaborada pelo autor

Resultados:

- Valores idênticos de intensidade nos canais RGB nos pixels interiores da foto;
- Valores divergentes de intensidade nos canais RGB nos pixels exteriores da foto e da área invadida pelo carimbo;
- Histogramas idênticos dos 3 canais de cor na área interior da foto.

3.6 Detecção de clonagens

Nesta última análise abordamos os seguintes elementos suspeitos da imagem: danificações artificiais nas bordas e letras provavelmente inseridas com um editor de imagens.

Com uso do ImageJ selecionamos as áreas suspeitas identificadas na fase de observação direta e utilizamos o plugin *Parallel Interactive Deconvolution 2D* utilizando as áreas demarcadas como PSF, obtendo os seguintes resultados após a deconvolução:



Figura 21 – Letra A do carimbo
Fonte: Elaborada pelo autor



Figura 22 – Sinal borda do meio
Fonte: Elaborada pelo autor



Figura 23 – Sinal borda superior (borda rotacionada em 90° à esquerda)
Fonte: Elaborada pelo autor



Figura 24 – Sinal borda inferior
Fonte: Elaborada pelo autor

Resultados:

- Resultado positivo de pico de sinal para as letras A do carimbo “CAPTURADO”;
- Resultado negativo para a borda do meio: apenas a própria borda sinalizou na deconvolução;
- Resultado positivo para borda superior esquerda ao rotacionarmos a borda do meio em 90° à esquerda;
- Resultado positivo para os desgastes na borda inferior esquerda da ficha criminal.

4. Conclusão

Como já observado em outros estudos sobre o caso concluímos que a ficha criminal é falsa. A imagem foi gerada pela composição de diversos elementos inseridos por meio de algum editor de imagens.

Com base nos resultados extraídos das análises é possível determinar a ilegitimidade da evidência digital. Houve semelhante grau eficácia com outros métodos de análise utilizados em trabalhos sobre o mesmo tema. A análise de coerência perceptiva, a análise de histograma nos canais de cor e a detecção de clonagens foram capazes de determinar em seus resultados as hipóteses detectadas na fase de observação direta. Estas hipóteses levantadas na

observação direta e os resultados obtidos nas análises determinaram as seguintes conclusões:

- a) As linhas e contornos da ficha foram inseridas digitalmente na imagem;
- b) A foto não foi escaneada e sim digitalmente manipulada e inserida;
- c) As letras do carimbo com a palavra “CAPTURADO” foram inseridas e não escaneadas;
- d) As bordas desgastadas foram digitalmente inseridas e reutilizadas/clonadas em alguns pontos da imagem: borda superior esquerda e borda lateral esquerda inferior. O provável objetivo do autor da manipulação foi dar um aparente aspecto de desgaste para a evidência nestas alterações.

Do ponto de vista da pesquisa, destaca-se o limitado acervo teórico nacional do assunto, sendo que boa parte das referências do tema encontram-se apenas na literatura estrangeira, salvando-se alguns trabalhos científicos nacionais citados durante este estudo. Além disso, no campo da detecção de clonagens há vários conceitos teóricos, no entanto, poucos trabalhos com sua implementação prática: o que pode dificultar uma análise comparativa de resultados.

Em suma, determina-se que as abordagens utilizadas foram adequadas para a perícia na evidência digital, sem prejuízos de outros métodos e técnicas disponíveis no estado atual da arte.

5. Referências

ARRUDA, Gustavo Henrique Machado de et al. Exames em Imagens Digitais. In: VELHO, Jesus Antonio (Org.). **Tratado de Computação Forense**. Campinas: Millenium Editora, 2016. cap. 6, p. 208-243.

AUTENTICIDADE de Ficha de Dilma não é provada. **Folha de São Paulo**, São Paulo, 25 abr. 2009. Poder. Disponível em: <<http://www1.folha.uol.com.br/folha/brasil/ult96u556855.shtml>>. Acesso em: 08 nov. 2017.

CUNHA, Lucas Marques da; REGO, Thaís Gaudêncio do; BATISTA, Leonardo Vidal. **Reconhecimento de adulteração de imagens JPEG através da inconsistência do Block Artifact Grid**. REVISTA COOPEX, v. 07, p. 1, 2016. Disponível em: <<http://coopex.fiponline.edu.br/pdf/cliente=3-6926315f8535d5893d0e84a139e4de7d.pdf>>. Acesso em: 10 maio 2018.

FREITAS, Greyce Martins de; ESQUERDO, Júlio César Dalla Mora; KORBES, André. Registro de imagens NOAA através de correlação de fase. **Anais... XIV Simpósio Brasileiro de Sensoriamento Remoto**, Natal, Brasil, 25-30 abril 2009, INPE. Disponível em: <<http://martes.sid.inpe.br/col/dpi.inpe.br/sbsr@80/2008/11.18.00.15/doc/6883-6887.pdf>>. Acesso em: 18 abr. 2018.

FREITAS, Andrey Rodrigues. **Perícia forense aplicada à informática**. Rio de Janeiro: Brasport, 2006. 240 p.

FRANCO, Deivison Pinheiro et al. Introdução à Computação Forense. In: VELHO, Jesus Antonio (Org.). **Tratado de Computação Forense**. Campinas SP: Millenium Editora, 2016. cap. 1, p. 1-15.

GOLDESTEIN, Siome; ROCHA, Anderson. **Análise de Procedência e Manipulações Digitais de Imagens**. 2009. 15 p. Disponível em: <http://www.eticaejornalismo.uff.br/PRIN_CIPAL/unicamp.pdf>. Acesso em: 08 fev. 2018.

GOLDESTEIN, Siome; ROCHA, Anderson. CSI: Análise Forense de Documentos Digitais. In: JÚNIOR, Wagner Meira; CARVALHO, Andre Carlos Ponce de Leon Ferreira de (Org.). **Atualizações em informática 2010**. 5. ed. Rio de Janeiro: PUC Rio, 2010. cap. 6, p. 263-317. Disponível em: <<http://www.ic.unicamp.br/~rocha/teaching/2012s2/mo447/docs/csi-analise-forense-de-documentos-digitais-menor.pdf>>. Acesso em: 18 fev. 2018.

GRUPO Terrorismo Nunca Mais. Disponível em: <<http://www.ternuma.com.br/>>. Acesso em: 21 nov. 2017.

Dezembro/2018

IMAGEJ: Image Processing and Analysis in Java. Disponível em: <<https://imagej.nih.gov/ij/index.html>>. Acesso em: 21 maio 2018.

IMAGEJ. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2018. Disponível em: <<https://pt.wikipedia.org/w/index.php?title=ImageJ&oldid=52149068>>. Acesso em: 21 mai. 2018.

LAMPA. **Ficha policial da Dilma, falsa ou verdadeira?**. Disponível em: <<https://www.mdig.com.br/index.php?itemid=6150>>. Acesso em: 15 nov. 2017.

MEMÓRIA da ditadura. **Folha de São Paulo**, São Paulo, 05 abr. 2009. Poder. Disponível em: <<http://www1.folha.uol.com.br/fsp/brasil/fc0504200908.htm>>. Acesso em: 08 nov. 2017.

TOMMASELLI, A. M. G. Introdução. In: **Fotogrametria Básica**. Santa Catarina. UDESC, 2009. P.1-14. Disponível em: <http://www.faed.udesc.br/arquivos/id_submenu/891/introducao_a_fotogrametria.pdf>. Acesso em: 20 fev. 2018.

WENDYKIER, Piotr. **Parallel Iterative Deconvolution**. Disponível em: <https://imagej.net/Parallel_Iterative_Deconvolution>. Acesso em: 14 mar. 2018.