Danilo Souza - 10080000801
Hugo Leonardo - 10080000701
Iago Medeiros - 1008000XX01
Welton Araújo - 10080000501

Análise Forense de Imagens

Belém

2013

Danilo Souza - 10080000801
Hugo Leonardo - 10080000701
Iago Medeiros - 1008000XX01
Welton Araújo - 10080000501

Análise Forense de Imagens

Cartilha destinada aos peritos do Instituto de Criminalísticas Renato Chaves com o intuito de informar sobre as principais técnicas relacionadas à Análise Forense de Imagens bem como mostrar as técnicas implementadas pelos alunos da UFPA.

Orientador: Ronal de Freitas Zampolo

Universidade Federal do Pará

Belém

2013

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

O Instituto Renato Chaves possui o difícil trabalho realizar perícias em diversas áreas e, assim como outras instituições com a mesma função, sofre com sobrecarga de trabalho, por trabalharem quase sempre de forma não automatizada. Portanto é importante que técnicas mais rápidas e com alto desempenho e confiabilidade sejam utilizadas para a análise do material a ser periciado. A compreensão dessas técnicas é importante para que os peritos possam entender principalmente suas limitações e ter o conhecimento sobre qual a técnica mais apropriada para ser utilizada em determinadas situações. Sabendo que em muitos casos os peritos do instituto não são da área da computação, a cartilha foi elaborada de forma bastante intuitiva para que todos os profissionais possam entender e até repassar esse conhecimento. Além de poder apresentar a cartilha para visitantes do instituto como forma de expansão de conhecimento e divulgação do trabalho realizado pela Instituição. Esta cartilha tem como objetivo principal informar os peritos da instituição sobre as técnicas existentes no âmbito da análise forense em processamento de imagens, mais precisamente na questão do reconhecimento imagem-câmera, onde através de uma imagem seria possível dizer de qual câmera essa imagem foi tirada.

2 Termos técnicos

2.1 Super resolução

2.2 PRNU

As imagens das câmeras são capturadas através de foto-sensores, que possuem imperfeições de fabricação que são únicas a cada sensor, essas imperfeições representam a diferença na forma com que cada sensor converte sinal luminoso em energia elétrica. Essa diferenças fazem com que cada imagem possua uma ?impressão digital? equivalente a ?impressão digital? da câmera. A PRNU é estimada para cada câmera sob suspeição, por meio de um processo de acquisição de imagens, a literatura recomenda o uso de 30 a 50 imagens. Para o processo de verificação, estima-se a PRNU da imagem suspeita e compara-se com a PRNU da câmera, o resultado é um número que indica a correlação entre a imagem e a câmera sob suspeição, para valores acima de um limiar resultante pode-se dizer se uma determinada imagem foi adquirida ou não de uma determinada câmera. A grande vantagem de se utilizar a PRNU para realizar análises forense, além de possui características únicas, como a ?impressão digital?, possui também uma forte resistência a perda de dados, ou seja, mesmo que a imagem tenha sido comprimida mais de uma vez em um determinado formato, a PRNU permanece intacta o suficiente para realizar a perícia com um alto grau de confiabilidade.

2.3 Manipulação de Imagens

Manipulação de imagens é o nome que se dá ao ato de mudar manualmente ou digitalmente uma fotografia. Atualmente, muitas das imagens são mudadas digitalmente por softwares especializados em edições de imagens, como o Adobe Photoshop. Mas a manipulação é uma prática antiga. No passado, para alterar as imagens, utilizavam algumas técnicas rústicas como múltipla exposição dos negativos, impressão sobreposta, montagem, retoques ou até mesmo pintura sobre

a foto. Os motivos da manipulação são diversos: marketing, políticos, estéticos ou até artísticos. E com o acesso cada vez mais fácil aos computadores e a distribuição crescente desses softwares de edição de imagens, devemos estar preparados para identificá-los.

2.4 *Fingerprint* (Impressão Digital)

É o conjunto de PRNUs de todos os foto-sensores da câmera. Como cada foto-sensor é único, todos eles juntos causam uma interferência também única em todas as mídias originadas a partir da mesma câmera.

3 *Principais técnicas relacionadas à PRNU*

3.1 Identificação de câmeras

O cenário mais frequente é a identificação da origem de uma foto ou vídeo. Muitas vezes a investigação possui uma câmera e uma foto, portanto é necessário definir se esta mídia foi capturada por esta câmera. Este processo ocorre com obtenção da impressão digital da câmera utilizando a PRNU. Em seguida, verifica-se se a imagem ou o vídeo contem ou não esta mesma impressão digital. Caso a correlação entre as duas impressões digitais seja alta, pode-se atestar a origem da mídia no dispositivo investigad

3.2 Associar imagens a um mesmo dispositivo

Etapas para identificaçã do dispositivo:

- Estimação da PRNU do dispositivo a sob análise: Para esta etapa recomenda-se o uso de 30 a 50 imagens que possuam iluminação uniforme e controlada, por exemplo, céu nublado e superfícies lisas. Assume-se que esse processo de estimação depende da intensidade luminosa que chega ao sensor, dos ruídos associados à aquisição da imagem, do rúido de quatização da codificação, geralmente para o formato JPEG, do fator de correção e também de uma componente, representada por uma matriz K com média zero.

- Avaliação da imagem de teste Calcular a correlação normalizada cruzada (NCC): Esta etapa calcula a correlação entre a imagem de teste e a matriz K?, sendo esta uma estimativa da matriz K da etapa anterior, e depende principalmente das transformações que possam ter sido realziadas na imagem, tais como rotação, redimensionamento e codificação. Calcular o pico de correlação de energia (PCE): Este parâmetro depende sumariamente do

maior valor de NCC calculado e é este resultado que vai indicar a conexão entre a imagem de teste e a câmera sob análise.

3.3 Comparar PRNU's

Cada PRNU é única. Sendo assim, a comparação de PRNU é um importante meio de saber se uma câmera é ou não dona de uma fotografia suspeita. Sabendo isso, estabelece-se um limiar e compara-se os PCE das câmeras avaliadas. Quanto maior o PCE estiver acima desse limiar, mais provável é a chance de que a fotografia suspeita seja proveniente daquela câmera.

4 Principais técnicas relacionadas à análise de adulteração de imagens

4.1 Baseadas em pixel

Todas as fotos e vídeos têm suas características mostradas a partir dos pixels. Neles são definidos as cores e bordas torna possível visualizar a imagem em um computador. Esse conjunto de pixels do arquivo mídia contém informações que podem ser extraídas para analisar a falsificação da mídia.

4.1.1 Clonagem

A forma de clonagem mais comum é inserção de um pedaço de uma imagem por cima da outra objetivando-se esconder uma pessoa ou objeto. Se esta manipulação for feita com qualidade, pode ser visualmente difícil detectá-la. Porém para detectá-la computacionalmente é impossível devido a posição, forma e tamanho serem desconhecidos , portanto seriam necessários testar todas as forma possíveis. A solução é utilização de alguns algoritmos eficientes para realizar a detecção.

4.1.2 Mudança de Escala

É comum ser necessário diminuir, aumentar, rotacionar ou esticar pedaços de imagem para que as novas imagens inseridas tenham compatibilidade com os tamanhos dos objetos da imagem original. Este processo gera uma correlação periódica entre pixels vizinhos com baixíssima probabilidade de acontecer naturalmente e pode ser detectada computaciolmante.

4.1.3 Junção de Imagens

Trata-se da junção de uma imagem ao lado da outra. Se realizada de forma cuidadosa pode ser difícil detectá-la visualmente, porém esta junção pode ser detectada devido a uma mudança significativa grande e repentina nos valores de medição da correlação entre as sequências de pixels.

4.2 Baseadas no formato

Grande parte dos dispositivos utilizados comercialmente hoje em dia realizam compressão no formato JPEG para armazenamento das imagens, este procedimento por si só já fere um dos princípios básicos da análise forense que é a preservação das evidências, porém este mesmo procedimento deixa rastros que podem ser utilizados pelos peritos para descobrir se uma imagem comprimida no formato JPEG sofreu ou não alterações ou se foi tirada ou não de um determinado dispositivo. A seguir será mostrado um breve resumo das principais técnicas que utilizam a compressão JPEG como aliada para auxiliar no trabalho de perícia.

4.2.1 Quantização JPEG

Apesar do formato de compressão ser o mesmo, os fabricantes costumam configurar seus dispositivos de forma diferente a fim de obter resultados entre compressão e qualidade de acordo com suas necessidades e esta diferença pode ser usada para descobrir se uma imagem veio de um determinado dispositivo. A principal diferença entre as codificações utilizadas por cada fabricante é a a escolha da tabela de quantização, utilizada para realizar a compressão, dessa forma uma assinatura de ?tipos? é incorporada à Imagem.

4.2.2 Dupla compressão JPEG

Qualquer manipulação de imagens digitais requer que uma foto seja carregada em algum editor de fotos e por suas vez salva novamente, na maioria das vezes no formato JPEG, como a maioria das imagens já foi salva nesse formato na hora da captação, ocorre uma segunda compressão em JPEG. A segunda compressão acaba introduzindo características específicas, que não ocorrem na compressão simples, na imagem, devido à natureza com perdas deste tipo de compressão. E essas características podem ser usadas como evidências de que a imagem foi manipulada, é possível ainda detectar se somente uma parte da imagem foi adultera.

4.2.3 Blocos JPEG

A base da compressão JPEG é a transformada discreta do cosseno (DCT) em blocos, cada pixel (bloco de imagem) é uma matriz 8X8 transformada e quantizada individualmente, esse processo deixa características aparentes nas bordas de blocos vizinhos na forma de arestas verticais e horizontais. Quando uma imagem é modificada e comprimida novamente, um novo conjunto de blocos é introduzido, porém esses blocos não se alinham com os blocos da imagem original.

4.3 Baseadas na câmera

Toda vez que uma câmera fotográfica tira uma foto, deixam certas "assinaturas" (ou impressões digitais) na imagem, mesmo sem querer. Por isso, detectar estas "assinaturas" em uma câmera tem grande utilidade.

4.3.1 Aberração cromática

Aberração cromática é um problema bem comum em câmeras fotográficas. O fenômeno acontece naturalmente nas fotografias e é potencializado quando fotografamos algo contra a luz ou em um ambiente com grandes diferenças de contraste. Figura 1 nos mostra esse ?defeito?.

Figura 1: Imagem corrigida (acima) e a imagem com aberração cromática (abaixo)

É bem usual que a aberração cromática ocorra nas bordas da imagem capturada ou nas figuras com muitos constrastes. As imagens nas câmeras são construídas utilizando as cores RGB (vermelho, verde e azul). Quando a aberração cromática acontece, essas três cores não são focadas no mesmo ponto (devido aos seus diferentes comprimentos de onda). Dessa forma, nota-se um desequilíbrio

das cores (desfocamento, ou até mesmo deformação lateral) que compõem aquele ponto da imagem fotografado.

4.3.2 Matriz de filtro de cor

A vasta maioria das câmeras trabalham com 3 cores básicas, RGB. Na teoria, para que um objeto seja perfeitamente fotografado e salvo pela câmera, deveria haver 3 tipos de sensores, um para registrar cada cor diferente (vermelho, verde, azul). No entanto, pouquíssimas máquinas fotográficas possuem 3 sensores diferentes. Normalmente, só há um sensor. Para sanar este problema, usa-se a interpolação da matriz (mosaico) do filtro de cor. Essa interpolação consiste em guardar uma única cor em um pixel, e estimar a quantidade das duas outras cores. O filtro de cor mais comum chama-se Filtro de Bayer (ou Bayer CFA), mostrado na figura 2.

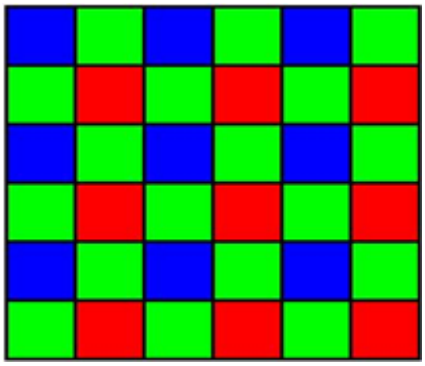

Figura 2: Disposição das cores no Filtro de Bayer

No filtro de Bayer, a imagem é capturada pelo sensor quando fotografamos. Ela dividirá toda a imagem em vários pixels, menor unidade de tela. E analisará cada pixel por vez. Em cada pixel, guardará ou R ou G ou B. Depois de estabelecer isso para um pixel, avançará para o adjacente e perguntará: ?Qual cor (RGB) melhor representa este minúsculo ponto?? Depois de escolhido apenas um dentre as três cores, avançará para o próximo pixel, analisará, salvará a cor correspondente e assim sucessivamente até que todos os pontos guardem uma cor. A proporção das outras cores não selecionadas em um pixel são estimadas, como visto na figura 3.

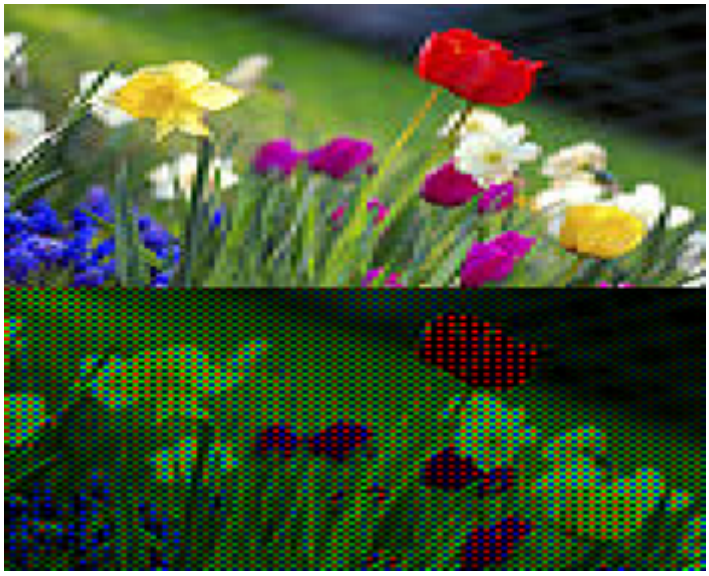

Figura 3: Original (acima) e imagem interpolada usando filtro de Bayer (abaixo)

4.4 Baseadas no meio físico

Fonte de luz, como a luz do sol, da lua ou de uma lâmpada, podem ser importantes aliados na detecção de imagens adulteradas. Sabendo disso, deve-se analisar com cuidado estas fotos para rapidamente detectar montagens.

4.4.1 Direção da luz (2D)

4.4.2 Direção da luz (3D)

4.4.3 Iluminação ambiente

4.5 Baseadas na geometria

4.5.1 Ponto principal