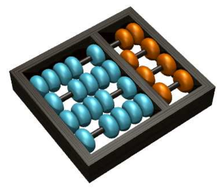
DETECÇÃO DE FALSIFICAÇÕES EM IMAGENS DIGITAIS

Orientador: Prof. Dr. Siome Klein Goldenstein

Aluno: Thiago Henrique Parra

LOCO - IC - UNICAMP

email: siome@ic.unicamp.br, ra046718@students.ic.unicamp.br



SAE/PIBIC

Adulteração de Imagens, Análise Forense de Imagens, Detecção Falsificações

Introdução

Com a difusão de câmeras digitais e softwares de edição de imagens, a captação e adulteração de cenas com fins ilícitos ou objetivando a manipulação de opiniões tornam-se a cada dia mais evidente. Há tempos a mídia utiliza-se da edição de imagens para enfatizar fatos captados ou até mesmo impactar a população com momentos criados digitalmente e que nunca aconteceram. Outra importante área atingida constantemente por imagens adulteradas é o Direito legal onde comumente imagens são utilizadas como provas em processos jurídicos. Por ser considerado um material válido como prova, faz-se necessária a comprovação da autenticidade de fotografias digitais. A manipulação de fotos é tão antiga quanto a própria fotografia. Algumas das mais antigas e relevantes evidências referem-se a década de 1930, quando Joseph Stalin assumiu o poder da União Soviética e, na tentativa de eliminar seus inimigos dos arquivos históricos soviéticos, tomou medidas como a edição de fotografias. Leon Trotsky, por exemplo, foi removido de imagens em que aparecia ao lado de Stalin (Figuras 1, 2, 3 e 4). Atualmente, o tratamento de fotografias digitais é bastante comum, a edição abrange desde simples ajustes no brilho e contraste, passando por mudanças de cor e formas, e chegando até a remoção, adição ou substituição de regiões e informações da imagem. Uma questão ética bastante recorrente a respeito de fotografias digitais é ”Qual seria a o limite na edição que separa uma fotografia autêntica e uma adulterada?”. A resposta a essa pergunta é bastante relativa ao impacto legal ou psicológico causado pelas adulterações. Um fator agravante nessa questão diz respeito à dificuldade de detecção de manipulações em imagens. A ausência ou mesmo não praticidade de marcas d’água em fotografias digitais impossibilita a verificação eficiente de sua autenticidade. Assim, há uma carência de informações explícitas sobre as alterações realizadas, e torna-se necessário o desenvolvimento de ferramentas que detectem perturbações nas imagens através da análise automática de suas informações (e.g., de seus pixels e suas correlações).

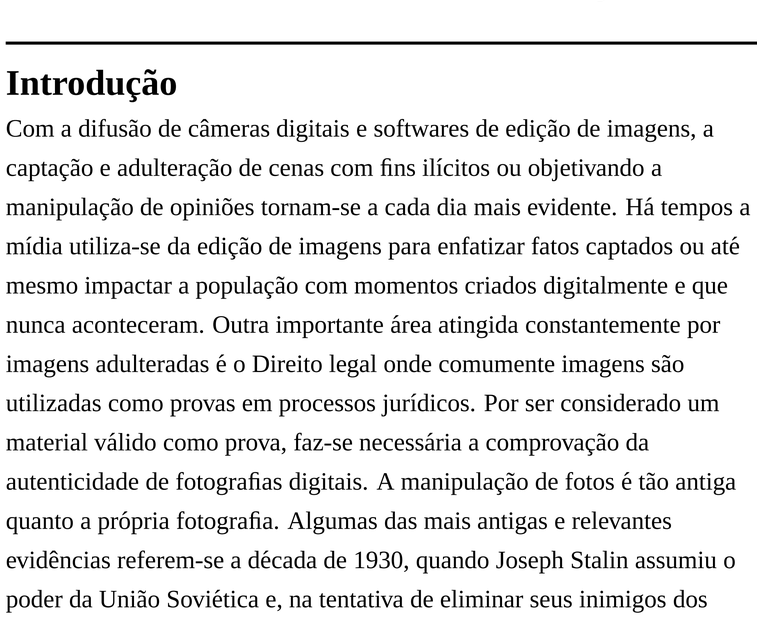


Figure 1: Imagem Manipulada

Figure 2: Imagem Original

Metodologia

Atualmente, as várias técnicas propostas para verificar a autenticidade de imagens digitais não têm padronização, e são testadas em bancos de imagens diferentes, tornando difícil a comparação de seus desempenhos. Buscamos implementar algumas dessas técnicas publicadas e testá-las em um mesmo conjunto de imagens, para tornar possível a comparação da efetividade e eficiência de cada uma delas. Posteriormente, objetivamos possíveis aperfeiçoamentos através de aprendizado de máquina e da combinação de suas características através de métodos para seleção de seus melhores atributos. Tendo realizado esse estudo inicial, selecionamos as principais técnicas propostas, para implementá-las. A primeira técnica foi a Binary Similarity Measures (BSMs). Esta abordagem explora as correlações dentro dos planos binários de menor ordem das imagens, que, por hipótese, são mais afetados por manipulações e, geralmente, preservam algumas das características da câmera combinadas com o conteúdo da imagem. Posteriormente, partimos para o segundo método: Image Quality Measures (IQMs). Este método avalia a autenticidade da imagem a partir da extração de características de medidas de qualidade. Para isso, foi feito um estudo de transformadas de sinais para o domínio da freqüência utilizando Transformada de Fourier e Transformada Discreta de Cossenos aplicadas a imagens.

Em seguida, iniciamos a implementação do terceiro grupo de técnicas: High-Order Wavelet Statistics (HOWS). Esta técnica extrai características da decomposição multi-escala da imagem para sua avaliação.

Paralelamente, também foi implementada uma ferramenta com interface gráfica para marcar regiões poligonais em imagens para a criação de máscaras. Essa ferramenta seria utilizada posteriormente na fase de testes dos métodos, para manter um controle das regiões onde terão sido feitas as manipulações nas imagens. Quando o projeto foi interrompido, estava sendo implementada a terceira técnica (HOWS). Após seu término, seriam feitos os primeiros testes com um banco de dados de imagens com manipulações simples, para verificar o funcionamento correto das técnicas e seus primeiros resultados, assim como dar início a etapa de aprendizado de máquina. Em seguida, partiríamos para a implementação de mais algumas técnicas, e para a construção de uma ferramenta automatizada para gerar um grande banco de imagens com diferentes manipulações. Posteriormente, seriam realizados os testes, em paralelo com os aprimoramentos, a fase de aprendizado de máquina e a combinação de características de diferentes técnicas. Ao término de todas essas fases, teríamos como resultado uma análise comparativa dos desempenhos das diferentes técnicas abordadas e, possivelmente, uma ferramenta aprimorada baseada em todas elas.

Figure 3: Imagem Original

Figure 4: Imagem Manipulada

Resultados

Durante o desenvolvimento do projeto, optamos por concentrar o trabalho primeiramente na implementação das três primeiras técnicas (BSM, IQM e HOWS). Após esta etapa, daríamos início aos primeiros testes de eficiência e efetividade dos métodos propostos. Até a interrupção do projeto, não foram obtidos resultados de teste/validação da aplicação das técnicas para que pudessem ser apontados aqui.

Conclusões

Devido a interrupção no desenvolvimento do projeto, paramos a implementação e não chegamos a fase de testes. Devido a isso, nenhum resultado pôde ser exposto aqui, mas ainda assim supomos uma boa eficácia para as técnicas apresentadas, restando apenas quantificá-las e compará-las.