Detecção de Adulterações em Imagens Digitais

Sérgio Xavier, Galileu Batista e Eduardo Amaral

***Abstract* — Today's image manipulation software makes tampering digital photographs accessible to the common user. Digital hoaxes arise all over the Internet. Some of these forgeries have criminal implications. This paper discusses several techniques to identify signs of these forgeries so the investigator can verify whether a digital image is authentic or not.**

***Index Terms*— Digital Forgery, Tampering, Digital Image.**

I. Introdução

Gostemos ou não, imagens adulteradas – as conhecidas montagens – estão em todos os lugares e fazem parte de nossa cultura hoje em dia. Graças à popularidade das câmeras digitais e a disponibilidade de softwares de edição de imagens, essas falsificações se tornaram "lugar comum", especialmente na Internet.

Nós vemos muitas imagens que desafiam o senso comum e é natural questionar sua autenticidade. A maioria de nós já viu imagens que são obviamente falsas, como uma imagem de um gato gigante escalando o cristo redentor, mas naturalmente assumimos que não passam de montagens criadas simplesmente para nosso divertimento. Entretanto, há vários casos em que uma montagem é divulgada como sendo real, deixando a nosso critério decidir se determinada imagem é real ou não.

Várias dessas montagens possuem fins ilícitos – de meras difamações até crimes eleitorais – cabendo à Perícia Criminal analisá-las e determinar se são autênticas ou se não passam de falsificações.

A perícia de imagens – sejam elas digitais ou não – deve-se basear mais do que no simples bom senso do perito. Ela deve ser fundamentada em uma metodologia de análise que, baseada nas evidências encontradas, permita determinar a sua autenticidade.

Infelizmente não há um método infalível para determinar se uma imagem é autentica. Entretanto, se entendermos como as adulterações são feitas e soubermos quais características da imagem analisar, poderemos detectar a maior parte dessas adulterações.

O presente trabalho visa descrever técnicas que permitam ao Perito encontrar evidências de adulterações em imagens digitais, a fim de determinar a sua autenticidade.

II. Um pouco de história

Adulteração de imagens não é algo novo e nem recente. Alguns dos mais conhecidos exemplos de adulterações de filmes fotográficos, por exemplo, datam dos primeiros anos da extinta União Soviética, onde tanto Lênin como Stalin costumavam remover os "inimigos do povo" dos registros históricos. (**Figura 1**). Essas e outras adulterações similares eram criadas utilizando manipulações de imagens tais como: clareamento, escurecimento, retoque, spray e ajuste de cores e contraste. [5]

- A técnica do spray funciona através do uso de uma pistola (em formato de lápis) que borrifa tinta líquida, em baixa pressão, com o auxílio de ar comprimido.
- Os retoques são realizados diretamente sobre a película do filme com um pincel de ponta bem fina.
- Clareamento e escurecimento são manipulações que mudam a intensidade da exposição, sendo utilizadas máscaras fotográficas para delimitar as áreas afetadas.
- O controle de cores e contraste é realizado com o auxílio de filtros de luz especiais e papel fotográfico.

Figura 1: Acima, a foto original de Stalin e Nikolai Yezhov. Abaixo, a versão alterada onde Yezhov foi removido.

Todas estas manipulações requerem um alto grau de conhecimento técnico e material fotográfico sofisticado, que, em geral, estão fora do alcance da maioria das pessoas.

Nos últimos anos, câmeras digitais de alta resolução, a preços acessíveis, vêm rapidamente substituindo suas contrapartes baseadas em filme fotográfico. Além disso, o advento de computadores de baixo custo e alto desempenho e sofisticados softwares de manipulação de imagens e computação gráfica permitiram ao usuário mediano realizar

manipulações complexas em imagens e criar montagens com relativa facilidade.

III. Imagens Digitais

Uma imagem digital é, essencialmente, uma matriz de números, onde cada número representa o tom de cada ponto que compõe a imagem, também chamado de *pixel* (**Figura 2**). Uma imagem de 8-bits pode ter 256 tons de cinza. Uma imagem colorida é feita através da combinação de três imagens, cada uma representando uma das cores básicas: vermelho, verde e azul (RGB). A adição de diferentes quantidades dessas três cores básicas produz todas as demais cores do espectro. [1]

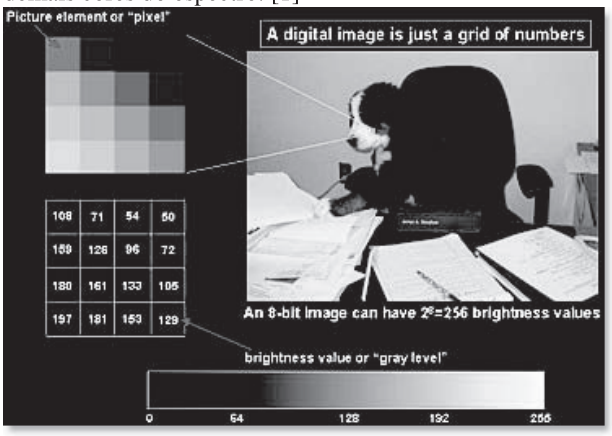

Figura 2: Uma imagem digital é simplesmente um array de números correspondentes aos tons da imagem.

Uma câmera digital funciona tal qual uma câmera tradicional, mas não requer filme para armazenar as imagens. Em vez disso, as imagens são armazenadas em chips de memória no interior da câmera. As imagens são capturadas por um dispositivo chamado *charged-coupled device* (CCD): uma coleção de milhares de células foto-sensíveis. Quando essas células são atingidas por um raio de luz, elas emitem sinais elétricos, que depois são convertidos na imagem digital.

IV. Adulterações em Imagens Digitais

Sendo, uma imagem digital, apenas um conjunto de números, é tecnicamente possível a um artista criar uma imagem "artificial" simplesmente escolhendo cada um dos números adequadamente para representar qualquer objeto ou cena que poderia ser capturado por uma câmera digital. Para uma imagem colorida (24 bits por *pixel*), há mais de 6 milhões de valores possíveis para cada *pixel*. Uma imagem 10cm x 15cm a 300 ppp (pontos por polegada) terá mais de 2 milhões de *pixels*, dando um total de mais de 36.000.000.000.000 de alternativas a considerar para se gerar uma imagem colorida.

Na verdade, nem todos os números possíveis precisam ser considerados pelo usuário, mas importantes considerações precisam ser feitas para se escolher os valores de cada *pixel*, principalmente quando iluminação e bordas são consideradas. Se uma imagem gerada por computador deve parecer ser real, então a imagem deve ser consistente com todas as leis da física aplicáveis às imagens reais.

Para se criar uma imagem digital que pareça real, os valores corretos de brilho devem ser escolhidos *pixel* a *pixel*, o que poderia levar meses (ou mesmo anos), dependendo do tamanho da imagem, sem a ajuda de software de computador para efetuar os cálculos. Esse tempo diminuiu bastante após o advento de softwares de computação gráfica, projetados para gerar imagens de objetos 3D com condições de iluminação realistas. Uma operação de renderização adiciona iluminação, sombras cores e texturas a um modelo de objeto que é criado pelo artista.

Modelos baseados na técnica de *Ray-Tracing* produzem os melhores resultados pela projeção de vários raios de luz e pela modelagem das interações desses raios com os objetos da cena, incluindo reflexão, refração e outros. O usuário deve simular uma quantidade suficiente de raios para cobrir todos os pontos da imagem, o que pode ser um processamento muito demorado. Os resultados são impressionantes e podem ser vistos em filmes de cinema. Entretanto, essa técnica é pouco utilizada na produção de imagens falsas devido à quantidade de cálculos necessários, sua complexidade e pelo fato do software envolvido não estar, geralmente, acessível ao usuário comum. (**Figura 3**)

Figura 3: Imagens geradas por computação gráfica com o auxílio dos softwares Maya, Mental Ray e Photoshop.

A maneira mais comum de se falsificar uma imagem, devido a sua simplicidade, é alterar uma imagem já

existente, que tenha sido capturada por uma câmera. A imagem pode ser alterada de duas formas: pela mudança de contexto e pela mudança de conteúdo.

A. *Mudança de Contexto*

Uma imagem pode ser alterada pela mudança de seu contexto. Um exemplo seria afirmar que uma imagem de uma lâmpada acesa é, na verdade, uma nave espacial alienígena.

Criar uma imagem falsa pela mudança de contexto tem sido, historicamente, o método preferido para se criar boatos, porque não necessita de nenhuma alteração na imagem, sendo a mesma uma imagem real. Dessa forma, a imagem (e seu negativo, se existir), vai passar por todos os testes científicos de verificação de autenticidade. Um exemplo conhecido é a famosa foto do monstro do Lago Ness, tirada em 1934 e que só foi confirmada como sendo falsa, após a confissão do autor, muitos anos depois. (**Figura 4**)

Figura 4: Foto do monstro do Lago Ness. Na verdade não passa de um submarino de brinquedo com uma cabeça de serpente anexada.

B. *Mudança de Conteúdo*

Tornou-se muito utilizada com o advento de softwares de tratamento de imagem de baixo custo, permitindo a qualquer um alterar rapidamente as imagens de forma criativa. As principais técnicas utilizadas nesse tipo de adulteração são:

- Composição: Uma das formas mais comuns de adulteração em imagens digitais, onde duas ou mais imagens são coladas juntas para a criação da montagem. A abordagem mais utilizada é simplesmente retirar uma parte de uma imagem e colá-la (digitalmente) em outra. O software permite ao usuário modificar a imagem recortada de forma a ajustar tamanho, rotação, brilho, etc. (**Figura 5**)

Figura 5: Montagem realizada por composição. O tubarão está iluminado a partir da frente enquanto que o resto da imagem está iluminado por trás.

- Retoques: É uma ampla classe de técnicas de adulterações que incluem spray, clareamento, escurecimento, desfocagem, cópia e colagem de regiões dentro da imagem. Softwares como o *Adobe Photoshop*™ e o *The Gimp* possuem uma grande variedade de ferramentas para retocar imagens. A **Figura 6** ilustra vários desses recursos.

Figura 6: Imagem original (acima) e imagem retocada (abaixo). Parte da barba foi removida e os dentes foram clareados.

V. Identificando Adulterações

Se uma imagem é suspeita, deve-se, primeiro, procurar pistas por inspeção visual e, se necessário, prosseguir com uma inspeção científica.

A primeira técnica a se considerar na identificação de adulterações é a própria percepção do Perito. A habilidade de sentir que há algo errado com a imagem, seguindo o bom senso, funciona na maioria das vezes. Se uma imagem parece ser inacreditável, então ela provavelmente não é verdadeira. Na **Figura 7**, o gato é obviamente grande demais para esta raça específica e o homem deveria estar mais curvado para segurar um animal tão pesado adequadamente.

Figura 7: O tamanho exagerado do gato sugere que há algo errado com a imagem.

Conhecimento sobre a tecnologia disponível na época em que a fotografia foi supostamente tirada pode, também, ajudar a determinar a veracidade de uma imagem. A montagem mostrada na **Figura 8**, dificilmente seria conseguida com o equipamento antigo (e pesado) disponível na época, principalmente dentro de um avião da primeira guerra mundial em pleno combate aéreo.

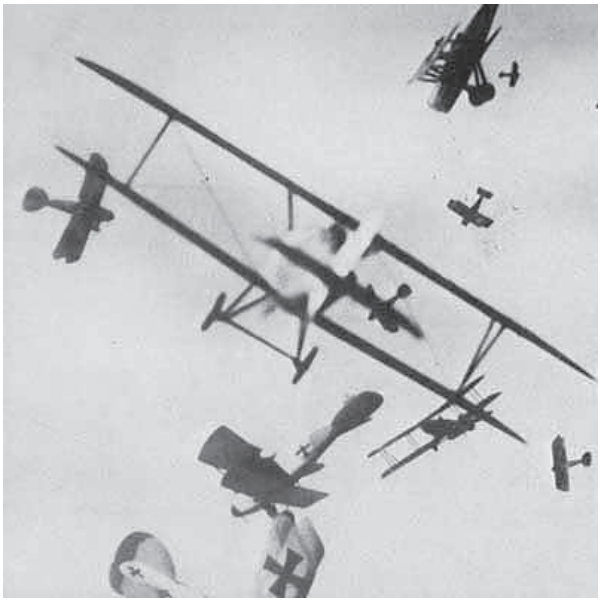

Figura 8: Cena de combate aéreo da primeira guerra mundial.

Uma adulteração realizada pela mudança de contexto é a mais difícil de detectar, pois na verdade a imagem é verdadeira, apenas o motivo da imagem é falso. A chave para se identificar uma imagem adulterada por mudança de contexto é identificar aspectos das imagens que são inconsistentes com sua descrição. Por exemplo, a data e hora do dia em que a imagem foi supostamente tirada podem ser inconsistentes com a posição do sol ou condições climáticas para aquela data.

Quando uma imagem é adulterada pela mudança de conteúdo, deve-se esperar que a parte alterada tenha inconsistências físicas que possam ser detectadas. Infelizmente, essas inconsistências nem sempre são aparentes e uma adulteração pode não ser descoberta até que a imagem original seja encontrada. A **Figura 9** ilustra uma alteração onde o rosto de uma atriz foi invertido, rotacionado e transferido para o corpo de uma outra modelo.

Figura 9: Montagem realizada por mudança de conteúdo. No detalhe, a inclinação do brinco denuncia a adulteração.

O processo de formação da imagem na câmera deve ser consistente com as leis da física de uma forma coerente em todos os pontos da imagem. Quaisquer incoerências podem ser indícios de adulteração. Os pontos a analisar são: condições de iluminação, resolução, mudança de tons, escala, gravidade, perspectiva e ruído.

Uma inconsistência comumente encontrada é a falha nas condições de iluminação. A parte alterada pode apresentar sombreamento inconsistente, indicando que foi iluminado em condições diferentes do resto da imagem (**Figura 5**). Além disso, deve-se considerar a iluminação difusa que ilumina o resto da cena. Diferenças aparecem quando um objeto fotografado com o auxílio de flash é adicionado a uma imagem com iluminação natural ou de estúdio.

Deve-se tomar cuidado ao analisar as características de iluminação de uma cena. As condições de iluminação e sombra podem levar ao erro, especialmente se aspectos referentes às três dimensões não forem considerados. A **Figura 10**, mostrando o pouso da Apollo 11 na lua, apresenta anomalias na direção das sombras, que podem ser explicadas pela topografia do terreno.

Figura 10: Imagem dos astronautas da Apollo 11 na lua. As sombras apontam para direções diferentes.

Normalmente, quem produz uma imagem adulterada ignora os recursos normalmente encontrados nas imagens reais, produzidas por uma câmera. Os efeitos mais significativos são: o realce das bordas, influenciado pela difração da lente, o foco, o desfocado causado por movimento (*motion blur*), a perspectiva e o ruído.

Quando um objeto é adicionado ou removido de uma imagem, uma borda com nível de realce inconsistente com o resto da imagem é, geralmente, criada. Esse realce é facilmente visível, de forma que é um sinal óbvio de que a imagem foi alterada, de forma que, ferramentas de desfocagem em softwares de manipulação de imagens são utilizadas para reduzir a visibilidade dessas bordas. Essa desfocagem, entretanto, vai produzir bordas borradas ao redor do objeto que serão inconsistentes com o resto da imagem.

Todos os objetos em uma imagem devem, também, estar na mesma perspectiva. Se a geometria de um objeto da imagem é inconsistente com a dos demais objetos, então ele, provavelmente, foi adicionado a partir de outra imagem. Por exemplo, em uma imagem autêntica, linhas paralelas convergem para o mesmo ponto, conhecido como ponto de fuga. Se linhas paralelas de um objeto não convergem para o mesmo ponto de fuga, então este objeto não pode ter sido fotografado pela mesma câmera que o resto da imagem. (**Figura 11**)

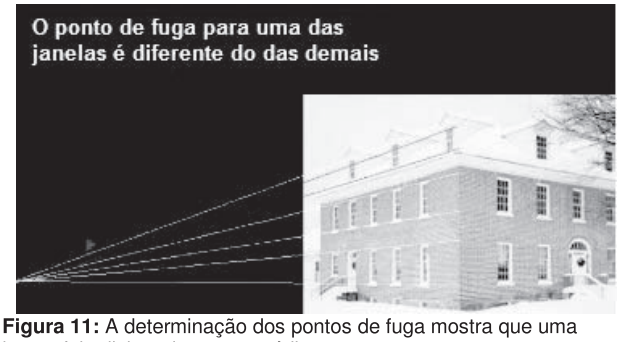

Figura 11: A determinação dos pontos de fuga mostra que uma janela foi adicionada a este prédio.

Para dar um efeito mais realista à adulteração, principalmente quando o objetivo é remover um objeto da imagem, é comum utilizar regiões da própria imagem para substituir os objetos que se quer ocultar. Em uma imagem autêntica, embora haja áreas muito parecidas, dificilmente será encontrado duas regiões exatamente iguais. A **Figura 12** ilustra esta técnica.

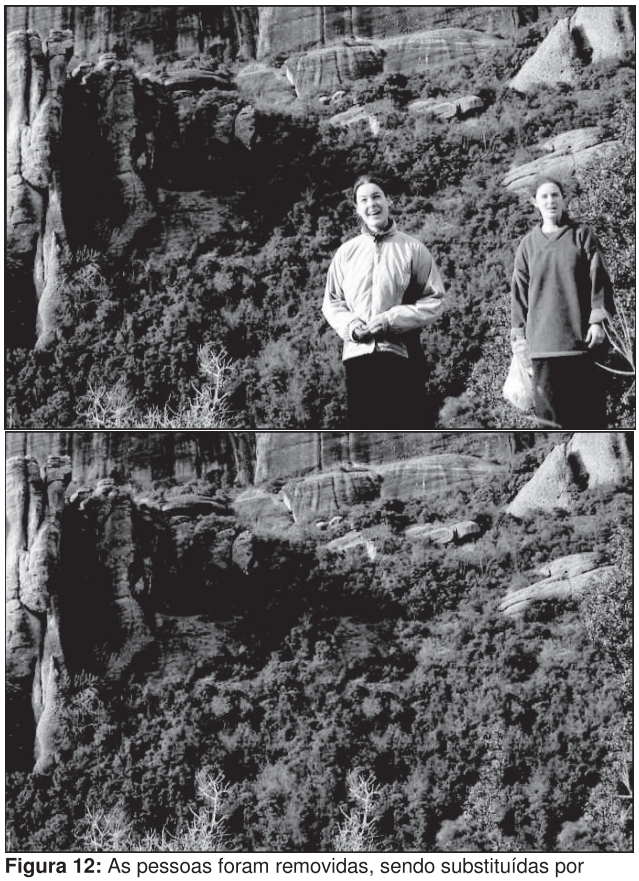

Figura 12: As pessoas foram removidas, sendo substituídas por outras regiões da própria imagem.

Infelizmente, a tarefa de dividir a imagem analisada em micro-regiões e comparar uma a uma é muito custosa para se realizar manualmente. Software especializado é necessário para viabilizar esta tarefa.

VI. Avanços Recentes

Pesquisas recentes estão desenvolvendo softwares que permitirão análises detalhadas das imagens que são impraticáveis de se realizar atualmente, mesmo com o auxílio de softwares de edição de imagens. Dentre os trabalhos de maior importância, podemos destacar:

- Farid e Popescu [4] e [5], do *Dartmouth College*, desenvolveram uma série de ferramentas, baseadas em técnicas estatísticas, capazes de detectar inserção de objetos nas imagens, alteração de cores, compressão JPEG dupla, regiões duplicadas e padrões de ruídos inconsistentes.
- Fridrich et al [8] e [9], da *State University of New York*, desenvolveram uma ferramenta que verifica se uma imagem digital foi fotografada em uma determinada câmera. Seu software baseia-se no fato de que cada câmera digital introduz um padrão de imperfeições único nas imagens capturadas. Esse padrão determina uma espécie de assinatura da câmera, que pode ser comparada com as características da imagem.

O trabalho de Farid e Popescu foi desenvolvido utilizando o software Matlab. Uma versão em Java está sendo desenvolvida neste momento e, em breve, estará disponível gratuitamente para os órgãos policiais de todo o mundo.

VII. Estudo de Caso

Em Setembro de 2006 foi enviado ao SETEC/SR/DPF/PE uma solicitação de perícia referente a uma investigação sobre falsificação de documentos com possível participação de funcionários do serviço de identificação da Secretaria de Defesa Social do Estado de Pernambuco. O material questionado consistia, dentre outros, de um arquivo em formato Microsoft Word (doc) contendo imagens de cédulas de identidade em branco. Um dos quesitos buscava determinar se as imagens haviam sido digitalizadas a partir de uma cédula de identidade já preenchida ou de uma cédula de identidade em branco. A **Figura 13** ilustra algumas das imagens encaminhadas a exame.

A análise detalhada das imagens em software especializado de manipulação de imagens (*Adobe Photoshop*™ e *IrfanView*) revelou uma série de detalhes das imagens:

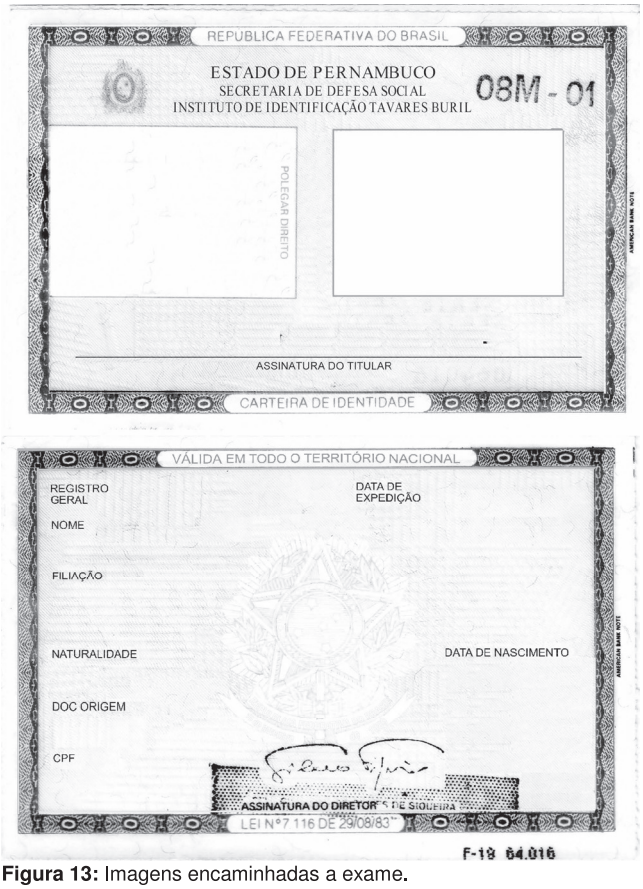

Figura 13: Imagens encaminhadas a exame.

- O padrão de fundo da imagem é consistente com o modelo de identidade utilizado pela Secretaria de Defesa Social de Pernambuco.
- Trechos contendo fibras de segurança repetidas, indicando que áreas da cédula onde estariam os dados do cidadão haviam sido sobrepostas. (**Figura 14**)

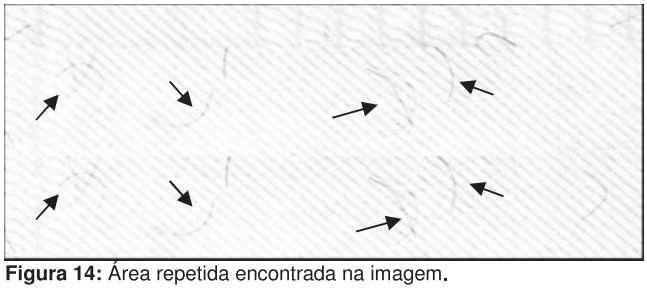

Figura 14: Área repetida encontrada na imagem.

- Textos com resolução maior que o resto da imagem, indicando que foi adicionado posteriormente. (**Figura 15**)

Figura 15: O texto à esquerda foi refeito após digitalização da imagem, por isso apresenta melhor definição que o texto à direita.

- Texto mal posicionado e erro de grafia no símbolo das armas nacionais. (**Figura 16**)

Figura 16: Texto contido no símbolo das armas nacionais foi reescrito ligeiramente fora da posição original e com um erro de grafia.

A partir desses indícios (e de outros que não foram incluídos neste trabalho), os Peritos concluíram tratar-se de uma imagem digitalizada a partir de uma cédula de identidade já preenchida.

VIII. Conclusões

Esse artigo apresenta uma série de técnicas utilizadas para a identificação de adulterações em imagens digitais. A maior parte dessas técnicas pode ser utilizada com o auxílio de software de baixo custo, facilmente acessível.

Embora as técnicas aqui descritas possam ajudar na detecção de muitas das adulterações, não há, atualmente, uma maneira de impedir que alguém, dispondo de tempo e recursos suficientes, crie uma montagem que não seja possível identificar. O que devemos esperar é que inconsistências possam ser encontradas, indicando que a imagem analisada é, de fato, uma montagem.

IX. Referências

[1] R. Fiete, “Photo Fakery”, http://oemagazine.com/fromTheMagazine/jan05/pdf/photofakery.pdf

[2] D. Brugioni, “Photo Fakery: The history and techiques of photografic deception and manipulation”, Brassey’s Inc, 1999.

[3] H. Farid. “Creating and detecting doctored and virtual images: Implications to the child pornography prevention act.”, Technical Report TR2004-518, Dartmouth College.

[4] A. Popescu e H. Farid, “Exposing digital forgeries by detecting duplicated image regions”, Technical Report TR2004-515, Dartmouth College.

[5] A. Popescu, “Statistical tools for digital image forensics”, Technical Report TR2004-531, Dartmouth College.

[6] The Museum of Hoaxes, www.museumofhoaxes.com.

[7] J. Fridrich, D. Soukal e J. Lukas, “Detection of Copy-Move Forgery in Digital Images”, Proc. of DFRWS, 2003.

[8] J. Fridrich, J. Lukas e M. Goljan, “Determining Digital Image Origin Using Sensor Imperfections”, Proc. SPIE Eletronic Imaging, 2005.

[9] J. Fridrich, J. Lukas e M. Goljan, “Digital Câmera Identification from Sensor Pattern Noise”, IEEE Transactions of Information Security and Forensics, vol. 1(2), pp. 205-214, Junho de 2006.