Avaliação de desempenho de técnica para identificação de dispositivo de aquisição baseada em PRNU com diferentes tipos de imagem de teste

Diego Marques do Carmo[1], Hermeson Barbosa da Costa[1], Ronaldo de Freitas Zampolo[1], Eurípedes Pinheiro dos Santos[2] e Adalbery Castro[3,4]

***Resumo*— Decorrente da disseminação de sistemas de aquisição, imagens digitais são cada vez mais comuns em processos criminais. Contudo, a facilidade de adulteração abre espaço para questionamentos sobre a veracidade do conteúdo apresentado e também sobre sua validade como prova em um processo. O presente trabalho aborda a identificação de dispositivo, cujo objetivo é verificar se uma imagem foi obtida ou não por uma dada câmera. Especificamente, é avaliado o desempenho de uma técnica baseada na não uniformidade da foto-reposta (do inglês *photo-response nonuniformity* – PRNU) do sensor de aquisição para imagens de teste de variadas características.**

***Palavras-Chave*— Identificação de câmera, PRNU, imagens digitais, perícia científica.**

***Abstract*— Since imaging systems are widespread, digital images are becoming increasingly common in criminal processes. However, their content veracity as well as their validity as criminal proofs are commonly questioned due to the many effortless ways of tampering and editing digital images. This work addresses the device identification issue, which aims to verify whether or not an image was obtained by a given camera. Specifically, the performance of a technique based on the sensor photo-response nonuniformity (PRNU) is evaluated for test images of different characteristics.**

***Keywords*— Camera identification, PRNU, digital images, forensics.**

I. Introdução

A popularização de máquinas fotográficas digitais, celulares e filmadoras faz com que imagens e vídeos digitais se tornem cada vez mais comuns em processos criminais. Contudo, a grande facilidade com que tais imagens e vídeos podem ser manipulados por editores cada vez mais sofisticados abre a possibilidade para que sejam feitos questionamentos em relação à validade de um dado material digital como prova em um processo. Esses dois aspectos, a popularização dos sistemas de aquisição e os questionamentos em torno da veracidade do conteúdo, vêm ocasionando um aumento no número de solicitações de perícia de material digital. Esse cenário, na maioria dos institutos de perícia científica brasileiros, contrasta com a carência de ferramentas técnicas específicas adequadas, dificultando o pronto atendimento aos casos e comprometendo a qualidade do serviço prestado. O presente trabalho aborda uma das situações de grande demanda em termos de perícia de imagens digitais: a identificação de dispositivo. Tal aplicação consiste na verificação se uma determinada imagem foi adquirida ou não por um dispositivo particular (telefone celular ou câmera digital, por exemplo). Trata-se da situação em que se deseja saber se imagens encontradas em um *pendrive* ou CD/DVD foram obtidas por uma dada câmera fotográfica que foi apreendida.

Uma das abordagens empregadas na identificação de dispositivo utiliza o que se pode chamar de "impressão digital" do sensor de aquisição. A componente mais importante dessa "impressão digital" é a não uniformidade da foto-reposta (do ingês *photo-response nonuniformity* – PRNU) [1], [2]. Decorrente do processo de fabricação dos elementos sensores, a PRNU representa a diferença na capacidade de tais elementos em converter luz em sinal elétrico. A PRNU apresenta algumas características que a tornam interessante na identificação de dispositivo: é única para cada sensor; está presente em todos fotossensores e, portanto, em qualquer imagem adquirida; é robusta a vários processos que podem inserir degradação em uma imagem, incluindo codificação com perdas, filtragem, redimensionamento e correção de gama [2]. Matematicamente, a PRNU é representada por uma matriz de mesmas dimensões do conjunto imagens usadas para estimá-la. A fim de melhor caracterizar o sensor, o processo de estimação da PRNU requer algo em torno de 30 a 50 imagens autênticas da câmera sob suspeição [2].

A técnica de identificação de dispositivo utilizada nesse trabalho é uma versão de menor complexidade computacional em relação àquela proposta em [2], pois considera que as imagens de teste não sofreram redimensionamento em relação às imagens usadas para a estimação da PRNU. As análises aqui realizadas buscam avaliar o desempenho da técnica em diferentes contextos, tais como: quando a imagem de teste é recodificada; quando a imagem de teste é rotacionada; e quando a imagem de teste foi obtida por câmera diferente da câmera sob suspeição, mas de mesma marca e modelo. O restante do texto é organizado como segue. A Seção II mostra detalhes da técnica utilizada para identificação de dispositivo. A Seção III descreve os testes realizados e analisa os resultados obtidos. E por fim, na Seção IV são apresentadas as conclusões

[1]Laboratório de Processamento de Sinais, Faculdade de Engenharia da Computação, Instituto de Tecnologia, Universidade Federal do Pará, Belém-PA, Brasil, E-mails:{diego.carmo, hermeson.costa}@itec.ufpa.br, zampolo@{ufpa.br, ieee.org}.

[2]Faculdade de Engenharia da Computação, Instituto de Tecnologia, Universidade Federal do Pará, Belém-PA, Brasil, Email: epsantos@ufpa.br.

[3]Laboratório de Sensores e Sistemas Embarcados, Programa de Pós-Graduação em Engenharia Elétrica, Instituto de Tecnologia, Universidade Federal do Pará, Belém-PA, Brasil, e [4]Centro de Perícias Científicas "Renato Chaves" (CPC-RC), Email: adalbery@ufpa.br.

Este trabalho possui apoio financeiro da PROEX/UFPA e do CPC-RC.

do trabalho.

II. Identificação de Dispositivo

Esta seção descreve a técnica utilizada neste trabalho, apresentando os elementos necessários ao entendimento da abordagem. Maiores detalhes podem ser obtidos nos trabalhos em que tal técnica foi apresentada originalmente [1], [2], [3].

O processo de identificação de dispositivo começa com a estimação da PRNU do dispositivo sob análise. Assume-se que o processo de aquisição de uma imagem é modelado por

$$\mathbf{I} = g^{\gamma}\left[\mathbf{Y} + \mathbf{Y}\mathbf{K} + \mathbf{\Omega}\right]^{\gamma} + \mathbf{Q} \tag{1}$$

onde g é o fator de ganho do sensor (diferente para cada canal cromático); $\mathbf{Y}$ corresponde à intensidade luminosa que chega ao sensor; a matriz $\mathbf{K}$ representa uma componente, de média zero, responsável pela PRNU; $\mathbf{\Omega}$ denota uma composição de diversas fontes de ruído; γ é o fator de correção de gama; e a matriz $\mathbf{Q}$ representa o ruído de quantização da codificação utilizada pelo sistema de aquisição (normalmente JPEG). Todas as operações que envolvem as matrizes na expressão (1) são do tipo elemento a elemento.

A estimativa de máxima verossimilhança da matriz $\mathbf{K}$ é dada pela expressão

$$\hat{\mathbf{K}} = \frac{\sum_{k=1}^{d} \mathbf{W}_k \mathbf{I}_k}{\sum_{k=1}^{d} \left(\mathbf{I}_k\right)^2} \tag{2}$$

onde $\hat{\mathbf{K}}$ é a estimativa de $\mathbf{K}$; $\mathbf{I}_k$ corresponde à k-ésima imagem de treinamento obtida com a câmera sob suspeição; d é o número total de imagens da câmera sob suspeição usadas na estimação de $\mathbf{K}$; e $\mathbf{W}_k$ é definido por

$$\mathbf{W}_k = \mathbf{I}_k - \hat{\mathbf{I}}_k^{(0)} \tag{3}$$

onde $\hat{\mathbf{I}}_k^{(0)} = F\left(\mathbf{I}_k\right)$ é uma versão da imagem $\mathbf{I}_k$ isenta de ruído. Detalhes sobre o filtro de eliminação de ruído empregado podem ser obtidos em [1], [4].

As imagens $\mathbf{I}_k$ utilizadas em (2), para que resultem em boas estimativas $\hat{\mathbf{K}}$, devem possuir baixa variância e valores médios de luminância elevados. Nesse sentido, recomenda-se que sejam utilizadas imagens do céu nublado ou de superfícies lisas com iluminação uniforme e controlada. Estimativas confiáveis são obtidas com o número de imagens de treinamento entre 30 e 50 $(30 \leq d \leq 50)$.

A próxima etapa compreende a avaliação da imagem de teste, que consiste primeiramente em calcular a correlação cruzada normalizada (*normalized cross-correlation* – NCC) entre a imagem de teste e $\hat{\mathbf{K}}$. A NCC [3] é dada por

$$\rho(s_1, s_2; \mathbf{u}) = \frac{\sum_{k=1}^{m}\sum_{l=1}^{n}(\mathbf{X}[k,l] - \mu_x)(\mathbf{Y}[k+s_1, l+s_2] - \mu_y)}{\|\mathbf{X} - \bar{\mathbf{X}}\| \cdot \|\mathbf{Y} - \bar{\mathbf{Y}}\|} \tag{4}$$

onde ρ denota a NCC; $\mathbf{u}$ é o vetor que caracteriza eventuais transformações da imagem de teste após a aquisição, tais como redimensionamento, rotação e codificação com perdas; m e n representam as dimensões de $\mathbf{X}$ e $\mathbf{Y}$; s_1 e s_2 definem o deslocamento entre $\mathbf{X}$ e $\mathbf{Y}$; μ_x e μ_y representam os valores esperados de $\mathbf{X}$ e $\mathbf{Y}$, respectivamente; e $\mathbf{X}$ e $\mathbf{Y}$ são definidos para o problema de identificação de dispositivo como

$$\mathbf{X} = \hat{\mathbf{K}}, \quad \mathbf{Y} = \mathbf{W}_t \tag{5}$$

onde $\mathbf{W}_t = \mathbf{I}_t - \hat{\mathbf{I}}_t^{(0)}$, sendo $\mathbf{I}_t$ a imagem de teste.

O pico de correlação de energia (do inglês *peak correlation energy* – PCE), parâmetro que caracteriza a conexão entre a imagem de teste e a estimativa da PRNU do dispositivo de aquisição sob análise, é determinado a partir do maior valor de NCC calculado. O PCE, para um certo $\mathbf{u}$, é dado pela expressão

$$PCE(\mathbf{u}) = \frac{\rho^2(\mathbf{s}_{\text{peak}}; \mathbf{u})}{\frac{1}{mn-|\Theta|}\sum_{\mathbf{s}\notin\Theta}\rho^2(\mathbf{s}; \mathbf{u})} \tag{6}$$

onde $\mathbf{s}_{\text{peak}}$ indica os valores de s_1 e s_2 para os quais a NCC $\rho(\mathbf{s}; \mathbf{u})$ é máxima; e Θ corresponde a uma região em torno de $\mathbf{s}_{\text{peak}}$.

O PCE é considerado um teste estatístico mais estável que a NCC e independe do tamanho da imagem, razões pelas quais é mais utilizado na identificação de dispositivo.

Por fim, é definido um limiar fixo τ, dependente da probabilidade de falso positivo, que servirá de valor de referência para comparação com o valor do PCE. Detalhes do cálculo de τ encontram-se em [1]. Caso o maior valor de PCE da imagem de teste, dentre os calculados considerando diferentes transformações $\mathbf{u}$, esteja acima de τ, considera-se que tal imagem foi adquirida pela máquina sob análise.

Este trabalho considera que as imagens de teste e de treinamento possuem as mesmas dimensões, o que torna as etapas de estimação e análise menos complexas do ponto de vista computacional.

III. Experimentos

Os experimentos realizados nessa seção visam testar a robustez da técnica de identificação de dispositivo em imagens obtidas por câmeras diferentes, mas de mesma marca e modelo. Este tipo de situação, em relação ao caso de imagens adquiridas por câmeras de diferentes fabricantes ou modelos, é considerado como de maior dificuldade em decorrência de se ter que diferenciar entre PRNUs de características possivelmente mais próximas. As imagens de teste também foram submetidas a diferentes processos de alteração de suas características originais, a saber: rotação seguida de recodificação JPEG, e recodificação JPEG com diferentes fatores de qualidade.

Foram usadas nos testes duas máquinas diferentes (números de série 6507300 e 6507323), mas de mesma marca (Sony) e modelo (DSC W210). A máquina de número de série 6507323 foi considerada como máquina sob suspeição, a partir da qual foi estimada a PRNU usando um conjunto de 30 imagens.

As imagens de teste foram obtidas pelas referidas câmeras com dimensões de 2952×1944, sendo usadas 50 imagens de cada câmera em cada caso testado.

A. Imagens de teste sem alteração

No primeiro teste realizado, procurou-se avaliar os resultados produzidos pela técnica quando a imagem de teste apresenta condições ideais, ou seja, não sofreu nenhuma alteração das suas características originais. A Figura 1 mostra os valores do PCE para cada imagem de teste em conjunto com o limiar calculado segundo [4]. Nota-se que uma eventual decisão baseada estritamente no limiar calculado apresentaria problemas, pois há várias imagens obtidas pela câmera diferente da suspeita, cujos PCEs estão acima do limiar. Suspeita-se que as razões para tal discrepância, ainda sob investigação, estariam nos modelos adotados no teste de hipóteses ou no procedimento estatístico utilizado para o cálculo de τ. Não obstante, verifica-se que o PCE consegue ser um bom discriminador entre imagens obtidas e não obtidas pela câmera suspeita, dada a aglutinação dos valores de PCE. Dessa forma, apesar dos limiares de decisão terem sido traçados nos gráficos de resultados dos outros casos considerados neste trabalho, tal limiar não foi adotado como elemento determinante do desempenho da técnica.

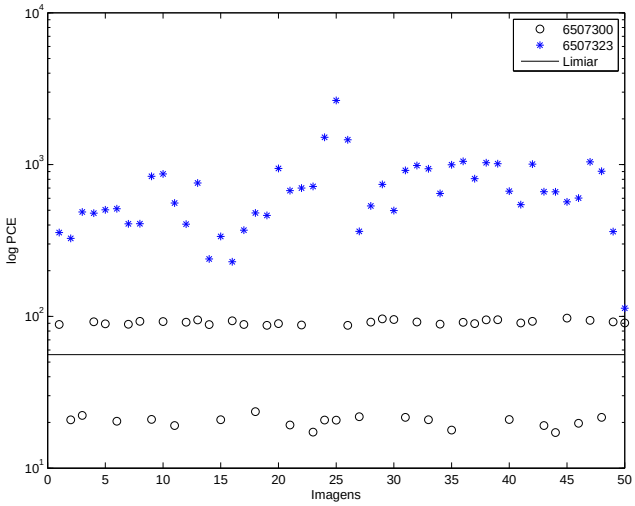


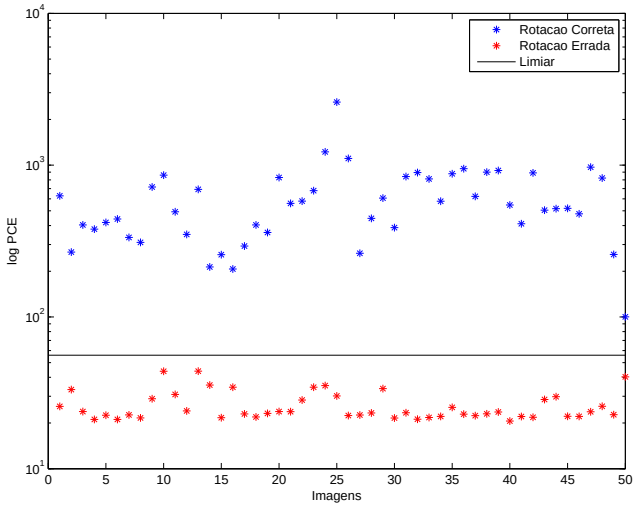
Fig. 1. Teste de identificação de dispositivo para imagens de teste sem alteração de suas características originais.

B. Rotação

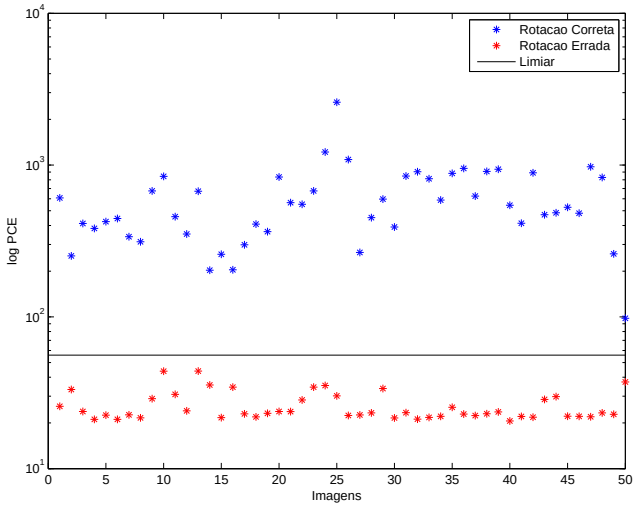
Segundo [1], uma das transformações mais comuns em uma imagem é a rotação por um ângulo de 90 graus, em sentido horário ou não, seguida de recodificação. Em termos práticos, ao se avaliar uma imagem de teste não se sabe *a priori* se foi realizada ou não uma rotação e qual o sentido de uma eventual rotação. A abordagem recomendada, assumindo eventuais rotações de $\pm$90 graus, consiste em considerar essas duas possibilidades e adotar o maior valor de PCE para determinar se imagem de teste foi obtida ou não pela câmera suspeita.

Nessa seção, é avaliado o desempenho da técnica quando as imagens de teste são modificadas mediante rotação de 90 graus seguida de recodificação JPEG (fator de qualidade 90).

Na Figura 2 (a), são apresentados os resultados obtidos quando as imagens de teste $\mathbf{I}_t$, todas adquiridas pela câmera suspeita, são rotacionadas no sentido horário e anti-horário antes do cálculo do PCE. Dessa forma, para cada imagem de teste são obtidos dois valores de PCE: um correspondente à rotação no sentido correto e outro ao errado. A Figura 2 (b) é semelhante, mas nesse caso, as rotações são aplicadas na imagem $\mathbf{W}_t$. O maior valor de PCE é usado para determinar se a imagem foi obtida ou não pela câmera sob análise. A identificação foi correta para os dois casos considerados.



(a) Imagem $\mathbf{I}_t$ rotacionada.



(b) Imagem $\mathbf{W}_t$ rotacionada.

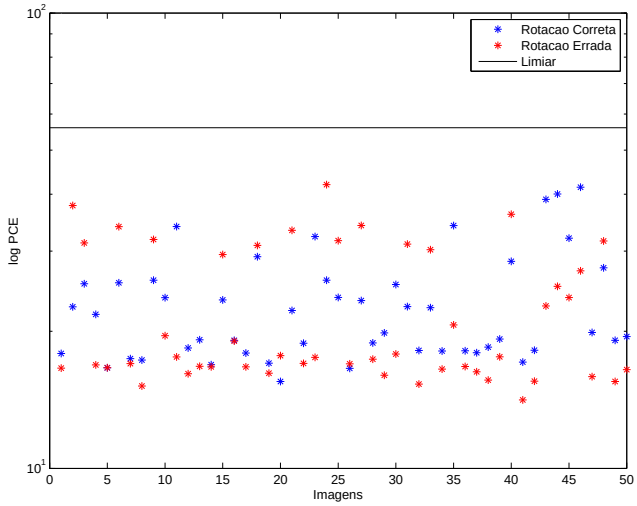
Fig. 2. Resultados para 50 imagens adquiridas pela câmera sob suspeição, rotacionadas de $\pm$ 90 graus.

A Figura 3 mostra os resultados referentes às imagens de teste não obtidas pela câmera sob análise. A rotação prévia de $\mathbf{I}_t$ mostra-se ligeiramente mais robusta que a rotação de $\mathbf{W}_t$.

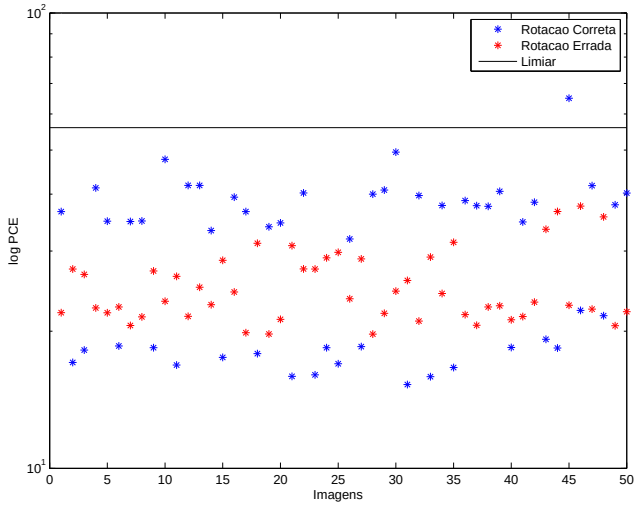
C. Recodificação JPEG

A codificação JPEG é bastante popular, sendo encontrada na maioria das câmeras digitais e câmeras de celulares. Nesta seção, avalia-se a robustez da identificação em relação ao fator de qualidade JPEG.

Nas Figuras 4 a 9 são apresentados os resultados obtidos a partir de 100 imagens de teste recodificadas usando fatores de



(a) Imagem $\mathbf{I}_t$ rotacionada.



(b) Imagem $\mathbf{W}_t$ rotacionada.

Fig. 3. Resultados para 50 imagens não adquiridas pela câmera sob suspeição, rotacionadas de $\pm$ 90 graus.

qualidade 90, 75, 60, 45, 30, e 15, respectivamente. Dentre as referidas 100 imagens de teste, 50 foram obtidas pela câmera sob análise e as 50 restantes não.

Nota-se que, em geral, a diminuição do fator de qualidade JPEG provoca uma perda na capacidade de identificação de dispositivo. Contudo, tal perda apenas faz-se intolerável somente para fatores de qualidade baixos.

IV. Conclusões

O trabalho apresentado consiste na avaliação de desempenho de uma estratégia de identificação de dispositivo baseada na estimação da PRNU de uma câmera sob suspeição. Especificamente, são utilizadas imagens de teste obtidas por duas câmeras diferentes, mas de mesma marca e modelo. Os resultados apresentados revelam que a técnica estudada é robusta tanto à rotação quanto à recodificação JPEG das imagens de teste, havendo, contudo, severo comprometimento na identificação para fatores de qualidade JPEG baixos. Foram detectados também problemas relacionados à determinação dos limiares de decisão, tal como estabelecem os autores originais da proposta. Esse aspecto ainda está sob investigação. Assim, as próximas etapas de desenvolvimento do trabalho pressupõem aprofundamento maior nas estratégias de decisão, com objetivo de identificar os problemas de cálculo de limiar de decisão para propor correções ou novas abordagens. Deve-se salientar que os resultados são parciais e fazem parte de um projeto em andamento sobre técnicas de processamento digital de sinais aplicadas na área forense. Tal projeto vem sendo desenvolvido pela Faculdade de Engenharia da Computação da Universidade Federal do Pará em conjunto com o Instituto de Perícias Científicas Renato Chaves com atuação no Estado do Pará.

Agradecimentos

Os autores agradecem à Pró-Reitoria de Extensão da Universidade Federal do Pará pelo apoio dado a esse projeto por meio do Programa Institucional de Bolsas de Extensão, e ao Centro de Perícias Científicas "Renato Chaves" pelo suporte técnico e orientação.

Referências

[1] J. Fridrich. Digital image forensics. *IEEE Signal Processing Magazine*, 26(2):16–37, March 2009.

[2] M. Goljan and J. Fridrich. Camera identification from cropped and scaled images. In *Proceedings of the SPIE Eletronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X*, pages 28–30, 2008.

[3] Miroslav Goljan, Jessica Fridrich, and Tomáš Filler. Large scale test of sensor fingerprint camera identification. In *Proc. SPIE, Electronic Imaging, Media Forensics ans Security XI,vol. 7254, San Jose, CA, January*, pages 17–21, 2009.

[4] M. K. Mihcak, I. Kozintsev, and K. Ramchandran. Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising. In *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, volume 6, pages 3253–3256, Phoenix, AZ, March 1999.

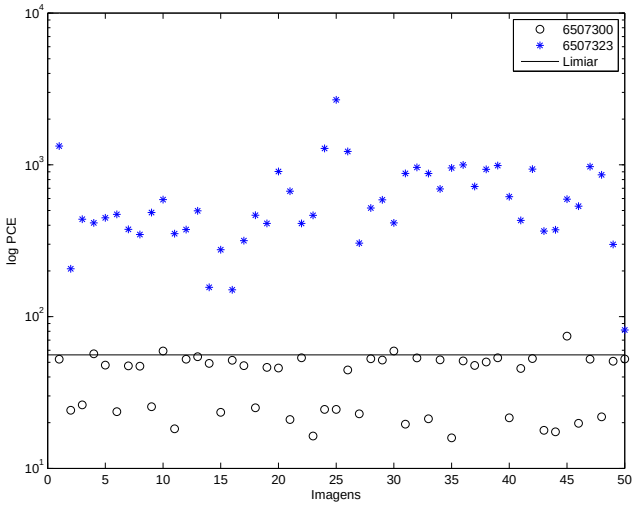


Fig. 4. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 90.

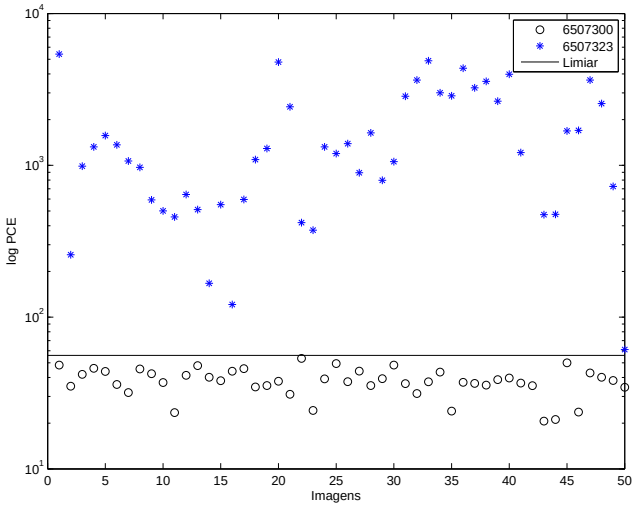


Fig. 5. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 75.

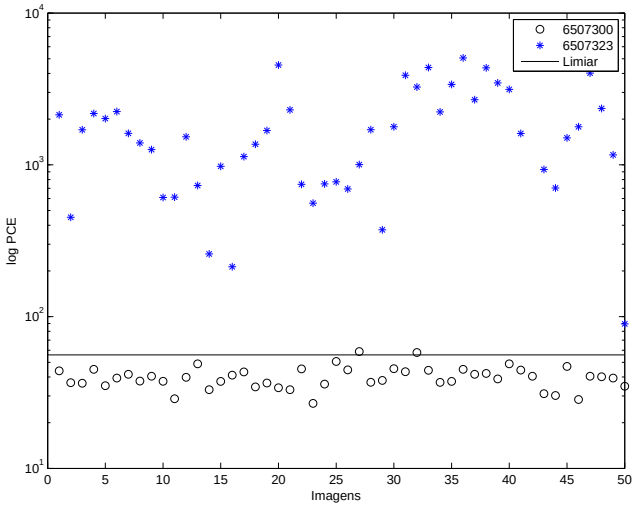


Fig. 6. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 60.

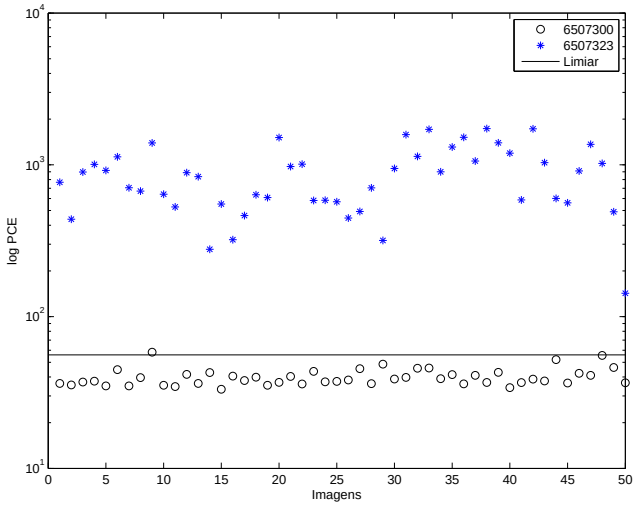


Fig. 7. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 45.

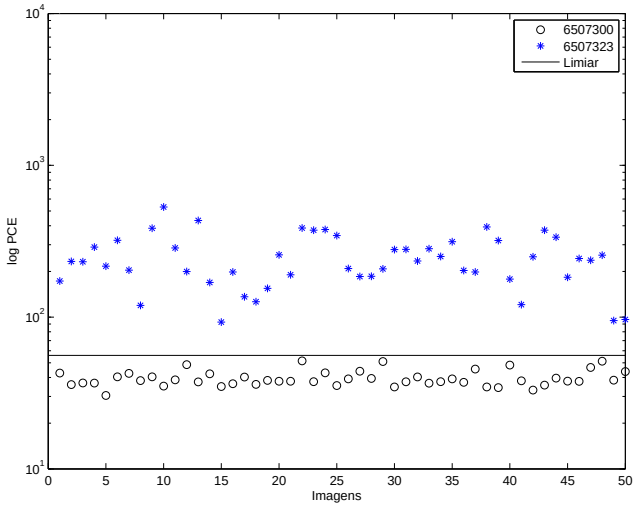


Fig. 8. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 30.

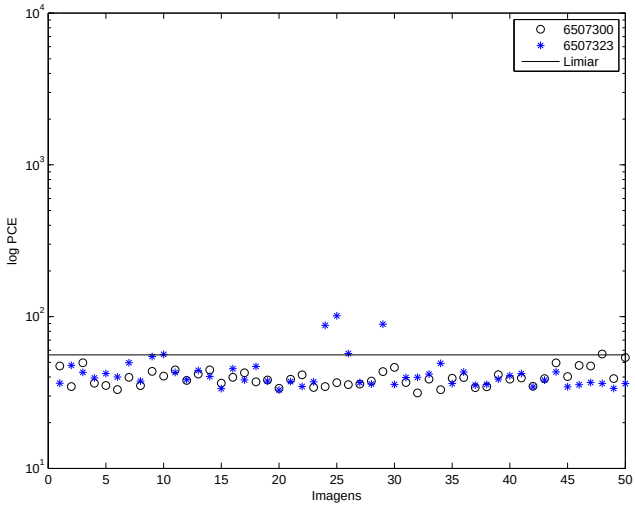


Fig. 9. Resultados obtidos para imagens recodificadas com fator de qualidade JPEG igual a 15.