

Identificação de Câmeras baseada no Ruído Padrão do Sensor usando Métodos Estatísticos

Leonardo Torres, Alisson S. Nascimento, Valter Ramos, José Alencar-Neto
Laboratório de Investigação e Perícia Digital – RASTRU
57057-780, Maceió, Brasil
Email: {ljmtorres, alisson.sa.nascimento, valter, alencar}@rastru.com.br

Abstract—Neste trabalho, propomos uma metodologia para identificação de câmeras usando o ruído padrão do sensor. Para cada câmera investigada são obtidas características de n -imagens, pela média e pela mediana do ruído residual por técnicas de filtragem, denotadas *fingerprints*. Então o ruído residual da imagem investigada é comparado com as *fingerprints* da câmera para mensurar sua correlação. Finalmente, no processo de decisão, o algoritmo utiliza métodos estatísticos e um limiar adaptativo nos resultados provenientes da correlação. Como melhores resultados obtivemos uma taxa FAR = 0% com FRR = 13.33% para o padrão estimado pela mediana usando 10-imagens.

Palavras-chave—Identificação de Câmeras, Forense, Ruído Padrão.

I. INTRODUÇÃO

Assumindo que uma imagem digital contém bem mais que somente a cena capturada, cada imagem leva consigo características inerentes a sua formação. Segundo Lukáš [1], o ruído padrão do sensor (*Sensor Pattern Noise* – SPN), formado no processo de imageamento, pode ser utilizado como uma impressão digital única para tratar diversos problemas na área forense envolvendo vídeos e imagens digitais.

As características provenientes do SPN podem provar a autenticidade e integridade de vídeos e imagens digitais, identificar dispositivo de origem e/ou validar se duas ou mais imagens podem ser correlacionadas como originadas de um mesmo dispositivo desconhecido, auxiliando a análise forense em crimes digitais.

A impressão digital do sensor, denotada *fingerprint*, pode ser estimada pela média do ruído residual de n -imagens naturais obtidas da câmera investigada, como em [1], [2].

Este trabalho tem como objetivo a identificação de câmeras baseada no ruído padrão do sensor. Inicialmente, estimamos a *fingerprint* das câmeras investigadas utilizando técnicas de filtragem para obtenção do ruído residual. Da mesma forma, obtemos o ruído residual da imagem investigada. Em seguida, definimos um limiar adaptativo para cada dispositivo com base nos atributos extraídos do ruído. Por fim, as correlações efetuadas entre a imagem investigada e as câmeras definem se pertence a algum desses dispositivos, ou não.

II. METODOLOGIA PROPOSTA

A metodologia proposta busca responder a seguinte pergunta: Dada uma imagem, pode-se provar se ela foi ou não produzida por uma certa câmera ou dispositivo digital? Nas seções subsequentes apresentaremos a metodologia adotada.

A. Ruído Padrão do Sensor

Lukáš et. al [1] descrevem que o ruído produzido no processo de aquisição pode ser dividido em duas categorias: (i) *Fixed Pattern Noise* (FPN) e (ii) *Photoresponse Nonuniformity* (PRNU).

O FPN é formada por pontos escuros, i.e., sensores que não são expostos a luz e que acabam não transmitindo informação para o *Color Filter Array* (CFA). Em imagem natural o que predomina é a PRNU, fortemente utilizada neste trabalho, que é formada pelo ruído devido a não uniformidade dos pixels (*Pixel Nonuniformity* – PNU) e pelos componentes de baixa frequência.

Os componentes de baixa frequência são causados pela luz refratada por partículas de poeira, superfícies ópticas e configurações de *zoom* durante sua aquisição [1].

B. Ruído Residual e Extração de Atributos

A supressão do ruído é um passo importante no processo de investigação e identificação de dispositivos através do SPN. Obtém-se o ruído residual, denotado w_k , por técnicas de filtragem e dado por $w_k = I_k - F(I_k)$ (vejam [1], [2] e [3]), em que I_k representa uma imagem natural e F um função de filtragem. Assim, a média do ruído residual de n -imagens, denotada η , é dada por

$$\eta = \frac{1}{n} \sum_{k=1}^n w_k, \quad (1)$$

em que n representa o número total de imagens. O filtro baseado em Wavelet 2-D foi usado no processo de filtragem [4]. São definidas *fingerprints* para cada câmera, denotadas como f_1 a obtida pela média (Equação (1)) e f_2 a obtida pela mediana.



Figure 1. Pre-processamento usado em imagem para obter o ruído residual: (a) Imagem de intensidade, (b) Imagem filtrada e (c) Ruído residual w_k .

C. Processo de Decisão

Inicialmente, definimos o conjunto de imagens que serão utilizadas para estimar a *fingerprint* e as imagens de treinamento (da mesma câmera que originou a *fingerprint*).

Em seguida, são correlacionadas as m -imagens de treinamento e as *fingerprints*, uma por vez, usando a correlação de Pearson em blocos 8×8 . A correlação de Pearson é dado por

$$\rho(X, Y) = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (2)$$

em que

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i, \quad \bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$$

são as médias dos blocos referente as imagens do ruído padrão da câmera e da imagem de treino, respectivamente.

Em posse das matrizes de correlação Z_j , $j = 1, \dots, m$ uma para cada imagem de treinamento, calculamos o coeficiente de variação s_{Z_j} , que é uma medida de dispersão definida por

$$s_{Z_j} = \frac{s_{Z_j}}{\bar{Z}_j} \quad (3)$$

em que s_{Z_j} é o desvio padrão e \bar{Z}_j a média da matriz de correlação Z_j . Assim, podemos definir um limiar adaptativo \mathcal{L}_C para identificar o dispositivo de origem, dado por

$$\mathcal{L}_C = \bar{s}_Z \pm (3 s_{s_Z}) \quad (4)$$

em que s_{s_Z} é o desvio padrão e \bar{s}_Z a média dos coeficientes de variação das Z_j , $j = 1, \dots, m$ de m -imagens de treino.

III. EXPERIMENTOS E RESULTADOS

Para validar a proposta, nós capturamos 20 imagens com resolução nativa provenientes de 3 câmeras (veja Tabela I), num total de 60 imagens. As imagens tiveram variações entre *indoor* e *outdoor*, de iluminação, de *zoom* e sem *flash*. Além disso, nenhuma imagem passou por conversão de formatos.

Table I
FABRICANTES E MODELOS DAS CÂMERAS UTILIZADOS NOS EXPERIMENTOS.

ID	Modelo da Câmera	Resolução Nativa
C_1	Samsung Galaxy Ace	2560×1920
C_2	Samsung Galaxy X	2592×1944
C_3	Motorola EX115	2046×1536

Para cada câmera foram utilizadas 10 imagens para estimar a *fingerprint*, 5 imagens para determinar o limiar \mathcal{L}_C e as 5 imagens remanescentes foram utilizadas nos testes.

Obtivemos as *fingerprints* f_1 e f_2 de cada câmera. No experimento cada *fingerprint* é correlacionada com as amostras de todas as câmeras destinadas para treinamento utilizando a Equação (2), incluindo as amostras da câmera a qual a *fingerprint* pertence.

Ao final deste processo, utilizando a Equação (3) calculamos os coeficientes de variação para cada dispositivo. A Tabela II apresenta os limiares, utilizando a Equação (4), para as câmeras envolvidas neste experimento.

Table II
LIMIARES DAS CÂMERAS ENVOLVIDAS NO EXPERIMENTO.

Câmeras	\mathcal{L}_C da f_1	\mathcal{L}_C da f_2
C_1	65.62769 ± 60.07475	32.21999 ± 25.50330
C_2	40.58637 ± 19.39327	19.82283 ± 9.619036
C_3	10.98961 ± 9.544547	12.68986 ± 11.44459

Submetemos as 15 imagens de teste para validar a metodologia proposta. Correlacionamos cada uma delas com as *fingerprint* f_1 e f_2 das três câmeras utilizando a Equação (2). Em seguida, extraímos de cada resultado o coeficiente de variação s_{Z_j} . Por fim, verificamos se cada coeficiente estava dentro do limiar \mathcal{L}_C (veja Tabela II) correspondente de cada *fingerprint* para cada modelo de câmera.

Os testes realizados com a *fingerprint* f_1 foram satisfatórios, obtiveram uma taxa de falsa aceitação FAR = 6.66%, erro associado ao padrão da câmera C_1 e uma taxa de falsa rejeição FRR = 13.33%, erro referente ao padrão da câmera C_2 .

Os testes realizados com a f_2 obtiveram melhor acurácia, com taxa de falsa aceitação FAR = 0%. Também obtivemos uma taxa de falsa rejeição FRR = 13.33%, erro associado ao padrão da câmera C_2 .

As imagens que resultaram na falsa rejeição em ambos os testes, foram capturadas com um *zoom* acentuado e, provavelmente, sua rejeição está relacionada a esta característica. Estudos mais profundos devem ser direcionados ao entendimento deste fenômeno.

IV. CONSIDERAÇÕES

Este trabalho propõe o desenvolvimento de métodos para análise forense em imagens digitais que responda à questão: Dada uma imagem, pode-se provar se ela foi ou não produzida por uma certa câmera ou dispositivo digital? A metodologia proposta foi validada utilizando o ruído padrão do sensor e duas *fingerprints* estimadas para cada dispositivo. Foi adotado um limiar adaptativo, onde para cada *fingerprint* existe um intervalo que identifica o dispositivo.

Como melhores resultados obtivemos uma taxa FAR = 0% com FRR = 13.33% para o ruído padrão estimado com a mediana de 10-imagens. Com a evolução desta metodologia espera-se utilizar um número menor de imagens para estimar o ruído padrão do sensor. Tendo em vista, que a aquisição destas imagens na área forense, em certas condições, pode ser onerosa ou não ser possível.

REFERENCES

- [1] J. Lukáš, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, Jun 2006.
- [2] X. Kang, Y. Li, Z. Qu, and J. Huang, "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 393–402, Apr 2012.
- [3] C.-T. Li, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, Jun 2010.
- [4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd ed. Nova York: Prentice Hall, 2008, ISBN: 978-0-13168-728-8.