UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

Detecção de Imagens Falsificadas Utilizando Descritores Locais

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno: José Antônio da Silva (jas4@cin.ufpe.br)
Orientador: Tsang Ing Ren (tir@cin.ufpe.br)
Área: Processamento de Imagens

03/04/2017

Contexto

Nos dias de hoje, imagens digitais tornaram-se importantes devido ao seu caráter atual como fonte principal de informação. Imagens transmitidas em jornais ou telejornais comumente são asseguradas como confiáveis [5]. Imagens digitais são um tipo importante de conteúdo, utilizado amplamente em investigações criminais, imagens médicas, jornalismo, serviços de inteligência, sistemas de vigilância, documentos financeiros, setor de transportes, publicações científicas, etc. No entanto, há uma crescente preocupação quanto à confiabilidade e autenticidade delas devido à facilidade de modificá-las e adulterá-las; isso é fruto da crescente popularidade de câmeras digitais, e a facilidade de uso e acesso a ferramentas de edição, como podemos citar o *Adobe Photoshop*®. Portanto, a capacidade de poder detectar manipulações em uma dada imagem tem sido um foco de pesquisa atual, e um domínio relevante no segmento de autenticação de imagens é o *Copy-move Forgery Detection* (CMFD) [1]: trata-se de um procedimento *pixel-based* na qual é possível constatar adulteração de uma foto onde uma região dentro de uma imagem é copiada e movida em outra seção na mesma imagem de forma a reforçar quantitativamente algum elemento de interesse. Uma outra forma de adulteração é copiar uma seção específica de uma imagem de origem, e colar este conteúdo em uma imagem de destino; este tipo de procedimento é chamado de *splicing*. Um exemplo de CMFD presente como conteúdo jornalístico pode ser visto na figura 1, presente em [11].

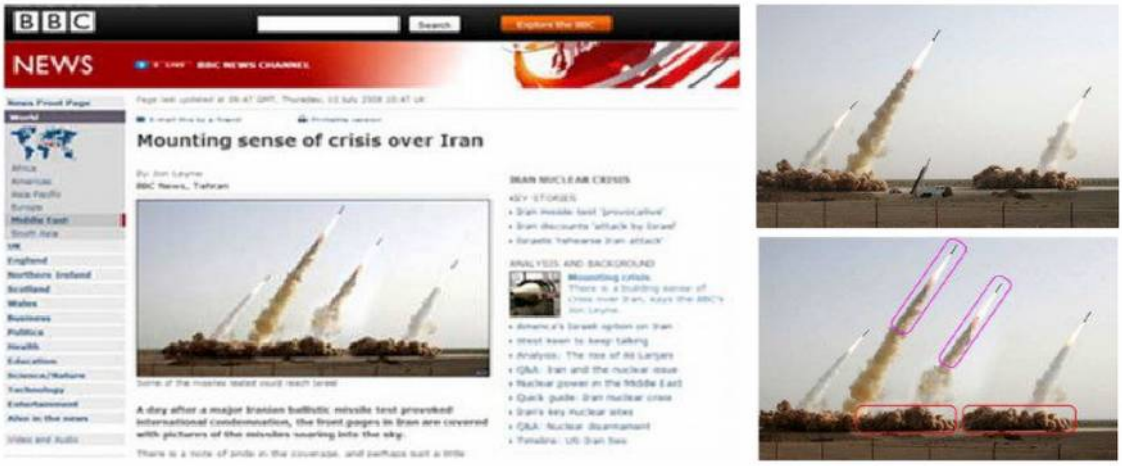

Figura 1: Exemplo de *copy-move forgery* em uma publicação jornalística, seguido do comparativo entre a imagem original e a manipulada.

Considerando o CMFD, o *workflow* usual é dividido em quatro etapas, que são: pré-processamento, extração de características, *matching* e visualização dos resultados [1]. O objetivo definido pelos pesquisadores tem sido o aumento da taxa de acerto e uma maior redução de complexidade computacional, fator ainda recorrente em parte das técnicas apresentadas. Para atacar o problema, foi focando principalmente uma melhor extração de características, como o uso de coeficientes da DCT (*Discrete Cosine Transform*) [2], *Principal Component Analysis* [3], *Scale-Invariant Feature Transform* [4], *Local Binary Patterns* [6] e *Weber Local Descriptors* [7]. Nesta última técnica mencionada, o método proposto [7] apresentou boas taxas de acurácia, comparado com outros métodos no estado-da-arte.

Proposta

A proposta principal deste trabalho de graduação é realizar, a partir do trabalho proposto em [7], uma combinação de *Weber Local Descriptors* Multi-Escala usando o *Local Binary Pattern* (LBP) como um extrator de características adicional, no intuito de aumentar a variabilidade do modelo. Primeiramente, a imagem de entrada é convertida para o espaço de cores YCbCr. Falsificadores geralmente fazem alterações no espaço de cores RGB e tentam encobrir quaisquer traços de adulteração. No entanto, o espaço de cores YCbCr armazena as informações de cores da imagem em termos de luminância (Y) e crominância (Cb e Cr). Os olhos humanos possuem uma melhor captação de luminância comparado à crominância, mas embora a imagem final pareça natural para nosso sistema visual, há traços de manipulação nos canais de crominância [8]. Em seguida, o componente de crominância (escolhe-se entre Cb ou Cr) é usado para extrair características com *Weber Local Descriptors* [9] na forma multi-escala, que nada mais é do que a geração de histogramas a partir de diferentes operações de variação (P,R) dos parâmetros do WLD, onde P é a n-vizinhança do pixel, e R é a escala espacial do operador; além destes, conjuntamente estará concatenada as *features* obtidas através do LBP. Finalmente, um classificador baseado no SVM (*Support Vector Machine*) é utilizado para classificar a imagem de entrada como autêntica ou forjada. O treinamento e teste serão executados sobre a base de imagens CASIA v1.0 [12] e v2.0 [13]. Os passos podem ser visualizados através do diagrama abaixo.

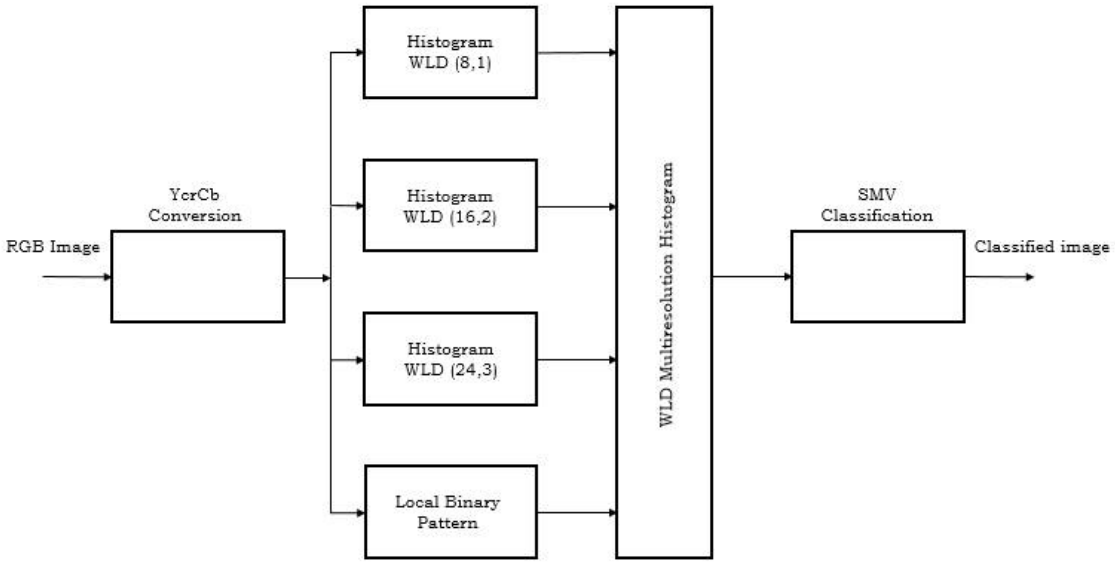

Figura 2: Diagrama em blocos do método proposto de detecção de imagens manipuladas.

Cronograma

	Período															
Atividade	Março		Abril				Maio				Junho				Julho	
Especificação do Tema	X	X														
Revisão bibliográfica	X	X														
Implementação			X	X	X	X	X	X								
Experimentos						X	X	X	X	X						
Avaliação dos resultados								X	X	X	X					
Escrita do TG									X	X	X	X	X	X		
Preparação da apresentação															X	X

Referências

[1] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, et al. “Copy-move forgery detection: Survey, challenges and future directions”. Journal of Network and Computer Applications, 75. pp. 259–278, 2016.

[2] J. Fridrich, D. Soukal, and J. Lukas. “Detection of copy move forgery in digital images”. Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 58.

[3] A. C. Popescu, and H. Farid. “Exposing digital forgeries by detecting duplicated image regions”. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[4] H. Huang, W. Guo, and Y. Zhang. “Detection of copy-move forgery in digital images using SIFT algorithm”. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, Dec. 2008, pp. 2726.

[5] Toqeer Mahmood1, Tabassam Nawaz2, Rehan Ashraf, et al. “A Survey on Block Based Copy Move Image Forgery Detection Techniques”. 2015 International Conference on Emerging Technologies (ICET), Dez 2015.

[6] Leida Li1;2, Shushang Li1, Hancheng Zhu1. "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns". Journal of Information Hiding and Multimedia Signal Processing. pp. 46-56, Volume 4, Number 1, January 2013.

[7] Sahar Q. Saleh1, Muhammad Hussain1, Ghulam Muhammad1, and George Bebis2."Evaluation of Image Forgery Detection Using Multi-scale Weber Local Descriptors". International Journal of Artificial Intelligence Tools 24(4). pp. 416-424, Ago 2015.

[8] Zhao, X., Li, J., Li, S., Wang, S. “Detecting digital image splicing in chroma spaces”. In: Kim, H.-J., Shi, Y.Q., Barni, M. (eds.) IWDW 2010. LNCS, vol. 6526, pp. 12–22. Springer, Heidelberg (2011).

[9] Chen, J., Shan, S., He, C., Zhao, G., Pietikainen, M., Chen, X., Gao, W.: WLD. “A robust local image descriptor”. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(9), 1705–1720 (2010).

[10] Hany Farid. “Image Forgery Detection – A survey”. IEEE Signal Processing Magazine pp. 16-25. Mar 2009.

[11] Bhavya Bhanu M P, Arun Kumar M N. "Copy-Move Forgery Detection Using Segmentation". 11th International Conference on Intelligent Systems and Control (ISCO), pp. 224-228, 2017.

[12] CASIA v1.0 Image Dataset, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Corel Image Database and the photographers, 2014. Disponível em:< http://forensics.idealtest.org/casiav1> Acesso em: 1 de abr. 2017.

[13] CASIA v2.0 Image Dataset, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Corel Image Database and the photographers, 2014. Disponível em:< http://forensics.idealtest.org/casiav2> Acesso em: 1 de abr. 2017.

Possíveis Avaliadores

Prof. Carlos Alexandre Barros de Mello

Assinaturas

Recife, 6 de Abril de 2017.

José Antônio da Silva

Nome

(Aluno)

TSANG DUG REN

Nome

(Orientador)