the maximum correlation value is chosen. The location giving maximum correlation value for the correct source estimates the exact scanning location. Two main issues in this extension of source camera identification methods [3-5] are increase in computational complexity in estimating the correlation between reference pattern and test noise patterns of different sizes and overheads in estimating the row reference patterns for the complete width of the scanner's bed (where file sizes can grow to more than 100MB). Use of linear scanning elements in flatbed scanners makes the whole process feasible as only row reference pattern needs to be estimated and not the estimation of the complete two dimensional reference pattern (covering scanner bed of size 8.5*11.7 square inches). This also reduces the search complexity in testing phase from O(N2) to O(N), when the image covering the complete scanner bed has O(N2) pixels. Experiments done on images scanned at 200dpi from ten different scanners show close to 90% classification accuracy for testing images scanned from different random locations of the scanner bed. Further experiments to extend this scheme for forgery detection are under progress. To detect the forged regions of a image claimed to coming from a particular scanner, first the scanning location (in horizontal direction) is determined by applying above steps and then each row of the noise pattern of the image in consideration is correlated with relevant section of the row reference pattern. The group of rows with comparatively lesser correlation (an experimental threshold can also be determined) is expected to correspond to forged region. We are also working on evaluating the robustness and accuracy of the proposed algorithm with varying scanner resolutions, JPEG compression and on images undergone filtering operations like sharpening, contrast stretching and resampling.

References:

1. (April 24, 2007) Check clearing for the 21st century act. [Online]. Available:

http://www.federalreserve.gov/paymentsystems/truncation/default.htm

2. T. Gloe, E. Franz, and A. Winkler, "Forensics for flatbed scanners," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007, p. 65051I.

3. J. Lukas, J. Fridrich, and M. Goljan, "Determining digital image origin using sensor imperfections," Proceedings of the SPIE International Conference on Image and Video Communications and Processing, A. Said and J. G. Apostolopoulos, Eds., vol. 5685, no. 1. SPIE, 2005, pp. 249-260.

4. J. Lukas, J. Fridrich, and M. Goljan, "Digital bullet scratches for images," Proceedings of the IEEE International Conference on Image Processing, 2005, pp. 65-68.

5. J. Lukas, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, San Jose, CA, January 2006

6. N. Khanna, A. K. Mikkilineni, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Scanner identification using sensor pattern noise," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007, p. 65051K.

7. Alessandro Foi, Vladimir Katkovnik, Karen Egiazarian, Jaakko Astola Proc. of the 6th IMA Int. Conf. Math. in Signal Processing, Cirencester (UK), "A novel anisotropic local polynomial estimator based on directional multiscale optimizations", Proc. of the 6th IMA Int. Conf. Math. in Signal Processing, Cirencester (UK), pp. 79-82, 2004.

8. H. Gou, A. Swaminathan, and M. Wu, "Robust scanner identification based on noise features," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, E. J. D. III and P. W. Wong, Eds., vol. 6505, no. 1. SPIE, 2007, p. 65050S.

6819-17, Session 4

Individuality evaluation for paper-based artifact metrics using transmitted light image

M. Yamakoshi, J. Tanaka, M. Furuie, M. Hirabayashi, National Printing Bureau of Japan (Japan); T. Matsumoto, Yokohama National Univ. (Japan)

Artifact-metrics is an automated method of authenticating artifacts based on a measurable intrinsic characteristic. Intrinsic characters such as microscopic random-patterns made during the manufacturing process, are very difficult to copy. Since the fiber distribution of paper is random, a transmitted light image of the distribution can be used for artifact-metrics. Little is known about the individuality of the transmitted light image, although it is an important requirement for artifact-metrics. Measuring individuality requires that the intrinsic characteristic of each artifact significantly differs, so having sufficient individuality can make an artifact-metric system highly resistant to brute force attack. Here we investigate the influence of paper category, matching size of sample, and image-resolution on the individuality of a transmitted light image of paper through a matching test. More concretely, we evaluate FMR/FNMR curves by calculating similarity scores with matches using correlation coefficients between pairs of scanner input images, and the individuality of paper by way of estimated EER with probabilistic measure through a matching method based on line segments, which can localize the influence of rotation gaps of a sample in the case of large matching size. As a result, we found that the transmitted light image of paper has a sufficient individuality.

6819-18, Session 4

Camera identification from printed images

J. Luká_, M. Goljan, J. Fridrich, Binghamton Univ.

In this paper, we study the problem of identifying digital camera sensor from a printed picture. The sensor is identified by proving the presence of its Photo-Response Non-Uniformity (PRNU) signature in the scanned picture using camera ID methods robust to cropping and scaling. Two kinds of prints are studied. The first are postcard size (4" by 6") pictures obtained from common commercial printing labs. These prints are always more or less cropped. In the proposed identification, a brute force search for the scaling factor is deployed while the position of cropping is determined from the cross-correlation surface. Detection success mostly depends on the picture content and the quality of the PRNU estimate. Full size prints on a desktop printer are the second kind of pictures investigated in this paper. They do not require any search for an unknown parameter but suffer more from non-linear geometric distortion. Removing this distortion is part of the identification procedure. From experiments, we determine the range of conditions under which reliable sensor identification is possible. The most influential factors in identifying the sensor from a printed picture are the accuracy of angular alignment when scanning, printing quality, paper quality, and size of the printed picture.

6819-19, Session 5

Toward robust watermarking of scalable video

P. Meerwald, Paris-Lodron-Univ. Salzburg (Austria)

This paper pulls together recent advances in scalable video coding and protection and investigates the impact on watermarking. After surveying the literature on the protection of scalable video via cryptographic and watermarking means, the robustness of a simple wavelet-based video watermarking scheme against combined bit stream adaptations performed on JSVM (the H.264/MPEG-4 AVC scalable video coding extension) and MC-EZBC scalable video bit streams is examined.

6819-20, Session 5

The video watermarking container: efficient real-time transaction watermarking

M. Steinebach, P. Wolf, E. Hauer, Fraunhofer-Institut für Sichere Informations-Technologie (Germany)

When transaction watermarking is used to secure sales in online shops by embedding transaction specific watermarks, the major challenge is embedding efficiency: Maximum speed by minimal workload. Video transaction watermarking presents a challenge here as video files usually larger than for example music files. Therefore online shops that want to protect their videos by transaction watermarking are faced with the problem that their servers need to work harder and longer for every sold medium in comparison to audio sales. In the past, many algorithms