Forensic Hash for Multimedia Information

Wenjun Lu, Avinash L. Varna and Min Wu
Department of Electrical and Computer Engineering,
University of Maryland, College Park, U.S.A
email: {wenjunlu, varna, minwu}@eng.umd.edu

ABSTRACT

Digital multimedia such as images and videos are prevalent on today's internet and cause significant social impact, which can be evidenced by the proliferation of social networking sites with user generated contents. Due to the ease of generating and modifying images and videos, it is critical to establish trustworthiness for online multimedia information. In this paper, we propose a new framework to perform multimedia forensics by using compact side information to reconstruct the processing history of a multimedia document. We refer to this framework as FASHION, standing for Forensic hASH for informatION assurance. As a first step in the modular design for FASHION, we propose new algorithms based on Radon transform and scale space theory to effectively estimate the parameters of geometric transforms and detect local tampering that an image may have undergone. The FASHION framework is designed to answer a much broader range of questions regarding the processing history of multimedia data than simple binary decision from robust image hashing, and also offers more efficient and accurate forensic analysis than multimedia forensic techniques that do not use any side information.

Keywords Multimedia forensics, image hashing, Radon transform, scale space theory

1. INTRODUCTION

Emerging and future communications are going much beyond dealing with one pair of sender and receiver. We have witnessed growing trends of communications involving multiple users in a distributed and heterogeneous environment such as peer-to-peer and wireless networks to deliver content-rich audio-visual data. The exact form of the multimedia data stream delivered to each user may no longer be bit-by-bit identical, as each stream becomes customized and optimized in an individual receiver for such needs as bandwidth adaptation, format conversion, and usage auditing [1]. This brings a new challenge toward establishing trustworthiness of digital multimedia, as having a conventional end-to-end hashing to provide binary integrity decision is no longer sufficient once a stream is adapted on the fly. A more complete knowledge about the entire processing history of the multimedia data is desirable to achieve better decision and usage of online multimedia information.

Recent information forensic research shows that it is possible to determine the origin and detect potential tampering for digitally acquired images/videos, even without proactive aids such as signature attachment or embedded watermark [2]. Given these new advances in non-intrusive multimedia forensics, a related and important research question is to explore whether by appending a short string as in the conventional hashing applications, we can use such additional information to augment the capabilities of both conventional hash and non-intrusive forensics to identify and estimate with high accuracy the processing history that the source data has undergone. Such capabilities of evaluating the integrity, provenance, and processing history enable us to assess the trustworthiness of data at a flexible and fine level and avoid the dilemma of one-size-fit-all designs. We refer to such a new framework for forensic research as "Forensic Hash for Information Assurance", or FASHION in short. Below we review some related literature and present the main idea and contribution of our work.

Prior work on multimedia forensics Recent research in multimedia forensics can determine whether a received image/video has undergone certain operations without knowing any information about the original data. This is accomplished by analyzing intrinsic traces left by devices and processing, and by identifying inconsistencies in signal characteristics [3]. Examples include image capturing device identification by learning color filter array (CFA) interpolation patterns [4, 5], resampling estimation by examining linear dependencies among image pixels [6], and image tampering localization by exploiting the inconsistencies of JPEG quality [7] or lighting direction [8]. These completely non-intrusive forensic analyses have limitations in terms of the accuracy levels and the scope of forensic questions that can be answered; a considerable amount of computational complexity is also involved in all-around analyses.

Prior work on robust image hashing Another related work is robust image hashing [9–11], which represents the image content by a compact hash that is robust against allowable operations but is sensitive against malicious tampering. Robust image hashing is an effective technique for image authentication, but a simple binary decision of authenticity is inadequate for the purpose of multimedia forensics. It is desirable to provide a complete processing history of the multimedia data, so that the end users will have the flexibility in decision making on whether to trust and how to use the received document for specific applications. Some recent work on image hashing can provide certain forensic capabilities. Roy and Sun [12] incorporate SIFT features [13] into the hash for geometric registration of the received image to the original and enable tampering localization. Lin et al. [14] use distributed source coding to encode information about the original image and use EM algorithm to estimate potential operations on the image. However, the use of SIFT feature in [12] results in considerable increase in the hash length and registration is not possible when the transmitted SIFT points are not available in the received image, while the EM algorithm used in [14] is computationally intensive.

Main idea and contribution of our work In this paper, we propose to extract properly selected information from an image into a compact representation, called forensic hash. The forensic hash is designed to be modular and contains various components to answer different forensic questions in a compact, efficient, and accurate manner. The forensic capability of the FASHION framework can be easily extended by adding new components. Given that geometric transform estimation is necessary to answer further forensic questions such as tampering localization, but is usually difficult and involves high computational cost in blind forensic analysis, we propose in this paper an alignment component for FASHION. We extract side information based on the Radon transform of the image and then perform estimation of rotation angle, scaling factor, and cropping amount with the help of scale space theory [15]. After geometric registration, one implementation of integrity check component is presented to localize image tampering using compact block-based information. The main contributions of our work include: (1) a modular and extensible framework for information assurance and multimedia forensics research; (2) novel construction of compact and scalable hash representation with efficient algorithm for geometric transform estimation, which can be extremely difficult without knowing the original image. Compared with the robust hashing work [12], our work achieves the registration using much shorter hash length and the result is more robust to content changes. We believe the proposed work can have applications in ensuring trustworthiness for digital multimedia data distributed online.

2. MULTIMEDIA FORENSICS USING COMPACT SIDE INFORMATION

The objective of the proposed FASHION framework is to achieve efficient and accurate multimedia forensics by properly designing forensic hashes that capture important side information about the original image. A forensic hash is a compact and modular representation of the original image to facilitate later forensic analysis. Unlike traditional robust image hashing, forensic hashes from similar images do not have to be similar in terms of smaller distance between the two hashes. Instead, delicate yet efficient algorithms are designed to analyze a forensic hash and a given image to identify potential operations that the image may have undergone and estimate the parameters of such operations. Desirable properties for forensic hash include robustness, scalability, and security. Robustness means that the forensic hash can provide accurate analysis for images that have undergone multiple operations and strong tampering; scalability ensures that the performance of forensic analysis can be improved as we include more side information; security guarantees that malicious tampering cannot evade detection. In this section, we present our algorithm for the alignment component of forensic hash for estimating geometric transforms, such as rotation and scaling. Once the image under question has been aligned with the original image, an integrity check component is devised to detect and localize any tampering by using block-based features. The forensic hash is designed to be as compact as possible and the forensic analysis has low computational complexity, which makes it possible to be used in band-limited channels and on small devices such as mobile phones.

2.1 Geometric Transform Estimation

Geometric transforms such as rotation and scaling are common post-processing operations and the estimation of transform parameters are important in order to compare the original and testing images on a common ground. Prior work [12, 14] on image hashing either result in considerable hash length to incorporate the geometric registration information or require high computational cost to estimate the transform parameters. In this section, we describe our compact forensic hash for efficient rotation and scaling estimation.

Rotation Estimation The direction of image edges can be used to capture the information about image orientation. For an original image $I(x, y)$, we first compute its edge map $E(x.y)$ using Canny edge detector [16]. Radon transform is then applied on the edge map $E(x, y)$. Radon transform of an image is essentially a line integral of that image along certain directions, defined as follows:

$$R_E(\rho, \theta) = \int_{-\infty}^{\infty} E(\rho \cos\theta - u \sin\theta, \rho \sin\theta + u \cos\theta) du. \tag{1}$$

Given another image I' which is obtained by rotating image I by α degrees counter-clockwise, its edge map E' would give a Radon transform $R_{E'}(\rho, \theta) = R_E(\rho, \theta + \alpha)$. Thus, in the Radon transform domain, rotation becomes a shift along the angle axis. This property of Radon transform has been exploited in the image registration [17] and authentication [18] literature, where a 1-D summarization of the Radon transform along the angle axis is used to estimate the rotation angle by cross-correlation. For the Radon transforms $R_E(\rho, \theta)$ and $R_{E'}(\rho, \theta)$, the 1-D summarization is derived as $\mathbf{m}(\theta) = \max_\rho(R_E(\rho, \theta))$, and $\mathbf{m}'(\theta) = \max_\rho(R_{E'}(\rho, \theta))$. In order to compactly represent the 1-D summarization about the original image, quantization and subsampling will be applied to $\mathbf{m}(\theta)$. Since downsampling will cause aliasing, we first pass the signal $\mathbf{m}(\theta)$ through a low-pass filter $f(\cdot)$ to obtain $\hat{\mathbf{m}}(\theta) = f(\mathbf{m}(\theta))$. If an n-byte hash is desired, we downsample the signal $\hat{\mathbf{m}}(\theta)$ to obtain the forensic hash $\mathbf{h} = \{h(1), \cdots, h(n)\}$ with $h(i) = \hat{m}(\lfloor (i-1) \cdot \frac{180}{n} \rfloor)$, $i = 1, 2, \cdots, n$.

Given a testing image I', the Radon transform of its edge map $R_{E'}(\rho, \theta)$ and the 1-D summarization $\mathbf{m}'(\theta) = \max_\rho(R_{E'}(\rho, \theta))$ will be generated. In order to compare with the forensic hash $\mathbf{h}$, the signal $\mathbf{m}'(\theta)$ will be passed through the low-pass filter and downsampled at different shift positions to obtain $\mathbf{h}'(\phi) = \{h'(1), \cdots, h'(n)\}$ with $h'(i) = \hat{m'}(\lfloor (i-1) \cdot \frac{180}{n} \rfloor + \phi)$, $\phi = 0, 1, \cdots, 179$. The shift amount which maximizes the cross-correlation between the two vectors $\mathbf{h}$ and $\mathbf{h}'(\phi)$ is then considered as the rotation angle between the two images I and I', i.e.

$$\alpha = \arg\max_{\phi} \sum_{i=1}^{n} h(i) h'(i + \phi), \ \phi \in \{0, 1, \cdots, 179\}. \tag{2}$$

To further compress the forensic hash, we can store only the rank order information of $\mathbf{h}$, i.e. $\text{rank}(\mathbf{h}) = \{r(1), \cdots, r(n)\}$ where $r(i) \in \{1, \cdots, n\}$ is the rank of $h(i)$. Given $\mathbf{h}'(\phi)$ of the testing image, its rank order information is denoted by $\text{rank}(\mathbf{h}'(\phi)) = \{r'(1), \cdots, r'(n)\}$. The shift amount which minimizes the L_1 distance between $\text{rank}(\mathbf{h})$ and $\text{rank}(\mathbf{h}'(\phi))$ will be the estimated rotation angle between the two images I and I', i.e.

$$\alpha = \arg\min_{\phi} \sum_{i=1}^{n} |r(i) - r'(i + \phi)|, \ \phi \in \{0, 1, \cdots, 179\}. \tag{3}$$

Experimental results show that rotation estimation using ranking information gives comparable performance to estimation using cross-correlation, which will be shown in Section 3.

Scaling Estimation Given original image I and its scaled version I' with scaling factor s, their Radon transforms have the property that the Radon projections at any particular angle θ, $f(\rho) = R_I(\rho, \theta)$ and $f'(\rho) = R_{I'}(\rho, \theta)$, have the same scaling factor s, i.e. $f(\rho) = s \cdot f'(s \cdot \rho)$. However, this scaling relation may not be exactly satisfied when the image has undergone additional cropping, local tampering, and other image processing operations such as filtering and contrast enhancement. The forensic hash should be able to reliably estimate the scaling factor even in such cases.

We propose to use scale space features of the 1-D signals $f(\rho)$ and $f'(\rho)$ to address this problem. Scale space theory [15] is a technique for analyzing signals at different scales, which makes it useful for automatic scale selection and scale invariant image analysis. Given $f(\rho)$ of the original image, we first generate its scale space representation $L(\rho;t)$ by convolving f with a 1-D discrete Gaussian filter to obtain

$$L(\rho;t) = g(\rho;t) * f(\rho), \text{ where } g(\rho;t) = \frac{1}{\sqrt{2\pi t}} e^{-\rho^2/(2t)}. \tag{4}$$

The scale space representation is a 2-dimensional signal with higher value of t indicating coarser scale.

With $L(\rho;t)$ computed, we then locate the space extrema of $L(\rho;t)$ at each scale t by detecting the zero-crossing positions of $\partial L(\rho;t)/\partial t$ for each t. For the 1-D signal f shown in Fig. 2, its local extrema across scales are illustrated in Fig. 1, where horizontal direction represents the signal and the vertical direction represents the scale. Extrema positions are marked black and from top to bottom the scale becomes coarser. The property of smoothing using Gaussian kernel is that no new extrema will be created in coarser scales, which means that the number of extrema will be fewer in the coarser scale and their evolution over scales will never cross each other.

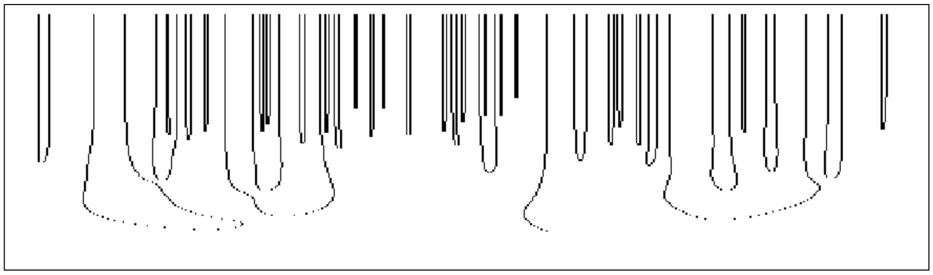

Figure 1: Space extrema across scales: horizontal direction represents the signal and the vertical direction represents the scale, with fine scale at the top

We can see from Fig. 1 that smoothing can cause the extrema to drift at coarse scales, therefore we trace the extrema from the coarse scale to the finest scale and use its position at the finest scale to accurately locate each extremum. During tracing, we also compute the lifetime of a space extremum, denoted as $\log(t_D)$, where t_D is the scale at which the extrema disappears. The use of logarithm is to make sure signals at different scales are treated in a similar way [15]. Extrema with longer lifetime are expected to capture more important information about the signal and are more robust against local variations of the signal. The 10 extrema of f with longest lifetime are shown in Fig. 2, which roughly captures the most stable extrema while ignoring small variations in the signal.

After computing $f(\rho)$ from the original image, the forensic hash for scaling estimation is generated by recording the positions of the n extrema of f with the longest lifetime across scales, where n can be determined by the desired hash length. Since the extrema with long lifetime are expected to be stable after scaling even with cropping and local tampering, we use their positions to estimate the scaling factor s. Given the extrema positions of the two signals $f(\rho)$ and $f'(\rho) = s \cdot f(s \cdot \rho)$, we iteratively choose two extrema from both $f(\rho)$ and $f'(\rho)$, respectively. An estimate of the scaling factor can be obtained by the ratio of the distance between extrema in $f'(\rho)$ to the distance between extrema in $f(\rho)$. We then scale the testing signal $f'(\rho)$ and align it to the original extrema from $f(\rho)$, following which the number of matched extrema between the two signals is recorded. After exhaustively comparing every two extrema from $f(\rho)$ to every two extrema from $f'(\rho)$, the scaling factor that gives the maximum number of matched extrema between the original signal and testing signal will be the

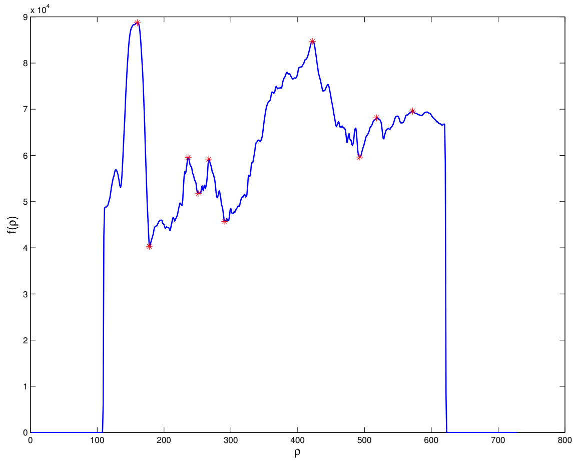

Figure 2: The 10 most stable extrema of $f(\rho)$

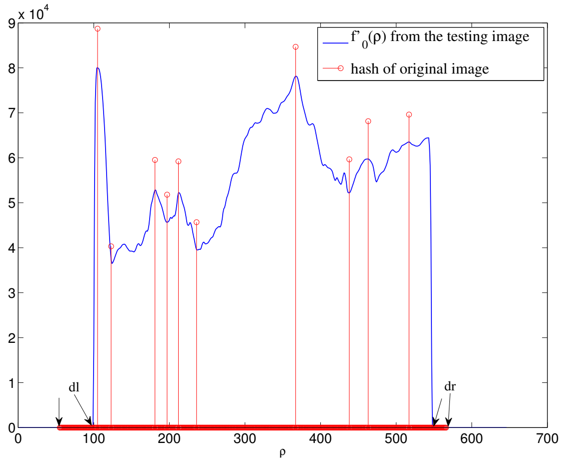

Figure 3: Cropping estimation by aligning extrema from original and testing signals

estimated scaling factor s. By computing the Radon projections of the original image along both the vertical and horizontal directions, we obtain two signals $f_0(\rho)$ and $f_1(\rho)$, respectively, and these two signals can be used to estimate the scaling factor of the testing image along those two directions.

2.2 Detecting and Locating Changes Made to An Image

Once the parameters of geometric transform are estimated, we can compare the testing image with the original image on a common ground. In this section, we describe how the above proposed alignment component of the forensic hash can enable image cropping detection and tampering localization.

Cropping Estimation Cropping can be used by an attacker to remove important information on the boundary of an image and render most image hashing schemes useless as they are typically sensitive to misalignment. We can use the forensic hash containing stable extrema proposed above to estimate the amount of cropping. Cropping on the left and right boundary of the image causes the same amount of cropping on the boundaries of the signal $f_0(\rho)$. Similarly, cropping on the top and bottom boundary causes the same amount of cropping on the boundaries of the signal $f_1(\rho)$.

Given a testing image I', we compute its Radon projections along the vertical and horizontal directions to obtain $f'_0(\rho)$ and $f'_1(\rho)$. The positions of the most stable extrema of $f'_0(\rho)$ and $f'_1(\rho)$ are also computed. After moderate amount of cropping, majority of the extrema in $f_0(\rho)$ and $f_1(\rho)$ are still available in $f'_0(\rho)$ and $f'_1(\rho)$. We can align the original extrema with the extrema from f'_0 and f'_1 such that the number of matched extrema is maximized, as described in Section 2.1. An example of the alignment is shown in Fig. 3. Once the two signals are properly aligned, the amount of cropping can be obtained by comparing the distance between the boundaries of the two signals. In Fig. 3, dl and dr are the estimated amount of cropping on the left and right boundaries of the original image. It should be noted that the accuracy of cropping estimation depends on the accuracy of scaling estimation, since the testing signal needs to be scaled before alignment. With an accurate scaling estimation, cropping estimation errors are typically within 1 or 2 pixels.

Tampering Localization Besides cropping, an adversary can modify local regions of an image and alter its original content by operations such as cut and paste. An effective methods to detect such local tampering is to represent the original image using block-based features and compare block-wise differences between the original and testing image. For this approach to work well, the two images need to be properly aligned before block comparison. Compared with tampering localization based on inconsistencies in image statistics, as used in blind multimedia forensics, block-wise comparison can achieve more efficient and more accurate tampering localization. The alignment component that we arrive at offers accurate geometric registration and therefore provides the necessary common ground to enable accurate block-based tampering localization.

Since a tampered part of an image usually has significant difference from the original in terms of their gradient information, features such as edge direction histogram have been used for tampering localization with good results [12]. Edge direction histogram and quantization of pixel gradient into a few directions provide good robustness against small rotation and scaling effect. In this paper, we quantize pixel orientation into four directions (horizontal, vertical, diagonal, and anti-diagonal) and compute the edge direction histogram for each block. These edge direction histograms form the integrity check component of the forensic hash. We examine the effectiveness of block-based edge histograms for tampering localization and show that non-uniform quantization of the histogram can provide enhanced performance over uniform quantization, which will be demonstrated in the next Section.

3. EXPERIMENTAL RESULTS

To examine the effectiveness of the proposed forensic hash, we collect 200 images from Flickr with 40 different tags, such as beach, building, flower, car, panda, etc. The size of each image is about 500x300. In order to evaluate the effectiveness and robustness of the proposed forensic hash, we perform over 20 operations for each of the 200 images, which gives us a database of over 4000 images. The operations are listed in Table 1. For the local tampering operation, we randomly select and swap two blocks within the image, where the block sizes are 50x50 and 100x100. After swapping, proper blending is introduced to avoid the sharp transition at the boundary of the tampered regions. For each of the 200 original images, we generate forensic hash capturing geometric and block-based features, and then evaluate the forensic analysis performance over the 4000 modified images.

Table 1 Image operations and their parameters

Operations	Operation parameters
Rotation	3, 5, 10, 30, 45 degrees
Scaling	scaling factor = 0.3, 0.5, 0.7, 0.9, 1.2, 1.5
Cropping	19%, 28%, 36% of entire image
Local tampering	block size 50x50, 100x100
JPEG compression	Q=10
Various combinations of rotation, scaling, cropping, and local tampering	

Rotation estimation results The rotation estimation accuracy for different hash length is given in Fig. 4. It can be observed from the figure that applying low-pass filter before downsampling the 1-D summarization of the Radon transform greatly improves the estimation accuracy. By further combining the estimation results from using normalized cross-correlation and ordinal ranking information, the proposed forensic hash can achieve rotation estimation error of about 3 degrees with a hash length of about 10 to 15 bytes. The estimation is also robust for images that have undergone multiple operations, such as combinations of rotation, scaling, cropping, and local tampering.

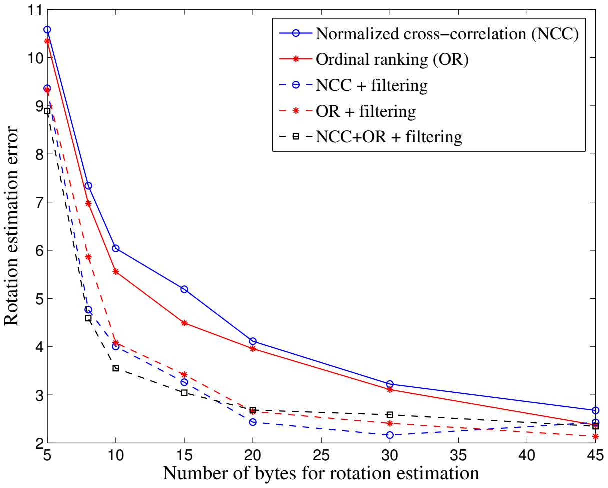

Figure 4: Rotation estimation accuracy

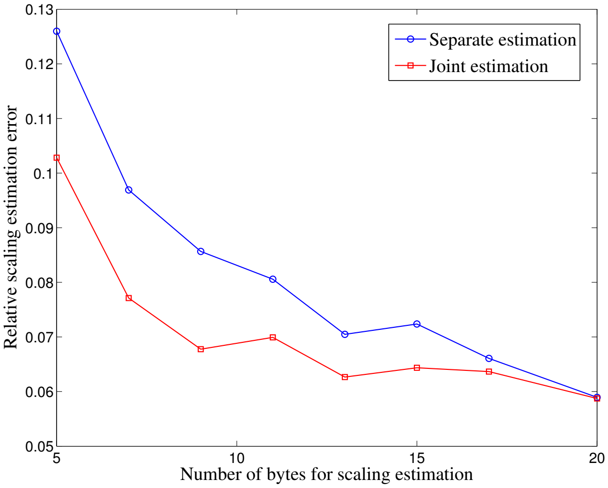

Figure 5: Scaling estimation accuracy

Scaling estimation results To estimate the scaling factor of a testing image, we perform Radon projection of the image along vertical and horizontal directions. Scale space extrema of the two projected signals are then encoded into the forensic hash to estimate the scaling factor along the two directions. The relative estimation error for scaling factor is shown as the blue curve with circle markers in Fig. 5, where lower than 10% relative error can be achieved when encoding only 10 extrema. Since scaling operation is usually done isotropically, we can use this prior knowledge to select the scaling factor estimation that has higher confidence between the two directions. This joint estimation result is shown as the red curve with square markers in Fig. 5, where around 7% relative error can be achieved using only 10 extrema or 10 bytes along each of the horizontal and vertical projection directions. It should be noted that majority of the errors are contributed by testing images whose estimated rotation angles are slightly different from the actual values. For images whose rotation estimation is accurate, the scaling estimation error is typically below 1%.

Tampering localization results For tampering localization, the choice of block size controls the trade-off between hash length and detection performance. Larger block size gives a smaller hash length but can introduce higher false detection than a smaller block size. For compact representation, the edge direction histogram in each block will be quantized. In Fig. 6, we compare tampering localization performance using uniform quantization and Lloyds quantization. The ROC curves are obtained by quantizing each component of the edge direction histogram to 4 bits using uniform quantization and Lloyds quantization, respectively. It can be observed that by slightly increasing the hash length to encode the quantization codebook, Lloyd quantization significantly improves tampering localization performance compared to using uniform quantization. We can use 1 byte per block with Lloyd quantization to achieve similar performance as compared to using 2 bytes per block with uniform quantization. An example of a tampered image and its tampering localization is shown in Fig. 7 and Fig. 8.

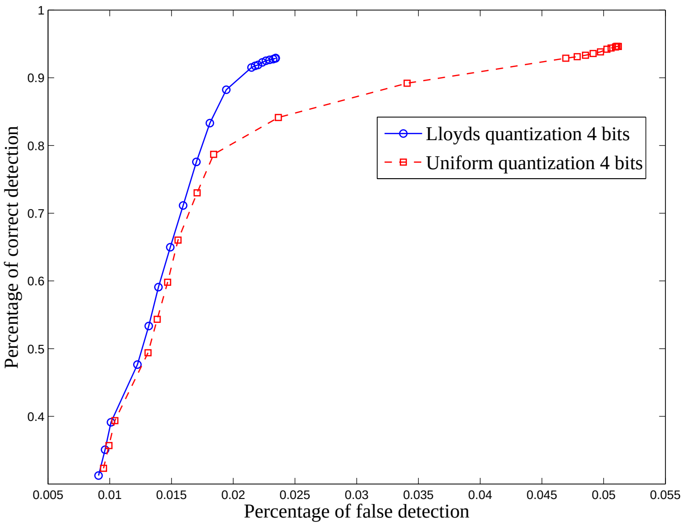

Figure 6: Tampering localization performance

For image authentication applications, after the testing image has been properly aligned with the original image based on the geometric transform parameters estimated using the forensic hash, block-based features can be used to authenticate the testing image. Due to the use of edge direction histograms, the probability that two different images yield similar histograms over most of the blocks is expected to be low. Very good authentication performance can therefore be achieved by setting a proper threshold on the percentage of matched blocks between the testing and the original images.

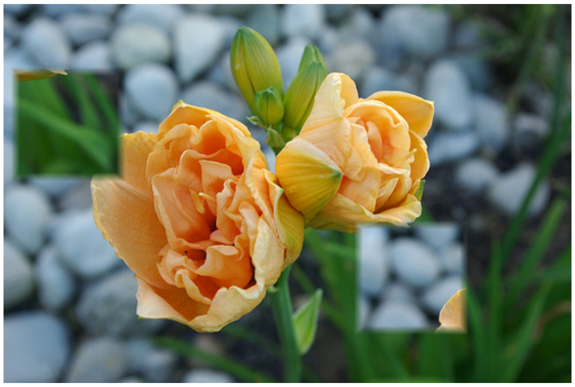

Figure 7: Tampered image

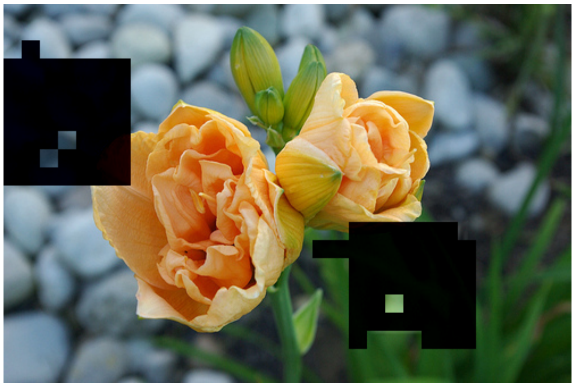

Figure 8: Tampering localization result

4. CONCLUSIONS

In this paper, we proposed a new framework called FASHION for multimedia forensics. Based on Radon transform and scale space theory, an alignment component of the forensic hash is designed to be as compact as traditional image hashing and can answer a broader range of forensic questions regarding the processing history of the image data. With 30-40 bytes, the forensic hash can provide accurate estimates of the parameters of geometric transforms that the image has undergone, providing the necessary registration for further forensic analysis such as tampering localization. Experiments show that the proposed forensic hash is robust against images that have undergone multiple operations. The main contribution of this work is the introduction of the new research framework on using compact side information for multimedia forensics. As future work, we plan to design new forensic hash components for other common image editing and malicious tampering operations, so that we can gain a more complete understanding on the processing history of an image and better evaluate its trustworthiness.

REFERENCES

[1] C.W. Chen, W. Zeng, and R. Steinmetz (eds), “Special Issue on Recent Advances in Distributed Multimedia Communications,” *Proc. of IEEE*, vol. 96, no. 1, January 2008.

[2] E. Delp; N. Memon; M. Wu (eds), “Special Issue on Forensics Analysis of Digital Evidence,” *IEEE Signal Processing Magazine*, vol. 26, no. 2, March 2009.

[3] H. T. Sencar and N. Memon, “Overview of State-of-the-art in Digital Image Forensics,” *World Scientific Press*, 2008

[4] S. Bayram, H. T. Sencar and N. Memon, “Source Camera Identification Based on CFA Interpolation,” *Proc. of IEEE Int. Conf. on Image Processing*, 2005.

[5] A. Swaminathan, M.Wu and K. J. Ray Liu, “Non-Intrusive Component Forensics of Visual Sensors Using Output Images,” *IEEE Trans. of Information Forensics and Security*, vol. 2, no. 1, pp. 91-106, March 2007.

[6] A. C. Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Traces of Re-Sampling,” *IEEE Trans. Signal Processing*, vol. 53, no. 2. pp. 758-767, 2005.

[7] H. Farid, “Exposing Digital Forgeries From JPEG Ghosts,” *IEEE Trans. Information Forensics and Security*, vol. 4, pp. 154-160, 2009.

[8] M. K. Johnson and H. Farid, “Exposing Digital Forgeries by Detecting Inconsistencies in Lighting”, *Proc. of ACM Multimedia Security Workshop*, 2005.

[9] R. Venkatesan, S. M. Koon, M. H. Jakubowski and P. Moulin, “Robust Image Hashing,” *Proc. of IEEE Int. Conf. on Image Processing*, vol. 3, pp. 664-666, 2000.

[10] J. Fridrich and M. Goljan, “Robust Hash Functions for Digital Watermarking,” *IEEE Proc. International Conference on Information Technology: Coding and Computing*, pp. 178-183, March 2000.

[11] A. Swaminathan, Y. Mao, and M. Wu, “Robust and Secure Image Hashing”, *IEEE Trans. on Information Forensics and Security*, vol. 1, no. 2, pp. 215-230, June 2006.

[12] S. Roy and Q. Sun, “Robust Hash for Detecting and Localizing Image Tampering,” *Proc. of IEEE Int. Conf. on Image Processing*, vol. 6, pp. 117-120, 2007.

[13] D. Lowe, “Distinctive Image Features from Scale-Invariant Keypoints,” *Int. J. Computer. Vision*, vol. 60, pp. 91-110, 2004.

[14] Y.-C. Lin, D. Varodayan, and B. Girod, “Distributed Source Coding Authentication of Images with Affine Warping,” *Proc. of IEEE Int. Conf. on Acoustic, Speech, and Signal Processing (ICASSP)*, 2009.

[15] T. Lindeberg, “Scale-Space Theory in Computer Vision,” *Kluwer Academic Publishers*, 1994.

[16] J. Canny, “A Computational Approach To Edge Detection,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 8, pp. 679-714, 1986.

[17] D. Wangrattanapranee and A. Nishihara, “Rigid Image Registration by using Corner and Edge Contents with Application to Super-Resolution,” *Proc. of the 2008 Digital Image Computing*, 2008.

[18] L. Frédéric and M. Benoit, “RASH: RAdon Soft Hash algorithm,” *European Signal Processing Conference (EUSIPCO)*, 2002.