

Content Based Image Authentication by Feature Point Clustering and Matching

Lei Yang

Department of Electrical and
Computer Engineering
University of Florida
Gainesville, Florida, 32611
Email: leiyang@ufl.edu

Jun Tian

Futurewei Technologies Inc.
400 Crossing Blvd, 2nd FL
Bridgewater, NJ, 08807
Email: jtian@huawei.com

Dapeng Wu

University of Florida
Gainesville, Florida, 32611
Telephone: (352) 392-4954
Fax: (352) 392-0044
Email: wu@ece.ufl.edu

Abstract

Digital multimedia makes fabricating and copying much easier than ever before. Therefore, it demands efficient and automatic techniques to identify and verify the content of digital multimedia. Image authentication is such a technique to automatically identify whether the query image is a fabrication or a simple copy of the original one. In this paper, we propose a perceptual image authentication technique based on clustering and matching of feature points of images. Feature points are first extracted from images with the k -largest local total variations, and clustered using Fuzzy C-mean clustering algorithm. Then feature points in the query image and the anchor image are matched into pairs in zigzag ordering along the diagonals of the images cluster by cluster. In the mean time, the outliers of feature points are removed. Then the system decisions about the authenticity of images are determined by the majority vote of whether three types of distance between matched feature point pairs are larger than their respective thresholds. The three types of distance include 1) histogram weighted distance, which is proposed in this paper, 2) normalized Euclidean distance, and 3) Hausdorff distance. The geometric transform between the query image and the anchor image is estimated and the query image is registered. The possible tampered image blocks are detected and the percentage of the tampered area is roughly estimated. The experimental results show the effectiveness and robustness of the proposed image authentication system.

Index Terms

Image authentication, image hashing, Fuzzy C-means clustering, histogram weighted distance, Morlet wavelet.

I. INTRODUCTION

Digital images become an important part of our daily lives due to the rapid growth of Internet and the increasing demand of multimedia contents from people. The upsoaring number of image applications facilitate image processing, and at the mean time, make fabricating and copying of digital contents easy, and lead us doubtful when digital images are used as evidences in court. Therefore, efficient and automatic techniques are desired to identify and verify the contents of digital images. Image authentication is such a promising technique to automatically identify whether a query image is a different one, or a fabrication, or a simple copy of an anchor image. Here, the anchor image is the ground truth image or the original image as an authentication reference, and the query image is the one under suspicion.

Image authentication techniques usually include conventional cryptography, fragile and semi-fragile watermarking and digital signature and so on. The authentication process can be assisted with the original image or in the absence of the original image. Image authentication methods, based on cryptography, use a hash function [1], [2] to compute the message authentication code (MAC) from images. The generated hash is further encrypted with a secret key from the sender, and then appended to the image as an overhead, which is easy to be removed. Fragile watermarking usually refers to reversible data hiding [3]–[6]. A watermark is embedded into an image in a reversible and unnoticeable way. If the original image is reconstructed and the embedded message is recovered exactly, then the image is declared as authentic. The conventional cryptography and reversible watermarking can guarantee the integrity of images, but they are vulnerable to any changes. A one-bit different version of the image will be treated as a totally different image. These methods cannot distinguish tolerable changes from malicious changes. Semi-fragile watermarking has attack-resistant ability between fragile and robust watermarking. It has the ability of tampering identification. Fridrich [7], [8] proposed block Discrete Cosine Transform (DCT) based methods to identify the tampered areas. But the block based method is susceptible to translation and cropping attacks. Besides, semi-fragile watermarking techniques will change the pixel values, and degrade the image quality once the watermarks are embedded, which is undesirable. And there is a trade off between image quality and watermark robustness. Digital signature based techniques are image content dependent, which are also called image hashing. An image hash is a representation of the image. Besides image authentication, it can also be used for image retrieval and other applications. Kozat *et al.* [9] proposed an image hash technique based on Singular Value Decomposition (SVD). It is assumed that the singular values are robust to general image processing, but not to malicious image tampering. It achieves high probability of detecting a tampered image at the cost of high false alarm probability. Venkatesan *et al.* [10] developed an image hash based on a statistical property of wavelet coefficients, which is

invariant to content-preserving modifications of images. But it is not intended to identify the locations of changes. The image authentication system proposed by Monga *et al.* [11] is based on feature points of images. The system is not sufficiently robust due to the outlier feature points produced by image processing, although Hausdorff distance is used to evaluate the distances between feature points. Monga *et al.* [12] also proposed a perceptual image hashing. The extracted features are the quantized magnitudes of the Morlet wavelet coefficients at feature points. Although the distribution of the magnitudes of the Morlet wavelet coefficients may be preserved under perceptually insignificant distortions, the location information is lost.

In this paper, we propose a perceptual image authentication technique based on clustering and matching of feature points of images to address the limitations of the aforementioned schemes. Feature points are first generated from a given image, but their locations may be changed due to possible image processing and degradation. Accordingly, we propose to use Fuzzy C-mean clustering algorithm to cluster the feature points and remove the outliers from the feature points. In the meanwhile, the feature points in the query image and the anchor image are matched into pairs in zigzag ordering along diagonals of the images cluster by cluster. Three types of distance are used to measure the distances between the matched feature point pairs. Histogram weighted distance is proposed, which is equivalent to Hausdorff distance after outlier removal. The authenticity of the query image is determined by the majority vote of whether three types of distance between matched feature point pair are larger than their respective thresholds. The geometric transforms through which the query images are aligned with the anchor images are estimated, and the query images are registered accordingly. Moreover, the possible tampered image blocks are identified, and the percentage of the tampered area is estimated.

The rest of the paper is organized as follows. Section II presents an overview of the proposed image authentication system. Section III describes how to detect feature points in images. In Section IV, we propose an efficient and effective algorithm to remove outliers of feature points, and the remaining feature points are ordered and matched into pairs. Histogram weighted distance is proposed and normalized Euclidean distance and Hausdorff distance are used in Section V. Majority voting strategy is used to determine the authenticity of images. In Section VI, possible attacks are identified, the query images are registered, the tampered image blocks are located, and the percentage of tampered area is estimated. Experimental results are shown in Section VII. Finally, Section VIII concludes the paper.

II. SYSTEM OVERVIEW

The services provided by the proposed image authentication system include:

- Identify a query image as a similar image, or a tampered image, or a different image, w.r.t. an anchor image;
- Evaluate similarity of two images by distance between them;
- Identify and locate three types of tampered area, i.e., added area, removed area, changed area;
- Estimate the percentage of tampered area.

The flowchart of the proposed image authentication system is shown in Fig. 3. First, feature points are extracted from the anchor image and the query image with the k -largest local total variations. Second, the feature points are clustered, then outliers of feature points are removed, and corresponding feature point pairs in the anchor and query images are zigzag aligned along the diagonals of images. Third, histogram weighted distance is proposed. Three types of distances between two images are evaluated and compared to thresholds. The low missing rate of authentication is desired in our system. Thus, majority voting strategy is used to make authentication decisions of images. If at least two distances are greater than their thresholds, the two images are declared as different. Otherwise, the two images are declared as similar for further examination. Forth, if the two images are considered to be similar, the possible attacks on the query image, i.e., geometric attacks and tampering attacks, are subject to detection. The query image is further registered. The locations and percentage of tampered area are estimated.

III. FEATURE POINT DETECTION

Feature points are geometric descriptors of the contents of images. Most information of signals is conveyed by irregular structures and transient phenomena of signals. Feature points such as corners can be used to characterize the saliency of images. Feature point based descriptor is more robust to geometric attacks than statistics-based descriptors. Feature points are also useful for registration and identification of possible underlying attacks (geometric or non-geometric), on query images.

A. Preprocessing

Preprocessing will change image pixels and may influence the detection and description of feature points. To extract the original information from the query image, we keep the query image intact except adapting its size to the size of the anchor image.

B. Feature Point Extraction

For different applications, different techniques to extract feature points are explored in the literature [13]. Since image authentication needs to be invariant to content-preserving processing, hence, robust and repeatable feature point detectors with small computation overhead are desired. Jaroslav *et al.* [14] proposed a feature point detector for blurred images, which we call

BFP in the paper. In our paper, a more robust feature point detector is proposed based on BFP. BFP is intended to efficiently detect points which belong to two edges regardless their orientations. It selects points with the k -largest local variances. The local variance (LV) is defined on the image block in Equation (1).

$$LV = \sum_{X \in \Omega} (I(X) - \bar{I}_{\Omega})^2 \quad (1)$$

where Ω is the image block centered at the current feature point, X is a vector representing the pixel coordinates, $I(X)$ is the pixel value at X , \bar{I}_{Ω} is the mean of the pixel values in the block. LV depends on pixel values, thus, is easily changed by any image processing.

Therefore, we propose to select feature points with the k -largest local total variations (LTV) [15]. LTV is defined as:

$$LTV = \sum_{X \in \Omega} |I'(X)|^2 \quad (2)$$

where Ω is the image block centered at the current feature point, $I'(X)$ is the gradient of image at coordinate $X = (x_1, x_2)$

$$|I'(X)| = \sqrt{\left(\frac{\partial I(X)}{\partial x_1}\right)^2 + \left(\frac{\partial I(X)}{\partial x_2}\right)^2} \quad (3)$$

LTV depends on local structure of images. It is more robust against content-preserving image processing than LV.

Therefore, our proposed feature point extraction algorithm is more robust than BFP. We use this method to determine the coordinates of the most salient feature points with the k -largest local total variations in images, as shown in Fig 2.

IV. FEATURE POINT CLUSTERING AND MATCHING

Due to possible changes applied to the query image, such as luminance changes and geometric transforms, the extracted feature points of the query image are different from those of the anchor image, no matter the query image and the anchor image are similar or not. The possibly missing, emerging and moving feature points may defeat the image authentication. If two images are similar, the possible missing, emerging and moving feature points of the query image, may enlarge their distance, and affect the similarity measure. If the query image and the anchor image are totally different images, the possible changes of feature points in the query image may decrease the distance between the two different images, and degrade the discriminability of the system. Besides, for distance evaluation, the feature point matching is needed between the anchor image and the query image. Therefore, to improve the performance of the system, the following clustering process is critical to remove outliers and match feature points into pairs in certain spatial ordering. We propose to use Fuzzy C-mean clustering to implement outlier removal and feature point matching in one pass.

A. Clustering by Fuzzy C-Means

Fuzzy C-means clustering algorithm is used to cluster the feature points. Fuzzy C-means clustering method, developed by Dunn [16] in 1973 and improved by Bezdek [17] in 1981, is based on minimization of the following objective function:

$$J_m = \sum_{i=1}^N \sum_{j=1}^C u_{ij}^m \|x_i - c_j\|^2 \quad (4)$$

where $1 \leq m < \infty$, u_{ij} is the degree of membership of x_i belonging to the cluster j , x_i is the i th feature point, c_j is the center of the cluster j , $\|\cdot\|$ is any norm evaluating the distance between any feature point and the center, N is the number of samples, and C is the number of clusters. The membership degree u_{ij} and the cluster centers c_j are updated by:

$$u_{ij} = \frac{1}{\sum_{k=1}^C \left(\frac{\|x_i - c_j\|}{\|x_i - c_k\|}\right)^{\frac{1}{m-1}}} \quad (5)$$

$$c_j = \frac{\sum_{i=1}^N u_{ij}^m \cdot x_i}{\sum_{i=1}^N u_{ij}^m} \quad (6)$$

B. Outlier Removal

The outliers are defined as extra points unmatched in corresponding clusters in the query image and the anchor image. For example, there are n feature points in cluster j in the anchor image, and $n + 1$ feature points in the corresponding cluster j' in the query image, then the one extra emerging feature point in cluster j in the query image with least degree of membership is regarded as outlier, and vice versa. Like noise, these points should not be considered in the measurement of distance between the anchor image and the query image, and the registration of the query image.

If the number of outliers in a cluster is greater than a threshold, this cluster is declared as ‘tampered’. If an image has at least one tampered cluster, this image is declared as ‘tampered’. The locations of the outliers are used to determine the locations of tampered area.

C. Spatial Ordering and Feature Point Matching

After outlier removal, the numbers of remaining feature points in corresponding clusters in the query image and the anchor image are the same. The feature point matching algorithm processes feature points cluster by cluster. In each cluster, the feature points in two images are ordered zigzag along diagonals of images. The proposed feature point matching algorithm may not result in exact pairs between feature points, but it is sub-optimal and very fast.

Given N feature points in the query image, finding the corresponding N feature points in the anchor image, incurs a computational complexity of $N!$. Whereas, the computational complexity of our proposed feature point matching algorithm is $O(N \log n)$, where n is the average number of feature points per cluster. Assume there are n feature points per cluster on average. Thus, there are $\frac{N}{n}$ clusters. For each cluster, the computation of ordering is $O(n \log n)$. After clustering and outlier removal, the computational complexity of feature point matching reduces to $O(N \log n)$ by cluster ordering and spatial ordering.

The spatial matching by diagonal ordering is optimal to raster ordering in terms of correct matching rate under the perturbation of possible attacks. The proposed matching algorithm is robust to outliers, and the case where feature points are removed, emerge or change their locations due to possible noise or attacks. It increases the similarity measure of similar images, and increases the distance between two different images.

D. Algorithm Summary

For feature point set X_A in the anchor image and feature point set X_Q in the query image.

- 1) Perform fuzzy C-means clustering on X_A and X_Q , which are clustered into clusters X_{A_j} and X_{Q_j} ($j = 1, \dots, C$), C is the number of clusters.
- 2) For cluster j ($j = 1, \dots, C$) do:

Ordering feature points in X_{A_j} and X_{Q_j} according to their coordinates (x_1, x_2) in zigzag ordering along diagonals of the images, i.e., ordering feature points with respect to $(x_1 + x_2)$.

 - a) if $\text{length}(X_{A_j}) = \text{length}(X_{Q_j})$, match $(X_{A_j}^{(i)}, X_{Q_j}^{(i)})$ into pairs, where $X_{A_j}^{(i)}$ is the i th feature point in the j th cluster of the anchor image and $X_{Q_j}^{(i)}$ is the i th feature point in the j th cluster of the query image.
 - b) if $\text{length}(X_{A_j}) > \text{length}(X_{Q_j})$, for each feature point $X_{Q_j}^{(i)}$ in X_{Q_j} , sequentially find the closest unmatched feature points $X_{A_j}^{(i')}$ in X_{A_j} . For pairs $(X_{A_j}^{(i')}, X_{Q_j}^{(i)})$ and $(X_{A_j}^{(i'')}, X_{Q_j}^{(i)})$, if $i_1 > i_2$, then $i'_1 > i'_2$. Other unmatched feature points in X_{A_j} are considered as outliers of X_{A_j} .
 - c) if $\text{length}(X_{A_j}) < \text{length}(X_{Q_j})$, for each feature point $X_{A_j}^{(i)}$ in X_{A_j} , sequentially find the closest unmatched feature points $X_{Q_j}^{(i')}$ in X_{Q_j} . For pairs $(X_{A_j}^{(i')}, X_{Q_j}^{(i)})$ and $(X_{A_j}^{(i'')}, X_{Q_j}^{(i)})$, if $i_1 > i_2$, then $i'_1 > i'_2$. Other unmatched feature points in X_{Q_j} are considered as outliers of X_{Q_j} .

V. DISTANCE EVALUATION

Three types of distance are used to evaluate the distances between images, among which histogram weighted distance is proposed. If at least two types of distance are larger than their corresponding threshold, the two images are considered different, otherwise similar. The thresholds are obtained by statistical experiments.

A. Normalized Euclidean Distance

The first type of distance is normalized Euclidean distance between the matched feature point pairs, which is given by:

$$E(X_A, X_Q) = \frac{1}{N} \sum_{i=1}^N \|X_A^{(i)} - X_Q^{(i)}\|_E \quad (7)$$

where N is the number of feature point pairs, $X_A^{(i)}$ is the coordinate of the corresponding i th feature point in the anchor image, $X_Q^{(i)}$ is the coordinate of the i th feature point in the query image, $\|\cdot\|_E$ is Euclidean norm.

B. Hausdorff Distance

The Hausdorff distance [18] is defined by:

$$H(X_A, X_Q) = \max(h(X_A, X_Q), h(X_Q, X_A)) \quad (8)$$

where

$$h(X_A, X_Q) = \max_{x \in X_A} \min_{y \in X_Q} \|x - y\| \quad (9)$$

Since it is minimax based distance, it is robust to outliers of feature points. It is also used in an image hashing system in paper [12].

C. Histogram Weighted Distance

We propose the third type of distance, i.e., histogram weighted distance, which is a perceptual based distance. The significance of a feature point is weighted by percentage of pixel values at that position. If the pixel values of feature points have higher percentage in the histogram of pixels, the distances between these pairs of feature points should be trusted more than others. The histogram weighted distance is given by:

$$W(X_A, X_Q) = \max\left(\frac{1}{N} \sum_{i=1}^N w_A^{(i)} \|X_A^{(i)} - X_Q^{(i)}\|_E, \frac{1}{N} \sum_{i=1}^N w_Q^{(i)} \|X_A^{(i)} - X_Q^{(i)}\|_E\right) \quad (10)$$

where N is the number of feature point pairs, $X_A^{(i)}$ is the coordinate of the i th feature point in the anchor image, $X_Q^{(i)}$ is the coordinate of the i th feature point in the query image, $w_A^{(i)}$ is the luminance percentage of the i th feature points in the anchor image, $w_Q^{(i)}$ is the luminance percentage of the i th feature points in the query image, and $\|\cdot\|_E$ is the Euclidean norm.

D. Majority Vote

The final decision is made from majority vote among whether three types of distance are larger than the respective thresholds or not as shown in Fig. 3. It is due to the ability and limitation of three types of distance. Normalized Euclidean distance is mostly used, but is easily perturbed by outlier feature points; Hausdorff distance is a kind of minmax distance, repels the outliers, but may lose some geometric information of images; histogram weighted distance considers pixel/color information, makes decision more robust, although it is influenced by outliers too. Therefore, majority vote is necessary to take advantage of these types of distance. Three types of distance are equal important and are treated with the same weight in the proposed system. They are diverse enough in our experiments to lower authentication error rate. More distance measures may repeat the performance of existing distance or dilute their functions, and will increase the system complexity.

E. Strategy for Threshold Determination

The thresholds of distance to differentiate similar images and different images are determined based on the statistical experiments. A novel strategy we take is to calculate distance among two video shots. A frame in one video shot is taken as the anchor image. The other frames are query images. Then the middle value between the average distance in the same video shot and the average distance in the different video shots is taken as the threshold. More results could be found in experiments in Section VII, especially as shown in Fig. 8.

VI. POSSIBLE ATTACK IDENTIFICATION

After distance evaluation, if the two images are considered similar, the possible geometric attacks and tampering, which the query image may experience are subject to further detection.

A. Geometric Attack Estimation and Registration

Registration algorithms, such as iterative close point (ICP) algorithm [19] and Kanade-Lucas-Tomasi Feature Tracker (KLT) [20] estimate the translation and rotation transforms between feature point pairs, but do not consider scaling transform. Scale-invariant feature transform (SIFT) algorithm [21], [22] considers the scaling transform, but requires high computation overhead. In this paper, we propose to estimate and recover images from possible geometric attacks in two stages. First, iterative close point (ICP) algorithm [19] is used to estimate the rotation and translation based on the matched feature point pairs. Then the query image is recovered from the rotation and translation transforms. Second, the scaling transforms are estimated. We propose to use the ratio of the standard deviation (STD) of feature points of the query image to the standard deviation of feature points of the anchor image to estimate the possible scaling transforms after rotation and translation registration.

B. Tampering Attack Identification

The possible tampered image blocks are detected and the percentage of the tampered area is estimated. The tampered image blocks are determined by the distances between local histograms of image blocks around the feature points in two images. The distance we use is earth mover distance (EMD) [23], [24]. We divide the tampering into three categories: adding new features, removing existing features, and changing existing features. Feature-added areas are identified around the outlier feature points in the query image, which do not appear in the anchor image. Feature-removed areas are identified around the outlier feature points in the anchor image, which do not appear in the query image. Feature-changed areas are the areas with matched feature points, which have large local histogram distances from the corresponding area in the anchor image. If the EMD between local histograms of image blocks around feature points in the anchor image and the local histograms of the corresponding blocks in the query image is larger than the threshold, the blocks in the query image are declared as tampered areas. After detection possible tampered areas, we sum up the area of these tampered blocks, and use the ratio of the sum of the tampered area to the area of the whole image as the percentage of the tampered area.

VII. EXPERIMENTAL RESULTS

A. Feature Point Detection

We will show the robustness of the proposed feature point detector in this subsection. We create differently distorted versions of image ‘Lena’ by tampering Lena’s hat, rotating the image by 3 degrees, and histogram equalization. In Fig. 2, feature points are denoted by red ‘o’. The feature points extracted from the original image, the tampered image, the rotated image and the image after histogram equalization are almost the same. It indicates the robustness of our proposed feature point detector against attacks.

B. Feature Point Matching Example

Fig. 4 shows the result of the proposed feature point matching algorithm. Specifically, Fig. 4(a) shows the original image; Fig. 4(b) shows the tampered and compressed image and Fig. 4(c) shows extracted, clustered and matched feature points. The axes in Fig. 4(c) denote the pixel coordinates in images. Each cluster concentrates in one ellipse. Feature points of different clusters are illustrated with different colors, ‘+’ and ‘*’ denote the matched and outlier feature points in the original image, and ‘o’ and ‘□’ denote the matched and outlier feature points in the query image respectively. Tampering the corner of the hat of Lena in Fig. 4(b) will add and remove feature points. By using the proposed feature point matching algorithm, the outliers of feature points can be efficiently and correctly detected, and corresponding feature points between images in Fig. 4(a) and Fig. 4(b) are matched into pairs in line with the fact. It shows the effectiveness of our feature point matching algorithm. And our algorithm runs fast.

C. Authentication Performance

We compare authentication performance of four image authentication systems: the proposed image authentication system, image hashing based on feature points [12], image hashing based on Singular Value Decomposition (SVD) [9] and image hashing based on Wavelet [10] in image hashing toolbox [25].

We test image authentication system on 6 test images. They are 512x512 gray images shown in Fig. 5.

Several types of attacks are made on these images: scaling images to 0.5 and 1.5 of their sizes, compressing images using JPEG with quality factor 50 [26], rotating images by 5 degrees, cropping 20% of images, adding white Gaussian noise ($\sigma^2 = 20$) to images, filtering images with Gaussian and Median filters.

The thresholds to distinguish similar images and different images are 1.5, 0.2 and 0.2 for normalized Euclidean distance, histogram weighted distance and Hausdorff distance respectively in the propose image authentication system. The proposed image authentication system can make correct authentication decisions in the cases where feature point based, SVD based and Wavelet based image authentication in image hashing toolbox [25] may not. Some experimental results are shown in Table I. Feature point based, SVD based and Wavelet based image authentication are denoted by FP, SVD and Wavelet in Table I respectively. The decisions of the image authentication systems are represented by ‘S’ for similar images and ‘D’ for different images. FP fails to authenticate the Lena and its tampered version, Lena and its compressed and enhanced version. SVD underestimates the distances and considers Lena and Mandrill are similar. Wavelet fails to recognize similarity between the image ‘Goldhill’ and its enhanced version. It fails in luminance adjusted cases. Our proposed authentication system makes correct decisions in these cases.

We also create 84 attacked images from six test images in Fig. 5. Each test image has 14 attacked versions, which suffers from scaling 0.5, scaling 1.5, JPEG compression with quality 50, 5 degree rotation, cropping 20%, white gaussian noise addition, filtering with Gaussian filter and Median filter, and 6 tampering attacks. We test similarity and difference among 3486 image pairs. The correct probability of the proposed system, FP, SVD and Wavelet are 84.5%, 81.9%, 83.2%, 79.1% respectively.

D. Distance Comparison

We compare the three types of distance in the proposed image authentication system with the distance of image hash based on feature points [12], the distance of image hash based on Singular Value Decomposition (SVD) [9] and the distance of image hash based on Wavelet [10] in image hashing toolbox [25]. They are denoted by Euclidean, Histogram weighted, Hausdorff, FP, SVD and Wavelet in Fig. 7 and Fig. 8.

Our experiments use the frames of two shots in video sequence *big_buck_bunny_480p_h264.mov* [27]. Each shot has 30 frames. The 20th frames in the two shots are shown in Fig. 6.

The distances between the 20th frame and the other frames in the first shot are shown in Fig. 7. The distances are all very small.

The distances between the 20th frame in the first shot and the other frames in two shots are shown in Fig. 8. The methods can distinguish two shots. Discriminability of SVD is the lowest, while discriminability of FP is the highest. The distances used in our authentication system have both robustness and discriminability, and the non-constant distances reflect the similarity between frames better than other methods since perceptually similar images have small distance between them. And FP, SVD and Wavelet based methods do not provide tampering location identification.

E. Tampering Detection

We detect tampering such as adding, removing and changing features as shown in Table II. Three types of tampering, i.e., adding, changing, and removing features, are shown in each row of the Table II. In the images in the first column of Table II, the '□' in images are basic image blocks used in local histogram distance evaluation. The '□' indicate the detected tampered blocks around some feature points. The tampered versions of 'Lena' are shown in the first column of the Table II. The percentage of tampering area is also estimated in the second column of the Table II, but is under-estimated. If we increase size of the '□', missing rate will be high for small-area tampered images, and it will increase EMD computation overhead. Thus we just choose 11x11 as the size of image blocks. The size of image blocks should be hierarchical and adaptive in our future work.

VIII. CONCLUSIONS AND FUTURE WORK

We proposed an efficient robust image authentication system. The feature points with the k -largest local total variations are extracted. Feature points are clustered by Fuzzy C-means algorithm. Then the outliers of feature points are removed and feature points pairs between the query image and the anchor image are matched in zigzag order cluster by cluster at the same time, which increases the robustness of the proposed image authentication system. Furthermore, the normalized Euclidean distance, the Hausdorff distance, the histogram weighted distance between the query image and the anchor image are evaluated. Based on the distances, whether the images similar or not are determined by majority voting. For similar images, possible geometric attacks are subject to detection and image registration is performed. Possible tampered areas are determined and classified, and the percentage of tampered area is estimated. The proposed image authentication system could serve as a building block in many applications such as copyright protection, image retrieval and video signature.

REFERENCES

- [1] S. Halevi and H. Krawczyk, "Strengthening digital signatures via randomized hashing," *Advances in Cryptology-CRYPTO 2006*, pp. 41–59, 2006.
- [2] V. Skala and M. Kucha, "The hash function and the principle of duality," in *Proceedings of Computer Graphics International 2001*, pp. 167–174, 2001.
- [3] M. Celik, G. Sharma, A. Tekalp, and E. Saber, "Reversible data hiding," in *Proceedings of IEEE International Conference on Image Processing*, 2, pp. 157–160, Citeseer, 2002.
- [4] J. Tian, "Wavelet-based reversible watermarking for authentication," in *Proceedings of SPIE Security and Watermarking of Multimedia Cont. IV*, 4675(74), pp. 679–690, 2002.
- [5] L. Yang, P. Hao, and C. Zhang, "Progressive reversible data hiding by symmetrical histogram expansion with piecewise-linear haar transform," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, 2007*, 2, 2007.
- [6] L. Yang and P. Hao, "Infinity-norm rotation transforms," *IEEE Transactions on Signal Processing* 57(7), 2009.
- [7] J. Fridrich, "Image watermarking for tamper detection," in *Proceedings of International Conference on Image Processing, 1998*, 2, 1998.
- [8] J. Fridrich, "Methods for tamper detection in digital images," *Multimedia and Security*, p. 29.
- [9] S. Kozat, R. Venkatesan, and M. Mihcak, "Robust perceptual image hashing via matrix invariants," in *Proceedings of International Conference on Image Processing, 2004*, 5, 2004.
- [10] R. Venkatesan, S. Koon, M. Jakubowski, and P. Moulin, "Robust image hashing," in *Proceedings of International Conference on Image Processing, 2000*, 3, 2000.
- [11] V. Monga, D. Vats, and B. Evans, "Image authentication under geometric attacks via structure matching," in *IEEE International Conference on Multimedia and Expo, 2005. ICME 2005*, pp. 229–232, 2005.
- [12] V. Monga and B. Evans, "Perceptual image hashing via feature points: performance evaluation and tradeoffs," *IEEE Transactions on Image Processing* 15(11), pp. 3452–3465, 2006.
- [13] T. Tuytelaars and K. Mikolajczyk, "Local invariant feature detectors: A survey," *Foundations and Trends in Computer Graphics and Vision* 3(3), pp. 177–280, 2007.
- [14] J. Kautsky, B. Zitová, J. Flusser, and G. Peters, "Feature point detection in blurred images," in *proceedings of IVCNZ*, pp. 103–108, 1998.
- [15] G. Aubert and P. Kornprobst, "Mathematical problems in image processing," 2006.
- [16] J. Dunn, "A fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters," *Cybernetics and Systems* 3(3), pp. 32–57, 1973.

- [17] J. Bezdek, *Pattern recognition with fuzzy objective function algorithms*, Kluwer Academic Publishers Norwell, MA, USA, 1981.
- [18] P. Cignoni, C. Rocchini, and R. Scopigno, "Metro: measuring error on simplified surfaces," in *Computer Graphics Forum*, **17**(2), pp. 167–174, 1998.
- [19] Z. Zhang, "Iterative point matching for registration of free-form curves," *Int. J. Comp. Vis* **7**(3), pp. 119–152, 1994.
- [20] B. Lucas and T. Kanade, "An iterative image registration technique with an application to stereo vision," in *International joint conference on artificial intelligence*, **3**, p. 3, Citeseer, 1981.
- [21] D. Lowe, "Object recognition from local scale-invariant features," in *proceedings of ICCV*, p. 1150, Published by the IEEE Computer Society, 1999.
- [22] D. Lowe, "Distinctive image features from scale-invariant keypoints," *International journal of Computer Vision* **60**(2), pp. 91–110, 2004.
- [23] Y. Rubner, C. Tomasi, and L. Guibas, "A metric for distributions with applications to image databases," in *Proceedings of the sixth International Conference on Computer Vision, 1998*, pp. 59–66, 1998.
- [24] E. Levina and P. Bickel, "The earth movers distance is the Mallows distance: Some insights from statistics," in *Proceedings of ICCV*, **2**, pp. 251–256, Citeseer, 2001.
- [25] <http://users.ece.utexas.edu/~bevans/projects/hashing/toolbox/index.html>
- [26] T. Recommendation, "Information technology - digital compression and coding of continuous-tone still images - requirements and guidelines," in *Recommendation T.81*, 1993.
- [27] <http://www.bigbuckbunny.org>

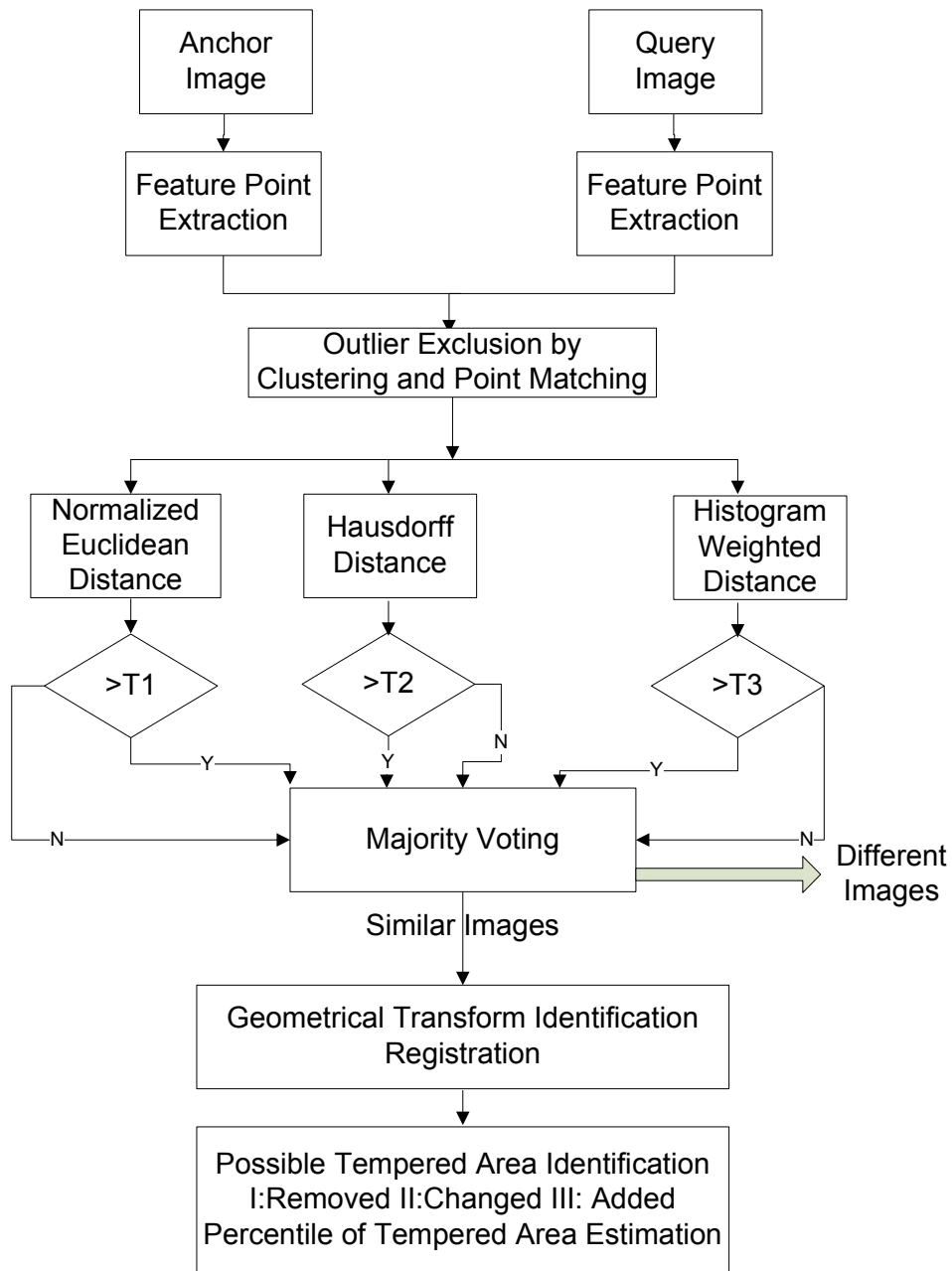


Fig. 1. The flowchart of the proposed image authentication system.



(a) The original image and extracted feature points. (b) The hat-tampered image and extracted feature points.



(c) The rotated image and extracted feature points. (d) The image after histogram equalization and extracted feature points.

Fig. 2. The stable feature point detector.

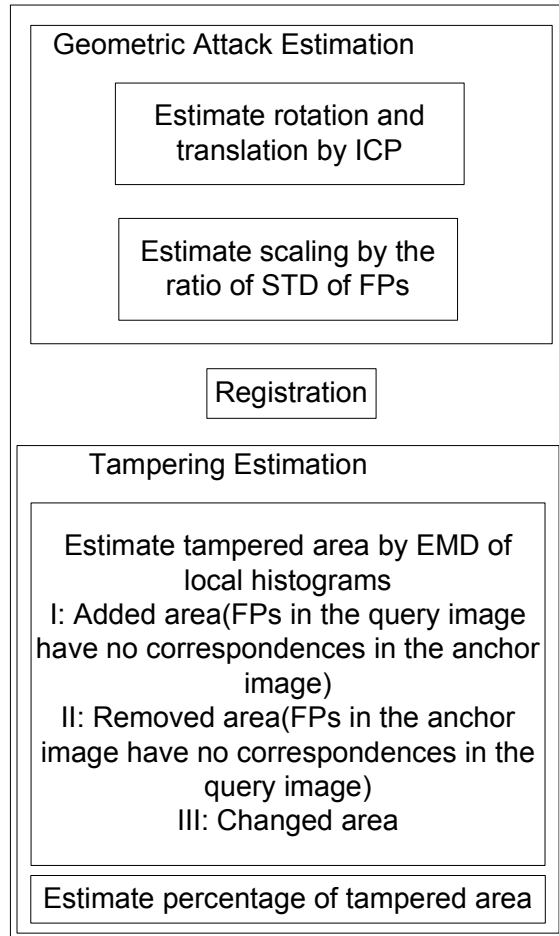


Fig. 3. Diagram of possible attack identification.

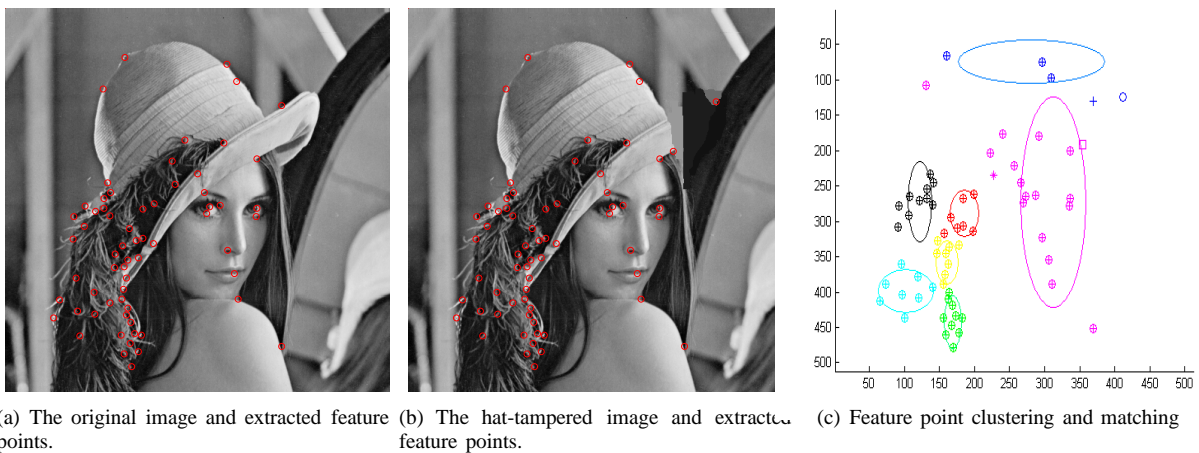


Fig. 4. Feature point clustering and matching.



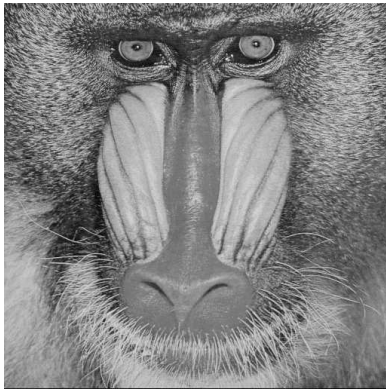
(a) Lena



(b) Barbara



(c) Boat



(d) Mandrill











(e) Jet



(f) Pepper

Fig. 5. Six test images for image hashing.

TABLE I
AUTHENTICATION PERFORMANCE COMPARISON AMONG DIFFERENT METHODS.

Image 1	Image 2	Proposed	FP	SVD	Wavelet
		S	D	S	S
		S	D	S	S
		D	D	S	D
		S	S	S	D



(a) The 20th frame in the first shot.

(b) The 20th frame in the second shot.

Fig. 6. The two frames in the test video shots *Bunny*.

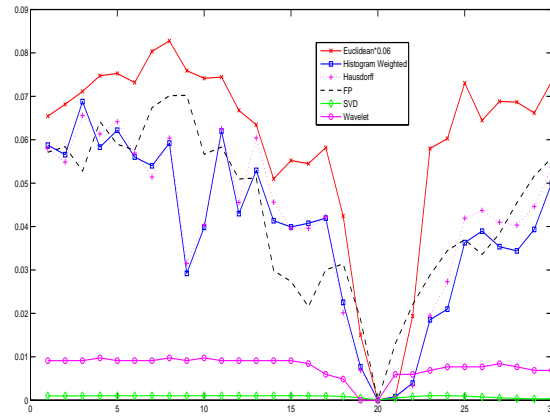


Fig. 7. Distance comparison among different authentication methods in one video shot.

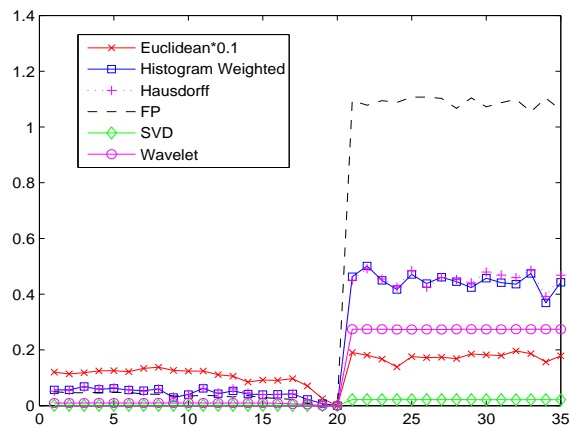



Fig. 8. Distance comparison among different authentication methods in two video shots.

TABLE II
TAMPERING DETECTION AND PERCENTAGE OF TAMPERING AREA ESTIMATION.

Detection results	Percentage of tampering area
	1.53%
	0.84%
	1.02%