Strong Image Alignment for Meddling Recognision Purpose

Mrs. Pradnya Gajendra Kshirsagar
*(Department of computer science, Vishwabharati academy's College of Engineering , University of Pune, India)

ABSTRACT: The *Vast use of classic and modern technologies of internet causes increase the interest on systems that will protect in visual images against the wrongful manipulation that may be processed during the execution / transmission .One reason behind this problem is the verification of image received during communication. This work will be performed by strong image, and for this the image must be first registered by taking advantage of information provided by specific part of connected image. We describe strong image setting method in which there is a use of hash element (signatures) . The required signature is also attached with image before the transmission of image as well as before the image will send at destination place to get the graphical transformation of the received image. The accessor is based on the selecting the image which is having highest preference in the parameter space to recovered the graphical transformation which is used to manipulate image. The required image encodes the spaces occurred to deal with textures and contrasted strong image types.*

A block-wise strong image will be detected which occurs a graphical representation showing the visual impression of distributed of data with directed slope can be also proposed. This can be also used to build the signature for each strong image block. This new technique shows that it gives nice result as compared with state-of-art method.

Keywords: *Bag of features (BOF), forensic hash, geometric transformations, image forensics, image registration, tampering***.**

I. INTRODUCTION

The growing demand of techniques useful to protect digital visual data against malicious manipulations is induced by different episodes that make questionable the use of visual content as evidence material [1], [2]. All those, methods used for validity and authenticity of received image are required in internet communication. This strong image recognition can be make by using watermarking approach. This watermark will be inserted into the image during strong image recognition, and problems will be extracted to verify if there were any bad executions on received image. Any damage into the watermark proves that strong image is under construction

To avoid the twisting of content of image in watermarking method there is another method introduced that is signature based method. In Signature –based approach the signature must be small and strong and cannot be overlap into Image and also it must be header information of that image. Different signature-based approaches have been recently proposed in literature [3]–[10]. Most of them share the same basic scheme: 1) a hash code based on the visual content is attached to the image to be sent; 2) the hash is analyzed at destination to verify the reliability of the received image.

This method image hash is used with the help of which all the information and image content will be available in condensed way. The Hashed image must be strong against the operation allowed to it as well as its appearance also different from other image. This image hashing techniques is very useful technique for validating or checking the image authentication by using proper communication channel. Image hashing techniques are considered extremely useful to validate the authenticity of an image received through a communication channel. The binary decision task used for image authentication is not sufficient in this process. In the application, Forensic Science is fundamental to provide scientific evidence through the history of the possible manipulations ,which is applied to the original image to obtain the one, in which analysis manipulations provides required information to the end user , to decide whether the image can be trusted or not. All image manipulation information should be recovered from the short image hash signature which is one of the most challenging task. The list of manipulations provides to the end user the information needed to decide whether the image can be trusted or not. In order to perform tampering localization, the receiver should be able to filter out all the geometric transformations (e.g., rotation, scaling, translation, etc.) added to the tampered image by aligning the received image to the one at the sender[3]–[8].

The image alignment can be done randomly where only received image can be available at destination level and there is no any reference image available . At this level the geometric transformation of received image which is taken from signature must be recover which is most challenging task. At this level for better performance of image alignment and tampering localization it requires to design robust forensic hash method. Despite the fact that different robust alignment techniques have been proposed by computer vision researchers [11]–[13], these different techniques are not suitable in forensic hashing, the basic requirement is that the image signature should be as “compact” as possible to reduce the overhead of the network communications. To fit the basic condition/requirement , authors of [6] have proposed to exploit information extracted through Radon transform and scale space theory in order to estimate the parameters of the geometric transformations (i.e., rotation and scale).

To make more strong the alignment phase with respect to manipulations such as cropping and tampering, an image hash based on robust invariant features has been proposed in [7]. The latter technique extended the idea previously proposed in [8] by employing the bag of features (BOF) model to represent the features to be used as image hash. This representation of bag of features (BOF) is useful to reduce the space needed for the image signature, by maintaining the performances of the alignment component. In [4] a more robust approach based on a cascade of estimators has been introduced; it is able to better handle the replicated matchings in order to make a more robust estimation of the orientation parameter. The use of the cascade of estimators, which allows a higher precision in estimating the scale factor, this is the more effective way to deal with the problem of wrong matchings has been proposed in [3], where a filtering strategy based on the scale-invariant feature transform (SIFT) dominant directions combined in cascade with a robust estimator based on a voting strategy on the parameter space is presented. Taking into account the technique in [3], we propose to extend the underlying approach by encoding the spatial distribution of the image features to deal with highly textured and contrasted tampering patterns.

The proposed estimator is based on a voting procedure in the parameter space of the model which is used to recover the geometric transformation occurred into the manipulated image. The proposed method of tampering detection obtains satisfactory results with a significant margin in terms of estimation accuracy with respect to [4] and [7]. Further, by encoding spatial distribution the proposed method performs the original method proposed in [3] when strongly contrasted and/or texture regions are contained into the image. I also propose a block-wise tampering detection based on histograms of oriented gradients representation ,which makes the use of a non-uniform quantization to build the signature of each image block for tampering purposes. Experimental results confirm the effectiveness of the non-uniform quantization in terms of both compactness of the final hash signature and tampering detection accuracy. The main contributions of the paper can be summarized as follows.

1) Lu et al. [7] simply consider only the single matching in the first estimation and refine the results later considering the remaining ones. Although the refinement can be useful, the correctness of the final estimation heavily depends on the first estimation (only a refinement is performed later). Our approach does not discard replicated matchings retaining their useful information. The ambiguity of the matching is solved considering all the possible pairs with the same. As discussed also in [4], this solution introduces additional noise (i.e., incorrect pairs) that has to be properly taken into account employing the voting procedure.

2) The strong image estimator is based on a signature voting strategy. This voting strategy under parameter space allows to map the matchings from the image coordinate space to the parameters space novel. Specifically, the equations related to the similarity model have been combined and reduced with respect to the simple application of the voting procedure in the four-dimensional parameters space.

3) Feature selection based on their spatial distribution. In previous works (Lu et al. [7], Roy et al. [8], Battiato et al.[4]) the features were selected considering only their contrast properties. The proposed approach introduces a novel selection strategy that considers both contrast properties and spatial distribution of the features.

4) Complex dataset of tampered images.

II. REGISTRATION

The Alignment of received image is one of the conmen steps of image tampering detection. Registration of image is little but difficult job since all the other tasks (e.g., tampering localization) usually assume that the received image is aligned with the original one, and hence could fail if the registration is not properly done. Because of limited information can be used like no any original image is available at destination and image hash should be as short as possible ,Classical registration approaches [11]–[13]cannot be directly employed in the considered context.

The schema of the proposed registration component is shown in Fig. 1. As in [3], [4], and [7], we adopt a BOF-based representation [15] to reduce the dimensionality of the descriptors we employ a transformation model and a voting strategy to retrieve the geometric manipulation [16].

In the proposed system, a codebook is generated by clustering the set of SIFT [17] extracted on training images. The clustering procedure points out a centroid for each cluster. The set of centroids represents the codebook to be used during the image hash generation. The computed codebook is shared between sender and receiver (Fig. 1).

This codebook is built only once, and then used for all the communications between sender and receiver (i.e., no extra overhead for each communication).The sender can extracts all SIFT features and sorts them in descending order with respect to their contrast values. After extracting of all features , the top SIFT are selected and associated to the label corresponding to the closest centroid belonging to the shared codebook. At last, the final signature for the alignment component is created by considering the label, the dominant direction, and the key point coordinates for each selected SIFT (Fig. 1).

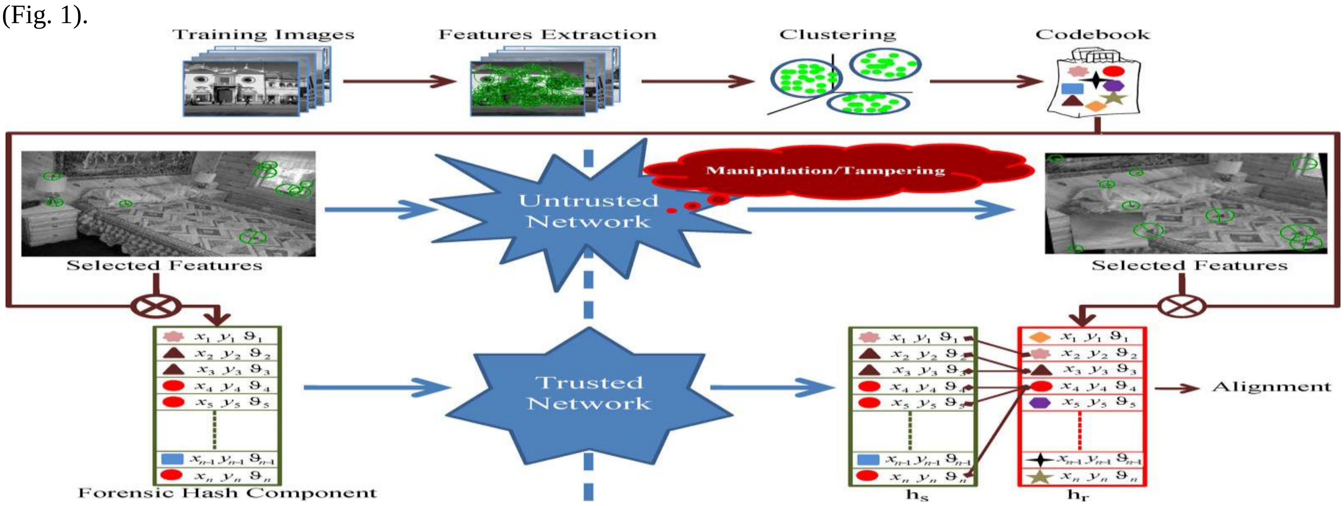


Fig. 1. Overall schema of proposed registration component

The source image and the corresponding hash component for the alignment are sent to the destination. As in [5] the system assumes that the image is sent over a network consisting of possibly untrusted nodes, whereas the signature is sent upon request through a trusted authentication server which encrypts the hash in order to guarantee its integrity.

After reaching the image at its destination, the receiver generates the related hash signature for registration by using the same procedure employed by the sender. Then, the entries of the hashes and are matched by considering the values (see Fig. 1,The alignment is performed by employing a similarity transformation of key point pairs corresponding to matched hashes entries (1) &(2). The earlier transformation is used to model the geometrical manipulations which have been done on the source image during the untrusted communication. Source image points are transforms with destination image point by combining rotate on, scaling and translation process.

III. INDENTATIONS AND EQUATIONS

The image signature to be used for alignment component must be strong enough against malicious manipulations. As well as, the image hash should be that much strong to handle different visual content to be encoded like (textures, contrast variations, etc.).

For the communication purpose a small subset of the strong image features is retained to compose the image hash for the alignment component. Fig. 4 shows an example of malicious tampering which deludes the typical SIFT-based systems presented in [3], [4], [7], and [8]. In Fig. 4(a) the image at the source is shown, whereas the malicious pattern added during the transmission is reported in Fig. 4(b). Sixty SIFT selected by the approach discussed in Section II, at both source and destination, are shown in Fig. 4(c) and Fig. 4(d).

As demonstrated by the figures, all the SIFT extracted by the sender which are used to build the alignment signature are concealed at destination, since all the 60 SIFT . The alignment procedure is hence invalidated, and all further processing to verify the authenticity of the image, to localize the tampered regions, and in general to tell the history of the manipulations of the image, will be unreliable. In order to improve the strongness of the registration phase we suggest modifying the initial step.

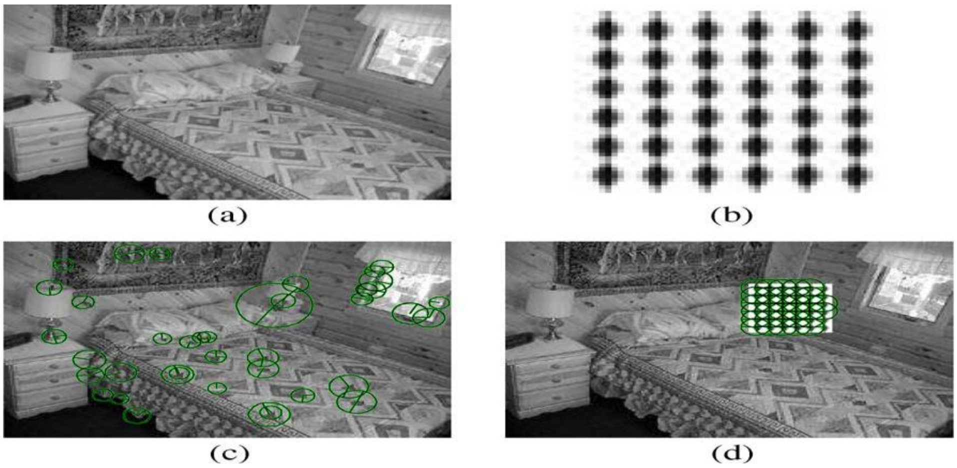


Fig. 4. Concealing true local features: (a) Original image, (b) tampering pattern, (c) 60 SIFT selected by ordering contrast values on the original image.(d) The 60 SIFT selected by ordering contrast values on tampered image.

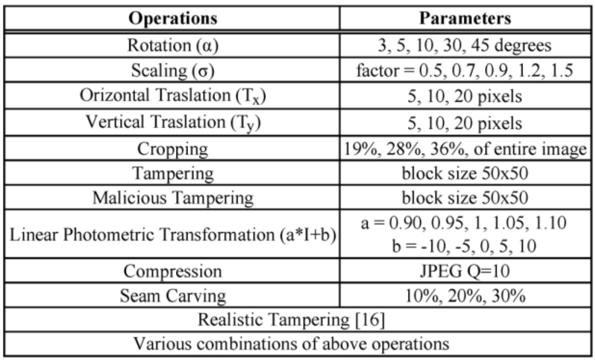
As reported in [19]–[21] the spatial distribution of the features on the entire image is a property that registration algorithms have to take into account. The proposed spatial-based selection process works as follows: first the SIFT are extracted and then grouped taking into account the spatial coordinates of the obtained feature key points. The grouping can be done employing a classic clustering algorithm (k-means, hierarchical clustering, etc.). For each cluster, the best SIFT in terms of contrast value is selected. In this way, the proposed feature selection procedure allows us to extract high contrasted features (corresponding to the clusters) well distributed in the image in terms of spatial position.

IV. FIGURES AND TABLES

The composition of the considered dataset allows for coping with the high scene variability needed to properly test methods in the context of application of this paper. The training set used in the experiments is built through a random selection of 150 images from the aforementioned dataset. Specifically, ten images have been randomly sampled from each scene category. Training and test sets are available for experimental purposes.1 The following image transformations have been considered (Table I): cropping, rotation, scaling, translation, seam carving, tampering, linear photometric transformation and JPEG compression. The considered transformations are typically available on image manipulation software. Tampering on the [22] subset has been performed through the swapping of blocks (50 50) between two images randomly selected from the training

The registration results can be obtained by employing the proposed alignment approach (with and without spatial clustering) with hash component of different size (i.e., different number of SIFT) are reported in Table II

TABLE I
IMAGE TRANSFORMATIONS

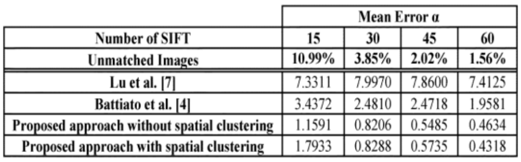


Operations	Parameters
Rotation (α)	3, 5, 10, 30, 45 degrees
Scaling (σ)	factor = 0.5, 0.7, 0.9, 1.2, 1.5
Orizontal Traslation (T_x)	5, 10, 20 pixels
Vertical Traslation (T_y)	5, 10, 20 pixels
Cropping	19%, 28%, 36%, of entire image
Tampering	block size 50x50
Malicious Tampering	block size 50x50

Linear Photometric Transformation (a*I+b)	a = 0.90, 0.95, 1, 1.05, 1.10
	b = -10, -5, 0, 5, 10

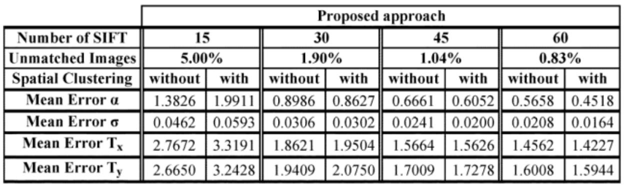
Compression	JPEG Q=10
Seam Carving	10%, 20%, 30%
Realistic Tampering [16]	
Various combinations of above operations	

TABLE II
REGISTRATION RESULTS OF PROPOSED APPROACH



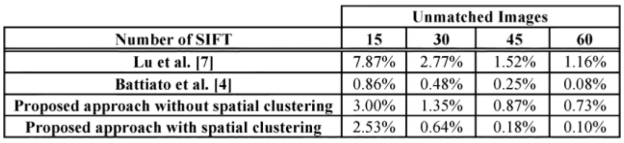
	Mean Error α			
Number of SIFT	**15**	**30**	**45**	**60**
Unmatched Images	**10.99%**	**3.85%**	**2.02%**	**1.56%**
Lu et al. [7]	7.3311	7.9970	7.8600	7.4125
Battiato et al. [4]	3.4372	2.4810	2.4718	1.9581
Proposed approach without spatial clustering	1.1591	0.8206	0.5485	0.4634
Proposed approach with spatial clustering	1.7933	0.8288	0.5735	0.4318

TABLE III
COMPARISON WITH RESPECT TO UNMATCHED IMAGES



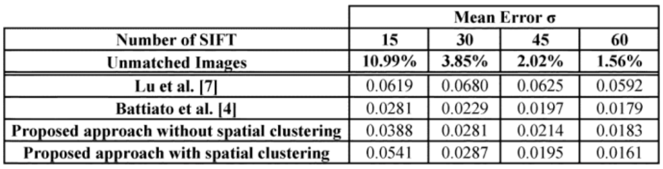
	Proposed approach							
Number of SIFT	**15**		**30**		**45**		**60**	
Unmatched Images	**5.00%**		**1.90%**		**1.04%**		**0.83%**	
Spatial Clustering	**without**	**with**	**without**	**with**	**without**	**with**	**without**	**with**
Mean Error α	1.3826	1.9911	0.8986	0.8627	0.6661	0.6052	0.5658	0.4518
Mean Error σ	0.0462	0.0593	0.0306	0.0302	0.0241	0.0200	0.0208	0.0164
Mean Error T_x	2.7672	3.3191	1.8621	1.9504	1.5664	1.5626	1.4562	1.4227
Mean Error T_y	2.6650	3.2428	1.9409	2.0750	1.7009	1.7278	1.6008	1.5944

TABLE IV
AVERAGE ROTATIONAL ERROR



	Unmatched Images			
Number of SIFT	**15**	**30**	**45**	**60**
Lu et al. [7]	7.87%	2.77%	1.52%	1.16%
Battiato et al. [4]	0.86%	0.48%	0.25%	0.08%
Proposed approach without spatial clustering	3.00%	1.35%	0.87%	0.73%
Proposed approach with spatial clustering	2.53%	0.64%	0.18%	0.10%

TABLE V
AVERAGE SCALING ERROR



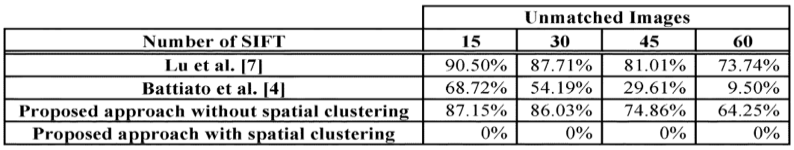
	Mean Error σ			
Number of SIFT	**15**	**30**	**45**	**60**
Unmatched Images	**10.99%**	**3.85%**	**2.02%**	**1.56%**
Lu et al. [7]	0.0619	0.0680	0.0625	0.0592
Battiato et al. [4]	0.0281	0.0229	0.0197	0.0179
Proposed approach without spatial clustering	0.0388	0.0281	0.0214	0.0183
Proposed approach with spatial clustering	0.0541	0.0287	0.0195	0.0161

As reported in Table III, by increasing the number of SIFT points the number of unmatched images decreases (i.e., image pairs that the algorithm is not able to process because there are no matchings between and) for all the approaches. In all cases the percentage of images on which our algorithm (with and without spatial clustering) is able to work is higher than the one obtained by the approach proposed in [7].

Tables IV and V show the results obtained in terms of rotational and scale estimation through mean absolute error. In order to properly compare the methods, the results have been computed taking into account the images on which all approaches were able to work (the number of unmatched images is reported into the tables). The proposed approach (with and without spatial clustering) out performs [4] and [7] obtaining a considerable gain both in terms of rotational and scaling accuracy. Moreover, the performance of our approach significantly improves with the increasing of the extracted feature points (SIFT).

A good gain in terms of performance is also obtained with respect to the scale factor (Table V).

TABLE VI
PERCENTAGE OF UNMATCHED IMAGES OBTAINED THROUGH MALICIOUS MANIPULATION



	Unmatched Images			
Number of SIFT	**15**	**30**	**45**	**60**
Lu et al. [7]	90.50%	87.71%	81.01%	73.74%
Battiato et al. [4]	68.72%	54.19%	29.61%	9.50%
Proposed approach without spatial clustering	87.15%	86.03%	74.86%	64.25%
Proposed approach with spatial clustering	0%	0%	0%	0%

TableVI shows the percentage of malicious manipulated images that cannot be considered by the different approaches (i.e., there are no matchings between and), whereas Tables VII and VIII report the results obtained y the different approaches on the malicious manipulated images have been found.

TABLE VII
AVERAGE ROTATIONAL ERROR ON IMAGES OBTAINED THROUGH MALICIOUS MANIPULATION

	Mean Error α			
Number of SIFT	**15**	**30**	**45**	**60**
Lu et al. [7]	85.6844	79.9884	88.4555	97.4700
Battiato et al. [4]	86.9447	92.0451	92.5144	91.8478
Proposed approach without spatial clustering	35.6087	33.6800	42.5111	38.5156
Proposed approach with spatial clustering	1.2458	0.0000	0.0000	0.0000

In Table IX the different approaches are compared taking into account only the images on which all the approaches are able to find matchings The results demonstrate that robustness can be obtained embedding spatial information during the selection of the features to be used as a signature for the alignment component. The embedded spatial information helps to deal with tampered images obtained by adding patches containing a highly texturized and contrasted pattern.

A novel test dataset has been hence built by using (16) and (17) for shear and (18) and (19) for the anisotropic scale (see Table XI). As reported in Tables XII and XIII the accuracy of the proposed affine solution, although dependent on the degree of the affine warping, can be considered satisfactory. Finally, the results obtained with the affine model by considering the dataset containing all the transformation in Tables I and XI are reported in Table XIV. The obtained results confirm the effectiveness of the proposed approach.

TABLE XI
IMAGE TRANSFORMATIONS

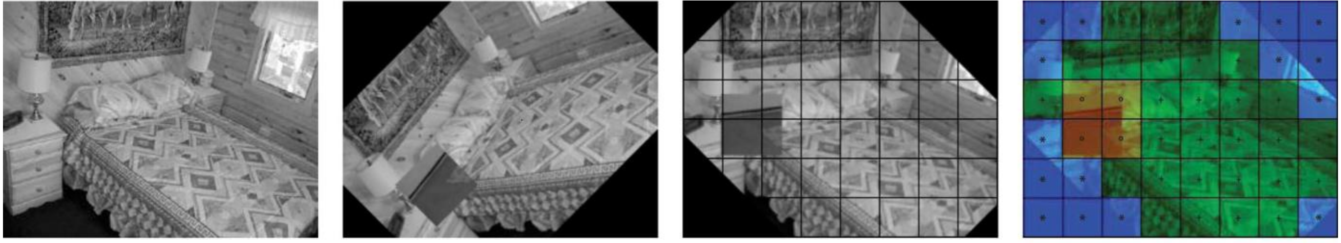
Operations	**Parameters**
Anisotropic Scaling (σ_x or σ_y)	0.7, 0.9, 1.2
Shear (k)	0.05, 0.1, 0.15

TABLE XIV
AVERAGE ERRORS OBTAINED BY PROPOSED SOLUTION BASED ON AFFINE MODEL. SIXTY SIFT HAVE BEEN CONSIDERED IN IMA HASH GENERATION PROCESS

Proposed approach with spatial clustering and affine estimation	
Unmatched	0.0824
Mean Error α	0.2093
Mean Error σ_x	0.0109
Mean Error σ_y	0.0069
Mean Error k	0.0274
Mean Error T_x	1.2210
Mean Error T_y	1.2742

V. CONCLUSION

The main contribution of this paper is related to the alignment of images in the context of distributed forensic systems. A strong image registration component which exploits an image signature based on the BOF paradigm has been introduced. The proposed hash encodes the spatial distribution of features to better deal with highly texturized and contrasted tampering patches. Moreover, a non-uniform quantization of histograms of oriented gradients is exploited to perform tampering localization. The proposed framework has been experimentally tested on a representative dataset of scenes. Comparative tests show that the proposed approach out performs recently appeared techniques by obtaining a significant margin in terms of registration accuracy, discriminative performances and tampering detection. Future works should concern a more in-depth analysis to establish the minimal number of SIFT needed to guarantee an accurate estimation of the geometric transformations and a study in terms of bits needed to represent the overall image signature.



(a) Original image. (b) Tampered image. (c) Image registration. (d) Tampering localization

Fig. 9. Example of proposed tampering detection workflow. In (d) orange indicates recognized tampered blocks, whereas green indicates blocks detected as not tampered. Blue indicates image blocks falling on border of images after registration. The 32 grid in (c) and (d) has been over imposed just for visual assessment. This result has been obtained employing alignment with spatial clustering and non-uniform quantization for tampering detection. (a) Original image. (b) Tampered image. (c) Image registration. (d) Tampering localization.

ACKNOWLEDGEMENTS

I would like to thank all the authors.

REFERENCES

Journal Papers:

[1] Photo tampering throughout history [Online]. Available: www.cs.dartmouth.edu/farid/research/digitaltampering/

[2] H. Farid, “Digital doctoring: How to tell the real from the fake,” Significance,vol. 3, no. 4, pp. 162–166, 2006.

[3] S. Battiato, G.M. Farinella, E.Messina, and G. Puglisi, “Robust image registration and tampering localization exploiting bag of features based forensic signature,” in Proc. ACM Multimedia (MM’11), 2011.

[4] S. Battiato, G. M. Farinella, E. Messina, and G. Puglisi, “Understanding geometric manipulations of images through BOVW-based hashing,” in Proc. Int. Workshop Content Protection Forensics (CPAF 2011), 2011.

[5] Y.-C. Lin, D. Varodayan, and B. Girod, “Image authentication based on distributed source coding,” in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2007, pp. 3–8.

[6] W. Lu, A. L. Varna, and M. Wu, “Forensic hash for multimedia information,” in Proc. SPIE Electronic Imaging Symp.—Media Forensics Security, 2010.

[7] W. Lu and M.Wu, “Multimedia forensic hash based on visual words,” in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2010, pp. 989–992.

[8] S. Roy and Q. Sun, “Robust hash for detecting and localizing image tampering,” in Proc. IEEE Computer Soc. Int. Conf. Image Processing, 2007, pp. 117–120.

[9] N. Khanna, A. Roca, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Improvements on image authentication and recovery using distributed source coding,” in Proc. SPIE Conf. Media Forensics Security, 2009, vol. 7254, p. 725415.

[10] Y.-C. Lin, D. P. Varodayan, and B. Girod, “Didstributed source coding authentication of images with affine warping,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing (ICASSP 2009), 2009, pp. 1481–1484.

[11] M. Irani and P. Anandan, “About direct methods,” in Proc. Int. Workshop Vision Algorithms, held during ICCV, Corfu, Greece, 1999, pp. 267–277.

[12] P. H. S. Torr and A. Zisserman, “Feature based methods for structure and motion estimation,” in Proc. Int.Workshop Vision Algorithms, held during ICCV, Corfu, Greece, 1999, pp. 278–294.

[13] R. Szeliski, “Image alignment and stitching: A tutorial,” Foundations Trends in Computer Graphics Computer Vision, vol. 2, no. 1, pp. 1–104, 2006.

[14] S. Battiato and G. Messina, “Digital forgery estimation into DCT domain— Acritical analysis,” in Proc. ACMConf.Multimedia 2009, Multimedia in Forensics (MiFor’09), 2009.

[15] G. Csurka, C. R. Dance, L. Fan, J. Willamowski, and C. Bray, “Visual categorization with bags of keypoints,” in Proc. ECCV Int. Workshop Statistical Learning Computer Vision, 2004.

[16] G. Puglisi and S. Battiato, “A robust image alignment algorithm for video stabilization purposes,” IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 10, pp. 1390–1400, 2011.

[17] D. G. Lowe, “Distinctive image features from scale-invariant keypoints,” Int. J. Computer Vision, vol. 60, no. 2, pp. 91–110, 2004. L. Shapiro and G. Stockman, Computer Vision. Upper Saddle River, NJ: Prentice-Hall, 2001.

[18] M. Brown, R. Szeliski, and S. Winder, “Multi-image matching using multi-scale oriented patches,” in Proc. IEEE Conf. Computer Vision Pattern Recognition, 2005, vol. 1, pp. 510–517.

[19] L. Gruber, S. Zollmann, D.Wagner, D. Schmalstieg, and T. Hollerer, “Optimization of target objects for natural feature tracking,” in Proc. 20th Int. Conf. Pattern Recognition (ICPR 2010), Washington, DC,2010, pp. 3607–3610.

[21] S. Gauglitz, L. Foschini, M. Turk, and T. Hllerer, “Efficiently selecting spatially distributed keypoints for visual tracking,” in Proc. IEEE Int.Conf. Image Processing (ICIP 2011), 2011.

[22] S. Lazebnik, C. Schmid, and J. Ponce, “Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories,” in Proc. IEEE Computer Soc. Conf. Computer Vision Pattern Recognition, 2006, pp. 2169–2178.

[23] J. Bi and K. P. Bennett, “Regression error characteristic curves,” in Proc. Int. Conf. Machine Learning, 2003, pp. 43–50.

[24] S.Maji, A. Berg, and J.Malik, “Classification using intersection kernel support vector machines is efficient,” in Proc. IEEE Int. Conf. Computer Vision Pattern Recognition, 2008, pp. 1–8.