Robust Mesh-based Hashing for Copy Detection and Tracing of Images

Chun-Shien Lu[†*], Chao-Yong Hsu[†], Shih-Wei Sun[‡], Pao-Chi Chang[‡]

[†] Institute of Information Science, Academia Sinica
Taipei, Taiwan 115, ROC
[‡] Dept. of Electrical Engineering, National Central University
Chung-Li, Taiwan 320, ROC
[*] Email: lcs@iis.sinica.edu.tw

***Abstract*— Due to the desired non-invasive property, non-data hiding (called media hashing here) is considered to be an alternative to achieve many applications previously accomplished with watermarking. Recently, media hashing techniques for content identification have been gradually emerging. However, none of them are really resistant against geometrical attacks. In this paper, our aim is to propose a geometry-invariant image hashing scheme, which can be employed for content copy detection and tracing. Our system is mainly composed of three components: (i) robust mesh extraction; (ii) mesh-based robust hash extraction; and (iii) hash matching for similarity measurement. Exhaustive experimental results obtained from benchmark attacks have confirmed the performance of the proposed method.**

I. Introduction

MEDIA hashing techniques have attracted much attention in content management recently due to its non-invasive property. Analogous to media hashing, there exists some synonymous terminologies including fingerprinting, digital signature, and passive/non-invasive watermarking. Their applications are mainly complimentary to copyright protection of watermarking. The major difference that distinguishes media hashing from watermarking is that the former measures similarity while the latter measures originality. Besides, media hashing is also different from media retrieval in that media hashing is required to resist (either malicious or incidental) attacks.

The previous works on media hashing will be discussed as follows. In 1998, Chang *et al.* proposed a wavelet-based Replicated IMage dEtector (RIME) [2] to search unauthorized image copying on the Internet. Regrettably, their system's capability is remarkably prohibited from resisting extensive geometrical distortions. In [7], [8], digital signature has been proposed for image authentication. Lin and Chang [7] created the mutual relationship of pairwise block-DCT coefficients to distinguish JPEG compressions from malicious modifications. Lu and Liao [8] built the so-called structural digital signature from the multiscale structure of wavelet transform to tolerate incidental manipulations and reflect intentional manipulations. However, the ability of resisting geometrical manipulations was a lack of [7], [8]. In [3], Fridrich and Goljan proposed a robust/visual hashing method. Their hash digests of digital images were created by projections of DCT coefficients to key-dependent random patterns. In [11], Venkatesan *et al.* proposed an image hashing technique, which contained (i) dividing a wavelet transformed image into tiles; (ii) extracting the statistical features of tiles as hashes. However, the two methods [3], [11] only allows limited resistance to geometrical distortions. In [6], Lefebvre and Macq developed a soft hash algorithm based on Radon transform and principal component analysis. Again, resistance to geometrical modifications depends on the limited invariance property of Radon transform. Kim proposed an image copy detection scheme [5] by means of ordinal measures of AC coefficients in the 8×8 DCT domain, i.e., the magnitudes of AC coefficients in a block were ranked in descending order to represent an image. Extensive signal processing attacks were conducted to test the robustness and discrimination in a large database. However, this system basically cannot resist geometrical distortions.

It is obvious from the above discussions that the major disadvantage of the existing image hashing techniques is their limited robustness against geometrical distortions (For instance, resistance to rotations is restricted to very small angles). The main cause lies in the fact that the previous methods did not really deal with the problem of resisting geometrical attacks. Consequently, the purpose of this paper aims to treat this challenging problem seriously. We shall propose a robust mesh-based image hashing scheme for content copy detection, identification, and tracing in a large database. Our major contribution is to achieve robustness against extensive geometrical distortions (e.g., Stirmark3.1 and Stirmark4.0 [9], [10]). Although the concept of image meshing has been applied to watermarking [1], we have taken notice of the stability of mesh extraction that is closely related to the success of intended purposes. In view of this, we have presented a robust mesh extraction method such that it won't be easily harmful to mesh-based hashing and matching. Under this circumstance, the robustness of mesh-based hashing could be mostly guaranteed. Extensive results obtained from benchmark attacks have further confirmed the performance of the proposed scheme.

0-7803-8603-5/04/$20.00

II. The Proposed Scheme

The block diagrams of the proposed mesh-based image hashing system and image query system are depicted in Fig. 1 and Fig. 2, respectively. The major components will be described in the remaining paper.

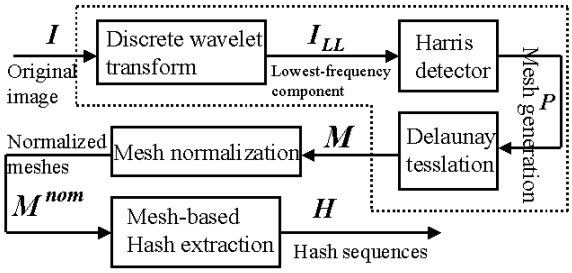

Fig. 1. Block diagram of the proposed mesh-based image hashing system.

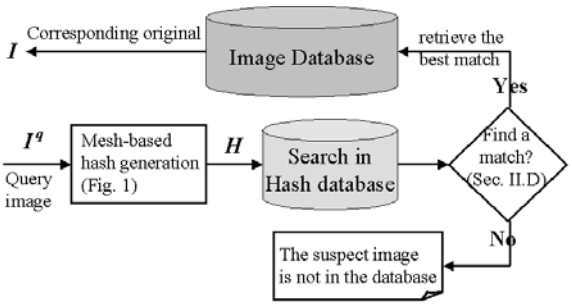

Fig. 2. Block diagram of the proposed image query system: a query enters into the hash database for possible retrieval of its original from the image database.

A. Robust Image Mesh Generation

Extraction of robust meshes plays an important role in our method since it is a prerequisite in resisting geometrical distortions. To generate meshes, the first step is to detect salient points of an image. Among the ubiquitous feature point extraction methods, Harris detector has been popularly used. However, the original Harris detector is still not robust enough to be used for our purposes. Thus, we propose to improve its robustness by carrying out it in the lowest-frequency subband of the discrete wavelet transform (DWT) domain. Our intention is to filter out noisy points before salient point detection.

Once the feature point extraction process is finished, the Delaunay tessellation can be used to decompose the image into a set of disjointed triangles. Each triangle (called a mesh hereafter) is regarded as the minimum unit for robust hash extraction. The overall mesh generation process is summarized as follows: (i) the original image $\mathbf{I}$ is discrete wavelet transformed to obtain the lowest-frequency subband signal, $\mathbf{I}_{LL}$; (ii) the set of feature points $\mathcal{P}$ are generated by means of applying the Harris detector on $\mathbf{I}_{LL}$; and (iii) Delaunay tessellation is performed using $\mathcal{P}$ to obtain a set of meshes $\mathcal{M}$.

An example of mesh extraction is shown in Fig. 3, which contains the generated meshes from the original Lenna and its Stirmark attacked Lenna images. By visual inspection, we can find that several meshes are consistently extracted. These results validate the effectiveness of mesh extraction from the lowest-frequency subband of an image.

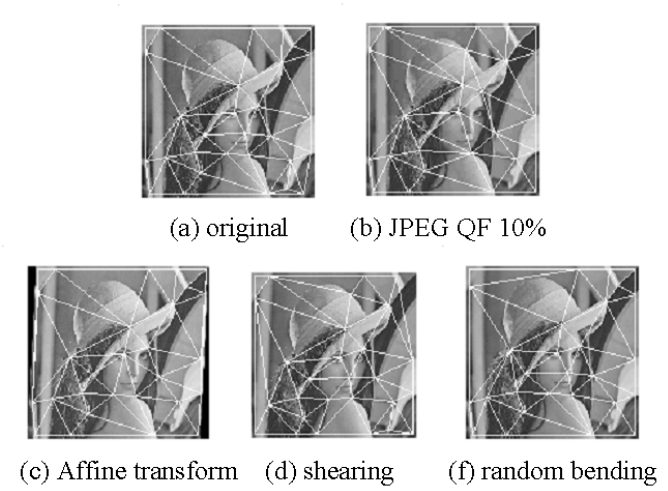

Fig. 3. Illustration of extracted meshes from original and attacked Lenna images (Initially, they are color.). Note that the meshes are detected at the lowest-frequency subband of an image after two-level wavelet decomposition.

B. Mesh Normalization

Once the set of meshes in an image has been produced, each original mesh $\mathbf{M_k}(\in \mathcal{M})$ will be normalized as $\mathbf{M_k^{nom}}$ to generate a mesh-based hash $\mathbf{H_k}$, where $\mathbf{M_k^{nom}}$ is a right-angled isosceles triangle with the size of 32×32. The aim of normalization is to maintain that all hashes are of the same size for efficient hash comparison. The normalization process is conducted by warpping $\mathbf{M_k}$ into $\mathbf{M_k^{nom}}$ through the processes of affine transform and interpolation.

C. Robust Mesh-based Hashing

Image hashing attempts to transfer an image content to a short sequence while preserving distinguishable features in order to facilitate similarity measurement. In this paper, for each normalized mesh $\mathbf{M_k^{nom}}$ its robust hash is extracted in the 8×8 block-DCT domain. First, each triangle $\mathbf{M_k^{nom}}$ is flipped and padded with its flipped version to form a 32×32 block, as illustrated in Fig. 4. For a pair of blocks, a hash bit, defined as the magnitude relationship between two AC coefficients, is represented as follows:

$$H_k(s) = \begin{cases} 1, & \text{if } |f_i(p_1)| - |f_j(p_2)| \geq 0, \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

where $H_k(\cdot)$ is a robust feature value in a hash sequence $\mathbf{H_k}$, and $f_i(p_1)$ and $f_j(p_2)$ are two AC coefficients at positions p_1 and p_2 in 8×8 blocks i and j, respectively. The DC coefficient will not be selected because it is not helpful in identification.

In addition, the two selected AC coefficients should be at lower frequencies because high-frequency coefficients are vulnerable to attacks. In this paper, p_1 and p_2 are selected to be the first two largest AC coefficients from the 64 available frequency subbands. We call this feature value $H_k(\cdot)$ robust because this magnitude relationship between $f_i(p_1)$ and $f_j(p_2)$ can be mostly preserved under incidental modifications. Please refer to [8] for similar robustness analyses. It should be noted that we don't adopt statistical features (e.g., mean, variance, ...) because they are easy to raise the collision problem.

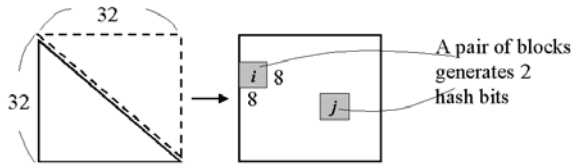

Fig. 4. Mesh padding for hash extraction in the block-DCT domain.

According to Eq. (1), there are two hash bits generated from a pair of blocks. Therefore, there are in total $2\mathcal{C}\begin{pmatrix}(\frac{32}{8})^2\\2\end{pmatrix} = 240 = |\mathbf{H_k}|$ hash bits for a normalized mesh $\mathbf{M_k^{nom}}$.

D. Mesh-based Matching Metric

In the applications of content copy detection and tracing, two images ($\mathbf{I_1}$ and $\mathbf{I_2}$) are determined to be similar if there are at least N pairs of meshes matched. It is said that a pair of meshes is matched if the bit error rate (BER) between their corresponding hashes is smaller than a threshold T ($0 \le T \le 1$), i.e.,

$$BER(\mathbf{H_i^{I_1}}, \mathbf{H_j^{I_2}}) = \frac{\sharp\{t | H_i^{I_1}(t) \neq H_j^{I_2}(t)\}}{|\mathbf{H_i^{I_1}}|} < T, \quad (2)$$

where $H_i^{I_1}(t)$ denotes the t-th element of the i-th hash in $\mathbf{I_1}$ and $\sharp\{\}$ denotes number of bit errors.

III. Experimental Results

In this paper, two major experiments were conducted to demonstrate the performance of the proposed mesh-based image hashing and query system.

A. Robustness: Resistance to Attacks

First, eight color images with different properties ($\mathbf{I_1}$: Pepper, $\mathbf{I_2}$: Lenna, $\mathbf{I_3}$: Bridge, $\mathbf{I_4}$: Sailboat, $\mathbf{I_5}$: Goldhill, $\mathbf{I_6}$: F16, $\mathbf{I_7}$: Baboon, and $\mathbf{I_8}$: Clock) were used to verify the robustness of our scheme to two Stirmark benchmarks (versions 3.1 and 4.0). Please refer to [9], [10] for more detailed parameters of Stirmark. In this test, the original image was used as a query to find out how many modified versions could be successfully detected. The results of robustness verification are summarized in Tables I and II, respectively. In the two tables, each attack's name is followed by a digit, which indicates the number of times that the attack was performed with different parameters. Besides, each field indicates the number of modified images that have been successfully identified. Here, $N = 3$ and $T = 0.25$, as explained in Sec. II-D, were adopted. It can be observed that most modified images could be successfully detected except for some exceptions. Several attacked images (obtained from Stirmark 4.0) that were failed to be identified are shown in Fig. 5 for visual inspections. We can observe from Fig. 5 that it is still not easy to correctly extract the meshes from the attacked images involving remarkably degraded fidelities and content eliminations. In particular, severe cropping and heavy noise adding are efficient in breaking the connectivities of meshes and thereby affect the hashes to defeat our system even the attacked images have lost their commercial value. However, compared with the existing methods [2], [3], [5], [6], [11], it is evident that our scheme indeed achieves promising resistance to extensive geometrical distortions.

In practice, few non-geometrical attacked images (e.g., added with heavy noises) that are not well detected in the above two tables are due to the destruction of meshes. Thus, the non-geometrical hashes can be additionally appended to the current hashes (and thereby increase the length of an image hash sequence) in order to thoroughly overcome various attacks.

TABLE I

Robustness of our scheme vs. Stirmark 3.1: attacks are denoted as SPA: Signal Processing Attack including median filtering, Gaussian filtering, sharpening, and Frequency Mode Laplacian Removal (FMLR); JPEG: compression with quality factors, $90\% \sim 10\%$; GLGT: General Linear Geometric Transform; CAR: Change of the Aspect Ratio; LR: Line Removal; RC: Rotation+Cropping; Scaling: with factors ranging from 0.5 to 2.0; RRS: Rotation+ReScaling; RB: Random Bending.

Stirmark 3.1	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	$\mathbf{I_7}$	$\mathbf{I_8}$
SPA (6)	6	6	6	6	6	6	6	6
JPEG (12)	12	12	12	12	12	12	12	12
GLGT (3)	3	3	3	3	3	3	3	3
Flipping (1)	1	1	1	1	1	1	1	1
CAR (8)	7	7	8	8	8	8	7	8
LR (5)	5	5	5	5	5	5	5	5
Cropping (9)	6	6	7	7	8	7	5	6
RC (16)	13	13	15	14	15	15	11	14
Scaling (6)	5	3	3	4	5	3	3	6
RRS (16)	16	13	14	15	14	14	11	12
Shearing (6)	6	6	6	6	6	6	6	6
RB (1)	1	1	1	1	1	1	1	1

B. Identification: Searching in a Large Database

The second part of our experiments was related to a retrieval problem in a large image database. In this searching system, the database is composed of the so-called original color images (which is composed of the Corel image database that contains 20000 images and ten traditional images such as Lenna, Baboon,

TABLE II

Robustness of our scheme vs. Stirmark 4.0: attacks are denoted as AffineTrans: Affine Transformation; ConvFilter: Convolution Filtering; Cropping: cropped into $\frac{3}{4}$, $\frac{1}{2}$, $\frac{1}{4}$, and $\frac{1}{5}$ sizes; JPEG: with quality factors, $90\% \sim 10\%$; MF: Median Filtering; Noise: noise adding; Scaling: with factors ranging from 0.5 to 2.0; RML: Removing Lines; PSNR: all pixel values added with the same quantity; and RC: Rotation+Cropping.

Stirmark 4.0	$\mathbf{I_1}$	$\mathbf{I_2}$	$\mathbf{I_3}$	$\mathbf{I_4}$	$\mathbf{I_5}$	$\mathbf{I_6}$	$\mathbf{I_7}$	$\mathbf{I_8}$
AffineTrans (8)	8	8	8	8	8	8	8	8
ConvFilter (2)	2	2	2	2	1	1	0	1
Cropping (4)	2	0	1	1	2	1	0	1
JPEG (12)	12	12	12	12	12	12	12	12
MF (4)	4	4	4	4	4	4	3	4
Noise (6)	1	2	2	2	2	2	1	1
Scaling (6)	4	2	3	3	5	4	3	5
RML (10)	10	10	10	10	10	10	10	10
Rotation (17)	17	17	17	17	17	17	14	17
PSNR (11)	11	11	11	11	11	11	11	11
RC (14)	14	14	14	14	14	14	14	14

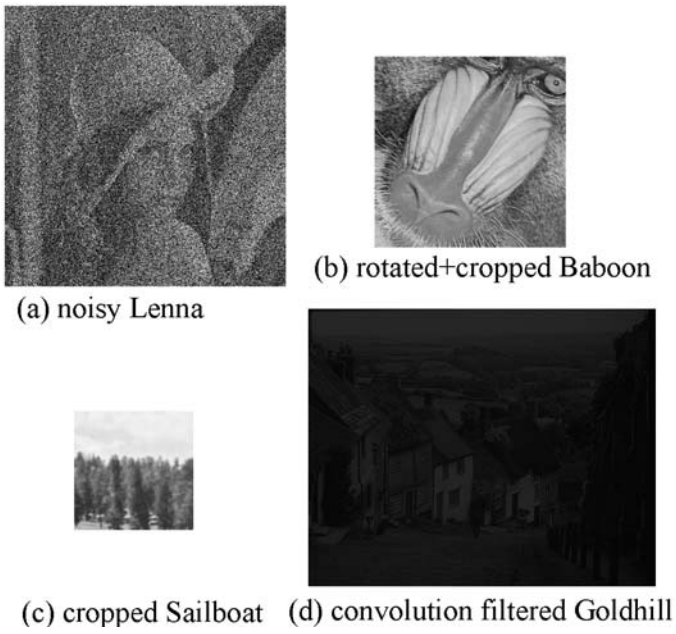

Fig. 5. Examples of failed identification.

..., etc.) while the query image is suspect in the sense that it may be a modified version generated from our database. We have used the attacked images, obtained from Stirmark 3.1 and 4.0, as queries of the database. In this test, it is said that a match is found if the detection condition is defined as the one that at least $N = 3$ pairs of meshes are found to have BERs lower than $T = 0.25$. By means of our method, among 1830 query images 1657 originals could be correctly identified (i.e., rank one) while none was falsely identified. This implies that the miss detection rate is 9.5% and the false alarm rate is 0%. Basically, these results reveal that the desired originals are hard to be identified for those query images (e.g., Fig. 5) that have been severely modified. Besides, the miss detected queries are nearly consistent with those of failed identification in the robustness test. One thing deserves to be mentioned is that no false detection occurs under the employed matching thresholds.

IV. Conclusions

A robust mesh-based image hashing scheme has been proposed in this paper for content management of digital images. Our system is mainly composed of three components including (i) robust mesh extraction; (ii) mesh-based robust hash extraction; and (iii) hash similarity measurement. The major contribution of our system is to significantly improve the resistance of image hashing to geometrical distortions over the existing methods. We have also demonstrated the use of the robust mesh-based image hashing system for content copy detection/tracing in a large database.

Some directions that are worth of further researching are identified as follows. First, robust identification of small images is still a challenging problem because it is not robust enough to extract mesh-based hashes from small regions. Fortunately, precious images are usually with large sizes and only attacked images can be of small sizes (may lose their commercial value). Second, although the creation of a hash database can be done in an off-line manner, the matching process within a large database should be further speeded up. Currently, we have not employed any sophisticated skill in this task. Thirdly, as mentioned in [4] secure compression of a hash sequence is an important issue that needs further studying. Finally, it is also interesting to realize the impact of different parameters (Sec. II-D) on the miss detection and false alarm rates.

References

[1] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Processing*, Vol. 11, pp. 1014-1028, 2002.

[2] E. Y. Chang, J. Z. Wang, C. Li, and G. Wiederhold, "RIME: A Replicated Image Detector for the World-Wide-Web," *Proc. SPIE: Multimedia Storage and Archiving Systems*, Vol. III, 1998.

[3] J. Fridrich, "Visual Hash for Oblivious Watermarking," *Proc. SPIE: Security and Watermarking of Multimedia Contents II*, 2000.

[4] M. Johnson and K. Ramchandran, "Dither-based Secure Image Hashing Using Distributed Coding," *Proc. IEEE Int. Conf. on Image Proc.*, 2003.

[5] C. Kim, "Content-based Image Copy Detection," *Signal Processing: Image Communication*, Vol. 18, pp. 169-184, 2003.

[6] F. Lefebvre, J. Czyz, and B. Macq, "A Robust Soft Hash Algorithm for Digital Image Signature," *Proc. IEEE Int. Conf. on Image Proc.*, 2003.

[7] C. Y. Lin and S. F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation", *IEEE Trans. on Circuits and Systems for Video Tech.*, Vol. 11, No. 2, pp. 153-168, 2001.

[8] C. S. Lu and H. Y. Mark Liao, "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme," *IEEE Trans. on Multimedia*, Vol. 5, No. 2, pp. 161-173, 2003.

[9] F. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on Copyright Marking Systems", *Proc. Int. Workshop on Information Hiding*, LNCS 1575, pp. 219-239, 1998.

[10] F. Petitcolas, "Watermarking Schemes Evaluation," *IEEE Signal Processing Magazine*, Vol. 17, No. 5, pp. 58-64, 2000.

[11] R. Venkatesan, S. M. Koon, M. H. Jakubowski, and P. Moulin, "Robust Image Hashing," *Proc. IEEE Int. Conf. Image Processing*, 2000.