HAL
open science

A Novel Secure Image Hashing Based on Reversible Watermarking for Forensic Analysis

Munkhbaatar Doyoddorj, Kyung-Hyune Rhee

To cite this version:

Munkhbaatar Doyoddorj, Kyung-Hyune Rhee. A Novel Secure Image Hashing Based on Reversible Watermarking for Forensic Analysis. 1st Availability, Reliability and Security (CD-ARES), Aug 2011, Vienna, Austria. pp.286-294, 10.1007/978-3-642-23300-5_22 . hal-01590409

HAL Id: hal-01590409

https://inria.hal.science/hal-01590409v1

Submitted on 19 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A Novel Secure Image Hashing based on Reversible Watermarking for Forensic Analysis

Munkhbaatar Doyoddorj [1], Kyung-Hyune Rhee [2]

[1] Dept. of Information Security, Pukyong National University,
[2] Dept. of IT Convergence and Application Engineering, Pukyong National University,
Busan, Republic of Korea
{d_mbtr, khrhee}@pknu.ac.kr

Abstract. Nowadays, digital images and videos have become increasingly popular over the Internet and bring great social impact to a wide audience. In the meanwhile, technology advancement allows people to easily alter the content of digital multimedia and brings serious concern on the trustworthiness of online multimedia information. In this paper, we propose a new framework for multimedia forensics by using compact side information based on reversible watermarking to reconstruct the processing history of a multimedia data. Particularly, we focus on a secure reversible watermarking to make the image hash more secure and robust. Moreover, we introduce an algorithm based on Radon transform and scale space theory to effectively estimate the parameters of geometric transforms and to detect local tampering. The experimental results show that the quality of the embedded image is very high and the positions of the tampered parts are identified correctly.

Keywords: Secure Image hashing, Radon transform, Reversible Watermarking, Forensic Analysis.

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 heterogeneous environment such as peer-to-peer and wireless networks to deliver content rich audio-visual data.

However, the digital nature of multimedia data and the advancement of multimedia processing technologies have made it easy to modify the digital content. Multimedia data can be intentionally altered to create a forgery and convey a different meaning. For example, objects can be removed from or inserted into an image, and multiple pieces of content may be combined into new creation. As such, it is critical to evaluate the trustworthiness of multimedia information and reveal its complete processing history in order to achieve better decision and usage of online multimedia information. Forensic hash is a short signature attached to an image before transmission and acts as side information for analyzing the processing history and trustworthiness of the received image.

There are two traditional techniques to evaluate image trustworthiness and authenticity, namely, robust image hashing [1-2] and blind multimedia forensics [3].

Robust image hashing is an extension from traditional cryptography hash. A cryptography hash is used to evaluate authenticity of text or binary data and is sensitive to a single bit difference, while image hash is designed to evaluate similarity between visually similar images that may have undergone some allowable operations but sensitive against malicious tampering. The distance between two image hashes is compared with a threshold to determine whether the received image is authentic.

The research objective of multimedia forensics is to provide tools for analyzing the origin, processing history, and trustworthiness of multimedia information. Recent research in multimedia forensics can determine whether a received image or 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. Thus, it is difficult to trace history of some operations such as cropping and rotation without any side information about the original image. Many signal statistics and traces left by image operations may be removed or altered by further post-processing. A considerable amount of computational complexity is also involved in most blind forensic analyses.

1.1 Background and Organization

Conventional image hashing only provides a binary authentication answer using simple distance comparison, and non-intrusive blind forensics techniques have limitations in terms of the scope of questions that can be answered and the computational complexity. We use the FASHION (**F**orensic h**ash** for informat**ion** assurance) framework to bridge these two research areas and combine their benefits. The FASHION [8] framework uses side information called forensic hash to assist forensic analysis. The relation between two other research areas is shown in Figure 1.

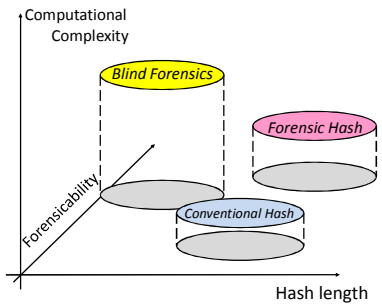

Fig. 1. Forensic hash as compared to image hashing and blind forensics

In this paper, in order to achieve a good accuracy performance as well as ensuring the security of image features, we propose a novel secure image hashing based on FASHION for forensic analysis by using side information captured in a secure hash

representation. Combined construction of two forensic analyses can provide robust estimation of geometric transform such as rotation and scaling.

The rest of this paper is organized as follows: Section 2 provides the requirements of reversible embedding method; the backgrounds of Radon transform and scale space theories are described. In Section 3, the proposed scheme of a new secure image hashing based on FASHION model is introduced in detail. Section 4 introduces a detection and localization of image tampering. Experimental results are presented and analyzed in Section 5. Finally, we conclude the paper in Section 6.

2 Preliminaries

2.1 Reversible Data Embedding by using Difference Expansion

This method can be applied to digital image, audio and video as well that employs an integer wavelet transform to losslessly remove redundancy in a digital image to allocate space for watermark embedding [4]. One basic requirement of digital watermarking is its imperceptibility, embedding a watermark will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military and medical data. In such scenario, every bit of information is important for forensic analysis.

Let's assume a sequence of pairs of grayscale values $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$, where $x_i, y_i \in \mathbf{Z}$, $0 \le x_i, y_i \le 255$, $1 \le i \le n$. We can embed the payload $b = \{b_1, b_2, \cdots, b_n\}$, where $b_i \in \{0, 1\}$, $1 \le i \le n$, by repeating the above process,

$$l_i = \left\lceil \frac{x_i + y_i}{2} \right\rceil, \qquad h_i = x_i - y_i, \qquad 1 \le i \le n.$$

For each difference number h_i, whose binary representation as:

$$h_i = r_{i,0}\, r_{i,1} \cdots r_{i,j(i)},$$

where $r_{i,o} = 1$, is the MSB, $r_{i,m} \in \{0,1\}$, for $1 \le m \le j(i)$, with $j(i) + 1$ as the bit length of h_i in its binary representation. Then we could embed b_i into h_i by

$$h'_i = r_{i,0}\, \boldsymbol{b_i}\, r_{i,1} \cdots r_{i,j(i)}.$$

Finally, we compute the grayscale values, based on the new difference number h_i and original average number l,

$$x' = l + \left\lceil \frac{h' + 1}{2} \right\rceil, \qquad y' = x' - h', \quad 1 \le i \le n.$$

From embedded pair (x', y'), the watermark detector (or authenticator) can extract the embedded bit b and get back the original pair (x, y) by a similar process as the embedding.

2.2 Radon Transform and Scale Space Theory

The radon transform [5] of a two-dimensional function $I(x, y)$ is defined as

$$R(\rho, \theta) = \int_{\infty}^{\infty} \int_{\infty}^{\infty} I(x, y)\delta(\rho - x\cos\theta - y\sin\theta)\, dxdy \quad (1)$$

The Radon transform has useful properties about rotation and scaling as outlined in equation (2)-(3).
Rotation by $\emptyset$:

$$I(\rho, \theta)\{I(x\cos\theta + y\sin\theta\,, -x\cos\theta + y\sin\theta)\} = R(\rho, \theta + \emptyset) \quad (2)$$

Scaling:

$$I(\rho, \theta)\left\{I\frac{x}{s}, \frac{y}{s}\right\} = sR(\frac{\rho}{s}, \theta) \quad (3)$$

Here, $R(\rho, \theta)$ is the Radon transform of $I(x, y)$, s is the scaling factor and $\emptyset$ is the rotation angle.

Radon transform is a line integral of an image alone certain directions. Such line integral captures salient information about the image alone particular directions, and is robust to small variations in the image content, which may come from noise, moderate cropping, local tampering, and content preserving operations. We use a compact summarization along the orientation axis in the transform domain for rotation estimation and use scale space theory to identify scale-resilient features along projections at different directions for scaling estimation.

Rotation Estimation. The direction of image edges can reveal information about image orientation. Given test image $I'(x, y)$ is obtained from original image $I(x, y)$ by rotating α degrees. First, we compute its edge map $E'(x, y)$. Radon transform is then applied to the edge map. $R_{E'}(\rho, \theta) = R_E(\rho, \theta + \alpha)$. Thus, in the transform domain, rotation becomes a shift along the angle axis. This property of Radon transform has been exploited in the image registration and authentication literature, where a 1-D summarization of Radon transform along the angle axis is used to estimate the rotation angle. Accordingly, 1-D summarization is derived as $m'(\theta) = max_{\rho}\left(R_{E'}(\rho, \theta)\right)$. For representation, quantization and sub-sampling are applied to $m'(\theta)$. Since down-sampling may cause aliasing, we first pass the signal $m'(\theta)$ through a low-pass filter $f(\cdot)$ to obtain $\widehat{m}'(\theta) = f(m'(\theta))$. If n-byte alignment component is desired, we downsample the signal $\widehat{m}'(\theta)$ to obtain the image hash $h'(\emptyset) = \{h'(1), \ldots, h'(n)\}$ with

$$h'(i) = \widehat{m}'(\left[(i-1)\cdot\frac{180}{n}\right] + \emptyset), \qquad \emptyset \in \{0, 1, \ldots, 179\}.$$

To further compress the image hash, we can store only the rank order information of h, $rank(h) = \{r(1), \ldots, r(n)\}$, where $r(i) \in \{1, \ldots n\}$ is the rank of $h(i)$. h is recovered SIFT (Scale-Invariant Feature Transform) features from image hash in each block of the original image I.

Our defined $h'(\emptyset)$ of I', its rank order information is denoted by $rank(h'(\emptyset)) = \{r'(1), \dots, r'(n)\}$. The shift amount that minimizes the L distance between $rank(h)$ and $rank(h'(\emptyset))$ will be estimated rotation angle between two images I and I'.

$$\alpha = argmin \sum_{i=1}^{n} |r(i) - r'(i + \emptyset)|, \qquad \emptyset \in \{0, 1, \dots, 179\}.$$

The rotation estimation using rank order information gives comparable performance to estimation using cross-correlation, and a proper fusion of the two similarity metrics can lead to even better estimation accuracy.

Scaling estimation. Scale space theory [6] is a technique for analyzing signals at different scales, which makes it useful for automatic scale selection and scale invariant image analysis. Given projection $f'(\rho) = s \cdot f(s \cdot \rho)$ of the scaled image, we generate its scale space representation $L(\rho; t)$ by convolving $f'(\rho)$ with a 1-D discrete Gaussian filter $g(\rho; t)$ at scale t:

$$L(\rho; t) = g(\rho; t) * f'(\rho), \text{ where } \; g(\rho; t) = \frac{1}{\sqrt{2\pi t}} e^{-\rho^2/(2t)}$$

The scale space representation is a 2-D 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.

Given the extrema positions of the two signals $f(\rho)$ and $f'(\rho) = s \cdot f(s \cdot \rho)$, we randomly choose two extrema x, y from $f(\rho)$ and two extrema x', y' from $f'(\rho)$. An estimate $\hat{s}$ of the true scaling factor s is given by the ratio of $|x' - y'|/|x - y|$.
By computing the Radon projections of the original image along both the vertical and horizontal directions, we can obtain the scaling factors along these two directions using the above method.

3 Proposed Approach

We proposed a secure image hashing based on reversible watermarking method, which is properly designing image hash that captures important side information from the original image. First, the original image is split into non-overlapping blocks. The SIFT points with higher contrast values are typically more stable against such image operations as rotation, scaling, and compression. The SIFT points of each blocks are extracted with contrast values above a certain threshold $\boldsymbol{\tau}$, and then utilizes a reversible data embedding by using difference expansion with an encryption by secret key k. In forensic analysis, the image hash is extracted through a decryption with a received secret key k and a reversible data extracting method, as shown in Figure 2. Cryptographic one-way hash function is very sensitive to changes in the input signal. Generally, single-bit change will produce a completely different hash, therefore transmission analysis can detect whether the recovered secure hash altered or not.
The extracted image hash is to be securely attached along with the transmitted image and assist the forensic analysis on the received image.

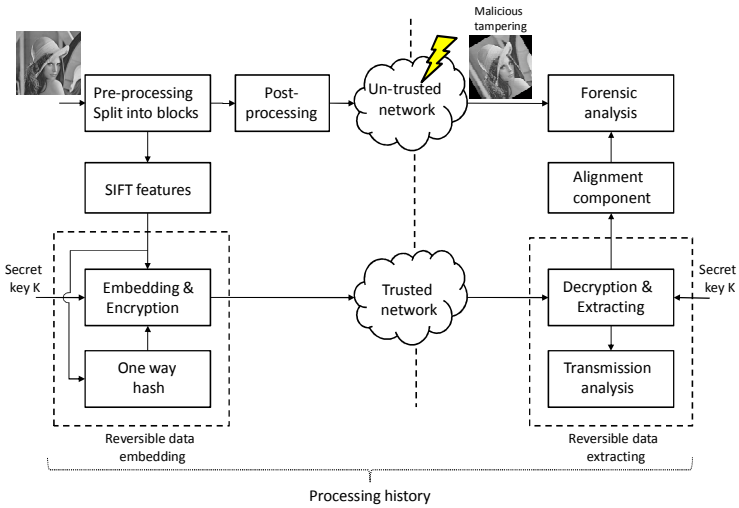

Fig. 2. Pipeline of the proposed method

The role of the post-processing block is applied a property of Radon transform to change the content of the image. For example, when the image is being distributed through different types of networks, to various receiving devices, some adaptations to the image format and content may occur, such as the image may resized and cropped for different screen sizes; logos may be inserted to the image corners.
Forensic analysis block is evaluated using a geometric transforms, such as rotation and scaling. More details introduced in the Section 2.

4 Detection and Localization of Image Tampering

In this section, we describe how the above proposed alignment component of the image hash can enable image cropping detection and tampering localization.

Cropping Estimation. Cropping can be used by an attacker to remove important part on the boundary of an image. We can use the image hash containing stable extrema proposed above to estimate the amount of cropping.

Given testing image I', is split into n blocks. We compute its Radon projections along the vertical and horizontal directions to obtain $f_o{}'(\rho)$ and $f_1{}'(\rho)$, respectively. The positions of the most stable extrema of $f_o{}'(\rho)$ and $f_1{}'(\rho)$ are also computed. Then, we can align the extrema which is recovered the SIFT features from image hash, with the extrema from $f_o{}'(\rho)$ and $f_1{}'(\rho)$ such that the number of matched extrema is maximized, as described in Section 2. 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 two different signals.

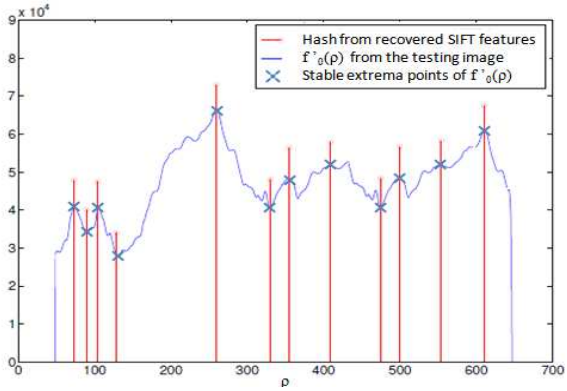

Fig. 3. Cropping estimation by aligning extrema from original and testing images

Thus, the accuracy of cropping estimation depends on the accuracy of the geometric estimation, since the testing image needs to be aligned with the original image through rotation and scaling.

Tampering localization. An adversary can modify local regions of an image and alter its original content by operations such as cut and paste. In this approach, the two images need to be properly aligned before comparison. Comparison for tampering localization based on consistencies in image statistics, as used in blind multimedia forensics, which consistencies can achieve more efficient and more accurate tampering localization. A tampered part of the image usually has significant difference from the original in term of their gradient information.

5 Experimental Results

In this section, we evaluate the performance of our proposed approach. All of our experiments are carried out on a PC machine 1.80 GHz Dual CPU with 2GB RAM. Also all of the simulation was carried out using Matlab version R2008a.

We test the integrity check component, rotation and scaling estimation accuracy of the proposed image hash on 50 images selected from the Corel database [7]. The image size is either 256x384 or 384x256. To evaluate the robustness of geometric transform estimation, we perform 15 operations for each of the 50 images, which give us a database of 750 images. The operations are listed in Table 1.

Table 1. List of image operations

Operations	Operation parameter
Rotation	5, 15, 45 degrees
Scaling	Scaling factor = 0.5, 0.8, 1.2, 1.5
Cropping	20%, 40% of entire image
Local tampering	Block size 50x50, 100x100
Various combinations of rotation, scaling, cropping and local tampering	

For the local tampering operation, we randomly select and swap two blocks within the image, where the block sizes are 50x50, 100x100. For each of 50 original images, we generate an image hash; composed of both alignment component, and integrity check component, and then evaluate the forensic analysis performance over 750 modified images. The confidence of geometric transform is computed both among same images and between different images. We show the discrimination performance in Figure 4, where all the hashes have roughly the same length, around 700 bits.

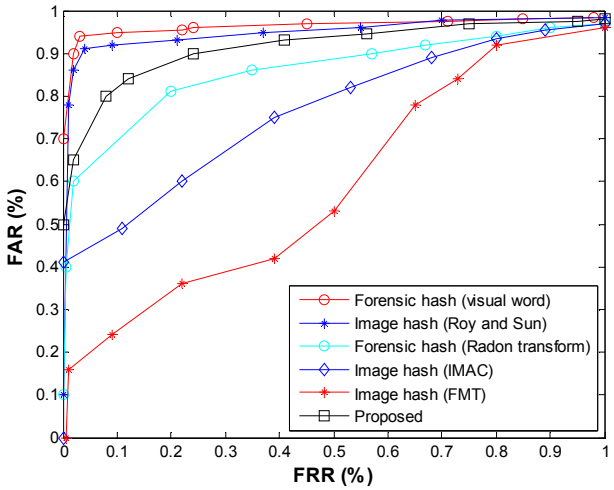

Fig. 4. Comparison of the discrimination performance

The quality of the embedded image is measured by Peak-Signal-to-Noise Ratio (PSNR) which is shown as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}, \qquad MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - I'(i,j)]^2;$$

where MSE is the mean square error between the original image and the corresponding embedded image. Generally, it is acceptable if typical values for the $PSNR$ in lossy image and video compression are between 30 and 50 db, where higher is better. Table 2 shows the effects of the embedded images. The quality of each embedded image is achieved very high ratio.

Table 2. The qualities of embedded images

Quality of embedded images	
The original images	PSNR of the embedded images
Lena	43.605
Beach	46.320
Architecture	43.021
Flower	42.253
Chemical-plant	45.468

In geometric transform estimation, we calculate the average estimation error for rotation and scaling over the 750 images using the alignment component as shown in Table 3.

Table 3. Geometric transform estimation accuracy

Threshold values ($SIFT > \tau$)	170	180	190	200	210	220
Length of hash (bpp)	~1116	~668	~535	~394	~241	~99
Rotation angle (α)	1.41^o	1.64^o	1.93^o	2.56^o	3.74^o	8.41^o
Scaling factor (s)	1.1%	1.3%	1.8%	2.2%	2.6%	6.8%

The 1-D summarization of Radon transform of the image is down-sampled to assist rotation estimation, but the stable extreme in the Radon projection along horizontal and vertical directions are used for scaling estimation. By increasing the length of image hash, more stable points and extrema can be included to improve the estimation performance. The length of the image hash depends on contrast values above a certain threshold $\boldsymbol{\tau}$.

6 Conclusion

In this paper, we proposed a novel secure image hashing based on reversible watermarking for forensic analysis. Our proposed method is order to achieve a good accuracy performance, as well as ensuring the security of image features. Compared to prior work, the proposed image hash can achieve more robust and accurate forensic analysis at the same hash length. The geometric transform offered by the image hash serves an important building block for further tampering localization using block based features.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Grant No. 2011-0012849).

References

1. Venkatesen, R., Koon, S.M., Moulin, P. : Robust image hashing. In Proc. of IEEE International Conference on Image Processing, vol.3, pp. 664-666 (2000)
2. Mao, Y., Wu, M. : Robust and secure image hashing, IEEE Trans. on Information Forensics and Security, vol.1, no.2, pp. 215-230, June (2006)
3. Delp, E., Memon, N. : Special issue on forensics analysis of digital evidence, IEEE Signal Processing Magazine, vol. 26, no.2, March (2009)

4. Tian, J. : Reversible data embedding using a difference expansion, IEEE Trans. on Circuit and Systems for Video Technology, vol.13, pp. 890-896, (2003)
5. Peiling, C., Junhong, L., Hongcai., Z. : Rotation and scaling invariant texture classification based on Radon transform and multi-scale analysis, Pattern Recognition Letters, vol.27, pp. 408-413, (2006)
6. Lindeberg, T. : Scale space theory in computer vision. Kluwer Academic Publishers. (1994)
7. Corel test set. [Online]. Available: http://wang.ist.psu.edu/~jwang/test1.tar
8. Lu,W.,Varna, A.l., Wu, M. : Forensic hash for multimedia information. In Proc. of SPIE Media Forensic and Security, pp. 7541 (2010)