SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 366–369

ISSN No: 2454-9614

Global and Local Features Based Image Authentication with Endured Hashing

R. Dhivya, K.P. Elangovan*, S. Viveka, S. Anbukkarasi

Department Of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode-638 052, Tamilnadu, India.

*Corresponding Author: R. Dhivya

E-mail: dhivyamahe23@gmail.com

,

Received: 10/11/2015, Revised: 12/12/2015 and Accepted: 11/03/2016

Abstract

A robust hashing method is developed for detecting image forgery including removal, insertion and replacement of objects and abnormal colour modification and for locating the forged area. Consequently, in recent years several hashing methods have utilized machine learning to improve the hashing quality by learning a group of hash functions. However, in the learning of hash functions, they either are sensitive to the data distributions or ignore the correlations of hash functions. So here a new hashing method, namely, Robust Hashing with Local Models (RHLM), for image authentication is created. The local models include position and texture information of object regions in the image. Secret keys are introduced in feature extraction and hash construction. While being robust against content-preserving image processing, the hash is sensitive to malicious tampering and, therefore, applicable to image authentication. The hash of a test image is compared with that of a reference image.

When the hash distance is greater than or less than a particular threshold, then the received image is judged as a fake. By decomposing the hashes, the type of image forgery and location of forged areas can be determined. Probability of collision between hashes of different images approaches zero. **Reviewed by* **ICETSET'16** *organizing committee*

Keywords: Robust Hashing, Image Hash, Forgery detection

1. Introduction

Digital information revolution has brought about many advantages and new issues. With the ease of editing and perfect reproduction, the protection of ownership and the prevention of unauthorized manipulation of digital audio, image, and video materials become important concerns. Digital watermarking, a scheme to embed special labels in digital sources, has made considerable progress in recent years. There are several categories of watermarking schemes. Among them, fragile watermarking is a technique to insert a signature for image authentication. The signature will be altered when the host image is manipulated. In this paper, we focus on digital

image authentication.

An effective authentication scheme should have the following desirable features:

1. To be able to determine whether an image has been altered or not;
2. To be able to locate any alteration made on the image;
3. To be able to integrate authentication data with host image rather than as a separate data file;
4. The embedded authentication data be invisible under normal viewing conditions;
5. To allow the watermarked image be stored in lossy compression format. Previously published methods for image authentication do not satisfy all the requirements.

In a heterogeneous network, there are servers, clients, and intermediate nodes with different computing capabilities. Clients receive multimedia data from servers through intermediate nodes that form a distribution chain. The distribution chain is not perfectly reliable, due to the following issues:

– Incidental distortion – the content may undergo re-encoding, e.g. a format change or re-compression, since it is necessary to adjust the data stream according to the client's capability and the network condition. Properties, such as resolution, contrast, etc., may change.

– Malicious modification – there might be malicious nodes that modify or replace the content.

In such a circumstance, an important question of the client is whether the received content is authentic. The above problem is easy when the original content is available for comparison, but in practice it is usually not the case. When the original content is not available, a possible solution is to generate a hash value on the server side and send it securely to the client side. The hash value is a compact abstract of the content. A client can re-generate a hash value from the received content, and compare it with the original hash value. If they match, the content is considered as authentic.

2. Techniques

2.1 Robust Hashing

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. Image hashing is a technique that extracts a short sequence from the image to represent its contents, and therefore can be used for image authentication. If the image is maliciously modified, the hash must be changed significantly. Meanwhile, unlike hash functions in cryptography such as MD5 and SHA-1 that are extremely sensitive to slight changes in the input data, the image hash should be robust against normal image processing.

When an image is sent to a user, a possible solution to prove the authenticity is to generate a hash value and send it securely to the user. The hash value is a compact string – an abstract of the content. A user can re-generate a hash value from the received image, and compare it with the original hash value. If they match, the content is considered as authentic. In order to allow incidental distortion, the hash value must possess some robustness.

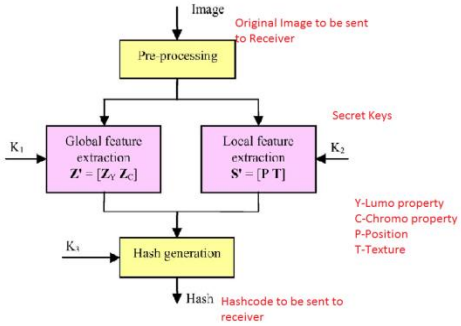
3. Edge Detection Mechanism

Embedding Algorithm should be developed to be robust to geometric distortions and improving the precision in locating the altered areas by implement via any digital multimedia networking application for verify the content of image transmission over RGB features. So this kind of implementation is desired to find features that better represent the image contents so as to enhance the hash's sensitivity to small area tampering while maintaining short hash length and good robustness against normal image processing like edge detection mechanisms and also include tracer routing to detect the content modified hacker system which is useful to reduce the hacking possibilities. So without the knowledge of this method, hacker information may be acknowledged to the sender once hacker receives the packet for content or object modifications.

4. IP Trace Routing

Tracer routing is to find out the unauthorized router access i.e the system which modifies the content of the image and forward to the destination in a routing process. This is verifying by getting packet processing time from each and every router in the routing process by a destination. Then the destination system finds out the timing differences with all routers if any timing is differed then it will be consider as unauthorized IP.

The overall idea of image processing is given in Fig. 1.



5. Conclusion

An image hashing method is developed using both global and local features. The global features are based on Zernike moments representing the luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. Hashes produced with the proposed method are robust against common image processing operations including brightness adjustment, scaling and noise contamination. The method proposed is used due to its acceptable accuracy and computation complexity. Since the edge detection mechanism is implemented, it gives us the exact object from the image.

References

[1] Jinkuan Song, Yi Yang, Xuelong Li, Fellow, IEEE, Zi Huang and Yang Yang, "Robust Hashing with Local Models for Approximate Similarity Search," ACM Comput. Survey, vol. 44, no. 7, 2014.
[2] R. Datta, D. Joshi, J. Li, J. Z. Wang, "Image retrieval: Ideas, influences, trends of the new age," ACM Compt. Survey, vol. 40, no. 2, 2008.
[3] L. Zhang, L. Wang, and W. Lin, "Generalized biased discriminant analysis for content-based image retrieval," TSMCB, vol. 42, no. 1, pp. 282–290, 2012.
[4] R. Cappelli, "Fast & accurate fingerprint indexing based on ridge orientation and frequency," TSMCB, vol. 41, no. 6, pp. 1511–1521, 2011.
[5] C. B¨ohm, S. Berchtold, and D. A. Keim, "Searching in high-dimensional spaces: Index structures for improving the performance of multimedia databases," ACM Comput. Survey, vol. 33, no. 3, pp. 322–373, 2001.
[6] D. Zhang, D. Agrawal, G. Chen, and A. K. H. Tung, "HashFile: An efficient index structure for multimedia data," in Proc. ICDE, 2011, pp. 1103–1114.
[7] Y. Tao, K. Yi, C. Sheng, and P. Kalnis, "Efficient and accurate nearest neighbor and closest pair search in high-dimensional space," ACM TODS, vol. 35, no. 3, 2010.
[8] A. Gionis, P. Indyk, and R. Motwani, "Similarity search in high dimensions via hashing," in Proc. VLDB, 1999, pp. 518–529.
[9] Q. Lv, W. Josephson, Z. Wang, M. Charikar, and K. Li, "Multi-probe LSH: Efficient indexing for high-dimensional similarity search," in Proc. VLDB, 2007, pp. 950–961.
[10] M. Datar and P. Indyk, "Locality-sensitive hashing scheme based on p-stable distributions," in Proc. SCG, 2004, pp. 253–262.
[11] R. Salakhutdinov and G. E. Hinton, "Semantic hashing," Int. J. Approx. Reasoning, vol. 50, no. 7, pp. 969–978, 2009.
[12] Y. Weiss, A. Torralba, and R. Fergus, "Spectral hashing," in Proc. NIPS, 2008, pp. 1753–1760.
[13] D. Zhang, J. Wang, D. Cai, and J. Lu, "Self-taught hashing for fast similarity search," in SIGIR, 2010, pp. 18–25.
[14] Y. Yang, D. Xu, F. Nie, J. Luo, and Y. Zhuang, "Ranking with local regression and global alignment for cross media retrieval," in Proc. ACM Multimedia, 2009, pp. 175–184.
[15] H. V. Jagadish, B. C. Ooi, K.-L. Tan, C. Yu, and R. Zhang, "iDistance: An adaptive B+-tree based indexing method for nearest neighbor search,"ACM TODS, vol. 30, no. 2, pp. 364–397, 2005.
[16] Li Weng, Rony Darazi, Bart Preneel, Benoit Mauq and Ann Dooms "Robust Image Content Authentication using perceptual Hashing and watermarking," in Proc. GOA/11/07.
[17] L. Sumalatha, V. Venkata Krishna V. Vijaya Kumar "Local Content Based Image Authentication for Tamper Localization," in MECS, 2012.