Fake Content Detection in an Image Hashing Approach with Feature Level Fusion

S.Narendhiran[1], K.Omprakash[2]

1 PG Scholar, Department of CSE, Al-Ameen Engineering College, Erode

2 Assistant Professor, Department of CSE, Al-Ameen Engineering College, Erode

[1]kingnarens@gmail.com

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 project, we propose a perceptual image authentication technique based on global and local features with a novel image authentication system by combining perceptual hashing and robustness. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. Secret keys are introduced in feature extraction and hash construction. These two hashes are compared to determine whether the test image has the same contents as the trusted one or has been maliciously tampered, or is simply a different image. We use a distance between hashes of an image pair as a metric to judge similarity/ dissimilarity of the two images. 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.

General Terms

Image authentication, hashing generation and encryption, Ip Tracer Routing.

Keywords

Perceptual hashing, watermarking, Decryption, Hashing, Clustering, Tamper Localization, fragile watermarking.

I.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. This paper has focused 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
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. Previous 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.

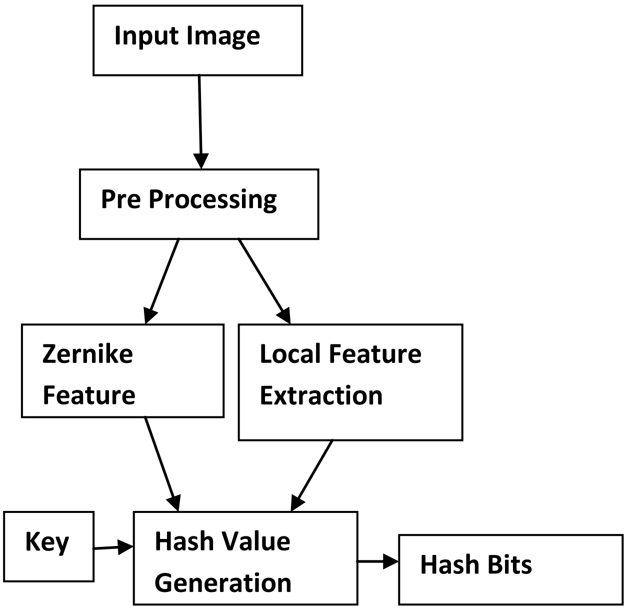

Fig.1 Overall structure of Proposed system

II.LITERATURE SURVEY

Semi-Fragile Zernike Moment-Based Image Watermarking For Authentication

With the development of advanced image editing software, it has become easier to modify or forge digital image. When the digital image contains important information, their credibility must be ensured. So a reliable image authentication system i necessary. Because the image can allow for lossy representations with graceful degradation, the image authentication system should be able to tolerate some commonly used incidental modification, such as JPEG compression and noise corruption. Therefore, the traditional bit-by-bit verification based on cryptographic hash is no longer a suitable way to authenticate the image. Image authentication that validates based on the content is desired. In content-based watermarking scheme for authentication, one of the most challenge issues is to define a computable feature vector that can capture the major content characteristic. A structural embedding method to locate the tampered areas by using the separability of Zernike moments-based feature vector. By using the semi-fragilities of the feature vector and the watermark, the proposed authentication scheme is robust to content preserved processing, while being fragile to malicious attacks.

Drawbacks

Not robust to geometric distortions and accuracy rate is not optimized in locating the altered areas.

The security of content-independent watermarking scheme is not so good.

Robust Image Content Authentication with Tamper Location

Image hashing maps an image to a short binary sequence representing the image’s characteristics.

This leads to problems such as copyright infringement and hostile tampering to the image contents. Recently, image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication. The concept of image hashing derived from cryptographic hashing. A novel image authentication system by combining perceptual hashing and robust watermarking. Perceptual hashing is a promising tool for multimedia content authentication Digital watermarking is a convenient way of data hiding. By combining the two, we get an efficient and versatile solution, one can verify the authenticity of images by comparing the embedded hash values with re-computed ones.

Drawbacks

The overall performance of such a system is lack in balance between the authentication performance under incidental distortion and the quality loss due to watermarking. Since the watermark embedding also brings distortion to the original image, it might affect the re-computation process. Robust Image Content Authentication Using Perceptual Hashing and Watermarking Perceptual hashing is a promising tool for multimedia content authentication. Digital watermarking is a convenient way of data hiding. By combining the two, got a more efficient and versatile solution. In a typical scenario, multimedia data is sent from a server to a client. The corresponding hash value is embedded in the data. The data might undergo incidental distortion and malicious modification. In order to verify the authenticity of the received content, the client can compute a hash value from the received data, and compare it with the hash value extracted from the data. The advantage is that no extra communication is required; the original hash value is always available and synchronized. However, on the other hand, image quality can be degraded due to water- mark embedding. Perceptual hash algorithms enable robust content authentication, whereas sometimes it is not easy to Setup a secure channel for transmitting hash values. Therefore, a more convenient approach comes fourth instead of sending through a secure channel, i can Deliver the hash value by imperceptibly embedding it into the content itself using robust Digital watermarking techniques. However, so far there is no practical design and in depth study on a complete content authentication system based on perceptual hashing and robust watermarking.

Drawbacks

The overall performance of the hash algorithm can be characterized by the low true positive rate and high false positive rate. A good algorithm should suppress the false positive rate while maintaining a high true positive rate

Content Based Image Authentication by Feature Point Clustering and Matching

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.A perceptual image authentication technique based on clustering and matching of feature points of images to address the limitations of the aforementioned schemes. Cluster the feature points and remove the outliers from the feature points. 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.

Drawback

Feature points are first generated from a given image, but their locations may be changed due to possible image processing and degradation. Local Content Based Image Authentication for Tamper Localization Digital images make up a large component in the multimedia information. Hence Image authentication has attained a great importance and lead to the development of several image authentication algorithms. It has been proposed a block based watermarking scheme for image authentication based on the edge information extracted from each block. An efficient image authentication method LECHES by embedding the content of the image into itself. In authenticating an image using the fragile watermark scheme, the watermark is extracted from the given image to verify its integrity. The local content-based watermark considered usually extracts robust feature point, and then partitions the image into multi-area using the feature point as the centre; finally the watermark is repeatedly embedding into each area.

Drawback

These mechanisms can detect if an image has been changed; however, they cannot locate where the image was changed.

III PROBLEM DESCRIPTION

Digital images are easy to store and share. However, they are susceptible to modification and forgery. Software development has made it easy for everyone to produce, edit, and distribute digital content. Since malicious content manipulation can lead to serious consequences, an important issue for the future world is the trustworthiness protection of multimedia data. When an image contains important information, its authenticity must be ensured. In this work, focused on image authentication. Digital images are often subjected to incidental distortion, e.g., format change, re-compression, resolution or contrast change, etc. Since incidental distortion usually preserves the content, the resultant image should still be considered as authentic. Therefore, image authentication should be based on content, not the binary representation.

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 to compute the message authentication code (MAC) from images. The generated hash is further encrypted with a secrete 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. 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. 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. 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 tradeoff 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.

IV IMAGE FEATURE EXTRACTION

A new method to construct robust and secure image hashes using Zernike moments, which is based on luminance and chrominance characteristics of the image. The image is first pre-processed. The pre-processing steps include re-sizing using bi-linear interpolation. The aim of re-sizing is to change the image into a fixed size, $M\times M$, to ensure that the generated image hash has a fixed length. As the luminance component contains most structural and textural information of an image i.e. evaluate brightness ratio of an image and chrominance represents RGB extraction from an image. Local Features – Coarseness extraction which is the parameter can be estimated heuristically from the contrast of textures in an image. The final hash sequence is obtained by pseudo-randomly permuting the binary sequence from the Zernike moments and local features.

V HASHING GENERATION AND ENCRYPTION

The global and salient local vectors are concatenated to form an intermediate hash. This is then pseudo-randomly

Scrambled based on a secret key to produce the final hash sequence. Here use advanced encryption algorithm to encrypt the hash sequence with respect to secret keys.

V DECRYPTION AND SIMILARITY RATIO

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 after successfully decrypt it 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.

VI HAMMING DISTANCE MATCHING

We use a distance between hashes of an image pair as a metric to judge similarity/ dissimilarity of the two images.

The hash sequence of a received image to be tested with the decrypted hash sequence under similarity ratio if difference is above the threshold then it has been maliciously tampered or legitimate image. The method can be used to locate tampered areas and tell the nature of tampering, e.g., replacement of objects or abnormal modification of colors.

VII IP TRACER ROUTING

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. If identified whatever tampered area then need to trace the unauthorized system using IP tracing technique.

Tracer routing enables the initiator or sender to trace the whole routing process and find out the unauthorized router access in a routing process.Sender verifying by getting automatic acknowledgment IP from each and every router in the routing process.

VIII 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.

ACKNOWLEDGMENT

I take great pleasure in expressing our profound gratitude to all those who have helped for the successful completion of the project. I am grateful to our respected Correspondent and Secretary Mr. ALHAJ. A.K.JAFFARULLAH, *Al-Ameen Engineering College*, Erode on guiding light for me in all the activities i had in our college premises. I would like to express our sincere thanks to our respected Principal **Dr.A.M.J.MD.ZUBAIR RAHMAN**, M.E., M.S., Ph.D for providing an opportunity to carry out the project work.

I am very much indebted to the Head of the Department of Computer Science and Engineering Professor Mr.M.MOHAMED MUSTHAFA., M.Tech, (Ph.D) for his support and guidance towards me and for his gracious permission to undertake this project work.

I am indeed grateful to our project guide Assistant Professor Mr. K.OMPRAKASH, M.E., Department of Computer Science and Engineering who helped and encouraged me throughout this project.

REFERENCE

[1] V. Monga, A. Banerjee, and B. L. Evans, “A clustering based approach to perceptual image hashing,” IEEE Trans. Inf. Forensics Security, vol.1, no. 1, pp. 68–79, Mar. 2006.

[2] S. Xiang, H. J. Kim, and J. Huang, “Histogram-based image hashing scheme robust against geometric deformations,” in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121–128.

[3] Z. Tang, S.Wang,X. Zhang, W.Wei, and S. Su, “Robust image hashing for tamper detection using non-negative matrix factorization,” J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.

[4] A. Swaminathan, Y. Mao, and M. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[5] Y. Lei, Y.Wang, and J. Huang, “Robust image hash inRadon transform domain for authentication,” Signal Process.: Image Commun., vol. 26, no. 6, pp. 280–288, 2011.

[6] F. Khelifi and J. Jiang, “Perceptual image hashing based on virtual watermark detection,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 981–994, Apr. 2010.

[7] V. Monga and M. K. Mihcak, “Robust and secure image hashing via non-negative matrix factorizations,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 376–390, Sep. 2007.

[8] K. Fouad and J. Jianmin, “Analysis of the security of perceptual image hashing based on non-negative matrix factorization,” IEEE Signal Process. Lett., vol. 17, no. 1, pp. 43–46, Jan. 2010.

[9] Z. Tang, S. Wang, X. Zhang, W. Wei, and Y. Zhao, “Lexicographical framework for image hashing with implementation based on DCT and NMF,” Multimedia Tools Applicat., vol. 52, no. 2–3, pp. 325–345, 2011.

[10] F. Ahmed, M. Y. Siyal, and V. U. Abbas, “A secure and robust hash based scheme for image authentication,” Signal Process., vol. 90, no. 5, pp. 1456–1470, 2010.

[11] X. Lv and Z. J. Wang, “Perceptual image hashing based on shape contexts and local feature points,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1081–1093, Jun. 2012.

[12] W. Lu, A. L. Varna, and M. Wu, “Forensic hash for multimedia information,” in Proc. SPIE,Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.

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

[14] H. Lin, J. Si, and G. P. Abousleman, “Orthogonal rotation-invariant moments for digital image processing,” IEEE Trans. Image Process., vol. 17, no. 3, pp. 272–282, Jan. 2008.

[15] S. Li, M. C. Lee, and C. M. Pun, “Complex Zernike moments features for shape-based image retrieval,” IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 39, no. 1, pp. 227–237, Jan. 2009.