A Study on Image Authentication Methods

Marakumbi Prakash R[1], Jayashree V. Khanapuri[2]

[1]*Asst.Professor, E&C Dept., Tontadarya College of Engineering, Gadag, Karnataka, INDIA*
[2]*Professor, E&T Dept., K J Somaiya Institute of Engineering and Information Technology, Mumbai, Maharashtra, INDIA*

---***---

Abstract - *Authentication plays an important role in protecting image against unauthorized access. Digital images are transmitted over insecure channels such as the internet. Images must be protected against attempts to manipulate them; such manipulation could tamper the decisions based on these images. To protect the authenticity of images several methods have been proposed. Image authentication methods have gained attention due to their significance in the areas of multimedia communications and multimedia networking applications. The existing image authentication methods are cryptographic authentication, robust image hashing authentication and watermarking authentication. The aim of this paper is to present different methods in authentication of images in multimedia applications.*

Keywords: Image Authentication, Watermarking, Cryptography, Hashing

1. INTRODUCTION

Authentication methods provide a means of ensuring the integrity of an image. Therefore there is need to protect these images against various attempts to manipulate them and it is important to make an effective method to solve image authentication problem that is ensuring the integrity of an image. Due to increase in the multimedia applications, image authentication techniques have gained attention. The existing image authentication methods are watermarking, cryptography and robust image hashing method. Digital watermarking is the science and art of embedding copyright information called watermarks in the files. Cryptography includes encryption and decryption to transfer documents or images. Robust image hashing is based on rotation-invariant moments that can effectively catch important information in an image.

2. REQUIREMENTS OF IMAGE AUTHENTICATION

The following are the requirements of image authentication:

- Sensitivity: The authentication system should be able to detect any content manipulation.
- Robustness: The authentication system must tolerate content preserving manipulations.
- Localization: The authentication system should locate the image regions that have been modified.
- Recovery: The authentication system should completely restore the image regions that were altered.
- Security: The authentication system must protect the authentication data against any falsification attempts.

3. IMAGE AUTHENTICATION METHODS

Various image authentication methods are being used to protect the images and information, and their communications. Virtual private network, firewall, encryption, cryptographic hash function such as digital signature, machine authentication code, manipulation detection code, and perceptual hashing are the examples of image authentication methods. Limitations of existing security like Firewall and virtual private network only protect the information up to the point of the internal networks. Encryption is an efficient tool for secure transmission, but when the sensitive data is decrypted, the information is not protected anymore. The drawback of cryptographic hash function is that it cannot locate where the images have been tampered.

The major methods for authentication of an image are cryptographic, robust image hashing and watermarking authentication.

3.1 Cryptographic authentication

Cryptography provides for secure communication in the presence of malicious third-parties known as adversaries. Encryption and Decryption are the two functions of cryptography. Traditional cryptography algorithms exhibit satisfactory results for image authentication with high tamper detection. Localization performances are not good but for some applications the method may be acceptable. Due to the sensitivity of the hash function, a small modification in binary image data causes changes. The image is said to be manipulated even when one bit of this image is changed; this is very severe for most of the applications. The advantage of Cryptographic based authentication is conventional cryptography show satisfying results for authentication of an image with high tamper detection. The disadvantages of Cryptographic authentication are hash functions are very sensitive, localization performances are not very good.

3.2 Robust image hashing authentication

Image hashing is used to identify the duplicate copies of the original images. A robust hashing technique is used for detecting image forgery, colour modification, and for locating the forged area. The robust hashing method is based on Random Transform performed on input image to obtain the projections in various orientations. The insignificant coefficients are removed. The invariant moments are calculated. DFT is performed on the invariant moments. Finally, the image hash value H is defined as the normalized and quantized version of the significant DFT coefficients and then the hash bits are generated. Most of the images hashing algorithms have their disadvantages in getting the desirable performance against a particular image processing attack. The disadvantage of robust image hashing is large area cropping.

3.3 Watermarking authentication

Digital watermarking involves embedding information into digital multimedia content such that the information can later can be extracted or detected by the recipient for different purposes such as control and copy prevention. The process of watermarking has to be resilient against tampering attacks, keeping the content of a watermark readable in order to be recognizable when extracted by the recipient. The significant features of watermarking system are robustness and fidelity. The size of the embedded information has to be considered. The data becomes less robust as its size increases. The watermark generation, watermark embedding, and watermark extraction for detection and authentication are three stages of digital watermarking system .A watermarking scheme can be classified into non-blind or blind watermarking based on the method used to detect watermark. A non-blind watermarking requires the original image to extract the watermark, while a blind watermarking does not. Watermark security refers to its resistance against unauthorized detecting and decoding, while robustness refers to a watermark's resistance against processing, such as filtering, geometrical transforms and compression. A study on watermarking research shows that many watermarking schemes give consideration to robustness more than security. However, a robust watermark is not enough to accomplish protection because the range of hostile attacks is not limited to common processing and distortions. Therefore, robustness and security should be considered in a watermarking system. Spread-spectrum technique is a popular approach to achieve the robust and secure watermarking for multimedia content. A spread-spectrum system encodes data in a chosen binary sequence that appears like noise to an outsider but can be recognized by a receiver with an appropriate key. A non-blind watermarking might be less applicable, because when watermark detection is required, the original image may not be available. To achieve security, the watermarking scheme is constructed based on chaotic maps. A chaotic map is function that exhibits some sorts of chaotic behaviour. The feature of chaos in the information hiding is its sensitivity to initial conditions. These characteristics make chaotic maps excellent candidates for securing watermarks.

4. COMPARISON OF IMAGE AUTHENTICATION METHODS.

Table -1: Comparision of image authentication methods

Techniques	Advantages	Disadvantages
Cryptographic authentication	high tamper detection	hash functions are very sensitive
Robust image hashing authentication	Hashes produced are robust; collision probability between hashes of different images is very low.	Large area cropping
Watermarking authentication	Image tampering detection, embedding watermarks is easy and identify the author of copyright work	Cannot locate where the images have been tampered.

5. CONCLUSION

In multimedia era the digital information is sent across the internet can potentially be intercepted by third party other than the intended recipient. Therefore digital information requires confidentiality, security service, authentication and determination of malicious activities. Literature Survey concludes that watermarking scheme constructed based on chaotic maps is more efficient compared to other methods, because Chaos in information hiding are sensitive to initial conditions and the outspreading of orbits over the entire space. These characteristics make chaotic maps excellent candidates for watermarking and encryption.

REFERENCES

[1] Y. Lei, Y.Wang, and J. Huang, "Robust image hash in Radom transform domain for authentication," IEEE Signal Process. Image Communication.vol.26, no.6, pp.280288, 2011.

[2] V.Monga, M.K.Mihcak, "Robust and secure Image hashing via nonnegative matrix factorizations," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp.376– 390, Sep.2007.

[3] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," in Proc. IEEE International

Conference on Image Processing, VOL.2, pp. 680-683, October 1997.

[4] C.Y. Lin and S.F. Chang, "Generating robust digital signature for image/video authentication," in Proc. Multimedia and Security Workshop at ACM Multimedia '98, Bristol, UK, September 1998.

[5] C Yu, X Zhang "Watermark embedding in binary images for authentication", IEEE Trans. Signal Processing, VOL.01, no.07, pp.865-868, September. 2004.

[6] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, VOL. 13, Dec. 2006

[7] Yan Zhao, Shuozhong Wang, Guorui Feng, Zhenjun Tang, "A Robust Image Hashing Method Based on Zernike Moments",IEEE Journal of Computational Information Systems6:3 717-725,2011.

[8] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Member, IEEE"Robust Hashing For Image Authentication Using Zernike Moments And Local Features" IEEE Transactions On Information Forensics And Security, Vol.8, No. 1, January 2013.

[9] Dachselt F and Schwarz. W. "Chaos and Cryptography. Circuits and Systems. Fundamental Theory and Applications", IEEE Transactions, 48(12), pp.1498-1509, DOI- 10.1109/TCSI.2001.972857, 2001.