A Survey on Image Authentication Techniques

S.Jothimani[1], P.Betty[2]

1- PG Scholar, Department of CSE, Kumaraguru College of Technology
2-Assistant Professor, Department of CSE, Kumaraguru College of Technology
Coimbatore, Tamil Nadu, India.

***Abstract*— Image authentication is the process of proving image identity and authenticity. Digital images are increasingly transmitted over non-secure channels such as the Internet. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Nowadays image authentication techniques have recently gained great attention due to its importance of multimedia applications. The traditional cryptographic hash functions, such as MD5 and SHA-1 are used for authentication. However, these hash functions are not suitable for image authentication. Because they are so sensitive that even one bit change of the input data will lead to a significant change of the output hash. Besides, image authentication system requires the main content sensitive. In order to make up for the disadvantage of the traditional cryptographic hash functions in image authentication, robust image hashing was first introduced which provide good ROC performance, low collision probability.**

***Keywords*— Authentication, Zernike moments, NMF, Random transform.**

I. INTRODUCTION

Image Authentication techniques enable the recipients to verify the integrity of the received image. The increasing need for trustworthy distribution of digital multimedia in business, industry, defence etc. has lead to the concept of content-based authentication. Nowadays manipulating digital images efficiently and seamlessly has become very easy with the availability of powerful software and necessary to ensure confidentiality as well as integrity of the images that are transmitted. Military, medical and quality control images must be protected. To protect the authenticity of images, several approaches have been proposed. Number of image processing tools to change images for different purposes, it leads to problems such as copyright infringement and hostile tampering to the image contents. Image authentication techniques have been developed rapidly to verify content integrity and prevent forgery. Image hashing is an important method for image authentication.

II. REVIEW OF BIOMETRIC TEMPLATE PROTECTION TECHNIQUES

Image hash function maps an image to a short binary string based on the image's appearance to the human eye. In a particular, perceptual image hash function should have the property that two images that look the same to the human vision map to the similar hash value, even if the images have different digital representations. This differentiates a perceptual hash from traditional cryptographic hashes, such as SHA-1 and MD-5. SHA-1 and MD-5 hashes are extremely sensitive to the input data.

Perceptual robustness constructs the hash function should map visually identical images to the same hash even if their digital representations are not same exactly. Sensitivity to visual distinction is perceptually important changes to an image should lead to a different hash value. This feature is essential for the image hash to be useful in image authentication and digital forensics.

A. *Authentication requirements*

1) Sensitivity: The authentication system must be able to detect any content modification or manipulation. For any authentication algorithms, detection of any manipulation is required and not only content modification.

2) Robustness: The authentication system must tolerate content preserving manipulations.

3) Localization: The authentication system must be able to locate the image regions that have been altered.

4) Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered.

5) Security: The authentication system must have the capacity to protect the authentication data against any falsification attempts.

B. Existing Image Authentication Techniques

The major techniques for authenticating an image are as follows,

- Watermarking based authentication
- Cryptography based authentication
- Robust image hashing authentication

1) Watermarking-based authentication

Digital watermarking is the art and science of embedding copyright information in the files; the information which is embedded in files is called watermarks. Digital watermark is one of the signals which are added to a document to authenticate it and to prove the ownership. Two approaches for watermarking data authentication are p ossible fragile watermarking and robust watermarking.

Advantages of watermarking

- Uniquely identify the author of copyright work.
- Implementation on pc platform is possible.
- Embedding watermarks is easy.
- Image tampering detection.

Disadvantages of watermarking

- Doesnt prevent image copying.
- Watermark vanishes if someone manipulates the image.
- Resizing, compressing images from one file type to another may diminish the watermark and it becomes unreadable.

2) Cryptographic–based authentication

Cryptography is the science of transforming the documents or images. It includes two functions encryption and decryption. Algorithms based on conventional cryptography show satisfying results for image authentication with high tamper detection. Localization performances are not very good but may be acceptable for some applications. Even a small change in the image pixels or even in the binary image data causes changes because the hash function is very sensitive. The image is classified as manipulated, when just only one bit of this image is changed; this is very severe for most of applications.

Advantages

Conventional cryptography show satisfying results for image authentication with high tamper detection.

Drawbacks

- Localization performances are not very good.
- Hash functions are very sensitive.
- Knowledge of private key
- Different to distinguish between malicious and innocuous modification
- Delay in transmission

3) Robust image hashing –based authentication

Perceptual hash function (PHF) extract a set of features from the image to form a compact representation which can be used for authentication. Robustness, fragility and security are the three key issues of image hashing. Robustness requires that image hashing should be invariant to incidental modifications, such as JPEG compression, blur, noise, enhancement and some other perceptually similar operations. Fragility means that the image hashing should have the ability to distinguish the visually distinct images. Security is the degree to prevent the attacker from tricking the authentication system with a maliciously tampered image. A robust and secure image hashes using Zernike moments, is based on rotation invariance of magnitudes. In image processing, orthogonal rotation-invariant moments (ORIMs) can effectively catch important information in an image.

Advantages

- Hashes produced are robust against common image processing operations including brightness adjustment, scaling, small angle rotation, JPEG coding and noise contamination.
- Collision probability between hashes of different images is very low.
- Reasonably short hash length and good ROC performance.

The robust hashing scheme based on Random Transform RT [4] is first performed on the input image to obtain the projections in various orientations. Then the insignificant coefficients are discarded. Next calculate the invariant moments. Subsequently, DFT is performed on the invariant moments. Finally, the image hash H is defined as the normalized and quantized version of the significant DFT coefficients and finally the hash bits are generated.

Compared with the existing works, the random transform scheme shows better performance to the malicious operations.

III. Comparative Study of Different Image Authentication Techniques

TABLE I
COMPARISION OF DIFFERENT IMAGE AUTHENTICATION TECHNIQUES

Method	Robust image hashing based authentication	Watermarking-based authentication	Cryptography based authentication
Approaches	Zernike moments, wavelet based, random transform	Fragile, robust watermarking	Extended visual cryptography
Tamper detection and localization	High	Medium	Medium
Merits	Combines global and local features, good ROC performance, low collision probability	Uniquely identify the author of copyright work, image tampering detection	Tamper detection
Demerits	Large area cropping	Resizing, Compressing image from one file type to another may diminish the watermark.	Hash functions are very sensitive.

IV. Conclusion

Image authentication is the process of proving image integrity and authenticity. Literature Survey concludes that robust image hashing based authentication is more efficient compared to other techniques because it provides short hash length, good ROC performance and low collision probability. Table 1 explains the methods of different image authentication techniques, its merits and demerits and disadvantages.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] V.Monga, 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.