IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-2, Issue-12 E-ISSN: 2347-2693

Study On Image Authentication Techniques

Vinitha.C[1*] and Dr.M.Azath[2]

[1*2]*Department of Computer Science and Engineering, Met's School of Engineering, Mala, India*
vinithasreeniketh@gmail.com, mailmeazath@gmail.com

www.ijcaonline.org

Received: Nov /22 /2014 Revised: Nov/30/2014 Accepted: Dec/12/2014 Published: Dec/31/ 2014

***Abstract*—** Image authentication is the process of proving an image, is an accurate representation of the original one. Image authentication techniques have recently gained great attention due to its importance of multimedia applications. Through non-secure channels like internet digital images are increasingly transferred. Several methods which include Fragile Water-marking, Semi Fragile Water-Marking, Conventional Cryptography are used to protect the authenticity of images. Methods are classified according to the service they provide, that is strict authentication, localization, selective authentication, tamper detection and reconstruction capabilities and robustness against different desired image processing operation. The main aim of the paper is to present a survey and comparison of emerging techniques for image authentication.

***Keywords*—** Conventional Cryptography , Fragile Water Marking , Image Authentication, Image Contents , Robust Image Hashing , Semi Fragile Water Marking

I. INTRODUCTION

Image processing [1] is a type of signal processing in which a raw image received from camera or sensors are taken as inputs and as a result an image or an image with set of characteristics are obtained as output. An image can be treated as a function of two real variables of the real world. Image processing can be termed as digital image processing which can be possible in two ways that is in the form of optical and analog image processing. An image is viewed as two-dimensional signal in which standard signal processing techniques are used. In various application area such as multimedia computing, secured image data communications, bio-medical remote sensing, texture understanding, pattern recognition, the image processing is needed. It is easy to modify the contents of digital images because of the wide availability of digital image processing tools which allows extensive manipulations and reuse of image materials, where modifications are not tolerated [2]. In many image processing operations for transformations, enhancement or restorations must be tolerated while others are not. To protect images from the attempts of manipulations, effective methods of image authentication must be provided.

A. Requirements For Digital Image Authentication System
Digital Image Authentication System [3] should satisfy following 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 system must accept content preserving manipulations.
3) Localization: The manipulated region must be traced by the authentication system.
4) Recovery: The authentication system can be able to partially or completely rebuild the image regions that were corrupted.
5) Security: The system must have the capability to save the authenticated data against any forgery attempts.
6) Portability: During any transmission, storage or processing operation the protected image must carry its signature.
7) Complexity: A real-time implemented algorithms must be followed by the authentication system.

II. EXISTING IMAGE AUTHENTICATION METHODS

Authentication is the science that studies how to protect the integrity of digital media. Generally, there are two basic forms of authentication: passive and active authentication. Passive authentication, also called forensic analysis, tries to understand whether a digital content has been tampered with by using statistical analysis with- out previously adding an authentication signal to the digital media. Passive authentication has the desirable characteristic of working with virtually any type of data, without requiring that they are modified at the time of creation. On the negative side, passive authentication is not always possible and doubts exist about its reliability and security. This is not the case with active authentication, whereby the integrity of a digital content is protected (and demonstrated) by embedding an authenticating signal within the digital content itself before sharing it with other users.

A. Water-Marking Based Authentication

Digital watermarking belongs to active authentication in which copy right information are embedded in the files, where information embedded are called as Watermarks [4]. To prove the ownership and to authenticate the documents, the digital watermarks can be added. The water-mark based

authentication can be classified in terms of robustness into Fragile and Semi-Fragile water-marks.

a. Fragile Water-Marking Based Authentication

Content authentications are generally done by Fragile Watermarking algorithms [5]. If a Watermark is broken or distorted by making some changes then it is called as fragile watermarking and it is mainly used for detecting tampered regions. In fragile watermarking, a water-mark for a set of image pixels are generated and that watermark is get inserted into it, to protect the image from further modification. Fragile Watermarking do not abide any image distortion and the watermarks should not be visible under normal condition. It works directly in spatial domain and transform domain. It is due to the sensitivity of fragile marks that is being used in image authentication. Fragile water-marking do not abide any image distortion and the water-mark should not be visible under normal condition. By providing correct key the detector can able to find and understand the changes made to an image.

b. Semi-Fragile Water-Marking Based Authentication

The digital contents can be reliably authenticated using Semi- Fragile Watermarking [6], which has the properties of Fragile Watermarking. The common method of Semi-Fragile Watermarking is, encrypt the features extracted from the given image using a private key and decrypt the watermark extracted from the received image using public key. It tolerates some modifications like JPEG lossy compression and adjustment of brightness on watermark. When compression rate increases the image cannot be able to authenticate due to its poor quality. The technique identifies the location of the degraded blocks and estimates the original image contents.

Advantages of watermarking: Uniquely identify the author of copyright work. Embedding watermarks is easy. Image Tampered regions in images can be detected.

Disadvantages of watermarking: It cannot prevent image copying. Watermark vanishes if someone manipulates the image. Re-sizing, compressing images from one file type to another may diminish the watermark and it becomes unreadable.

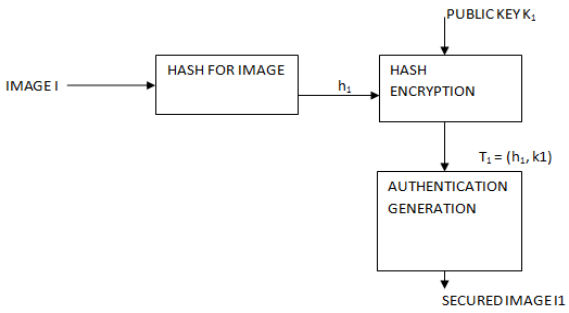

Fig.1 Generation of Secured Image

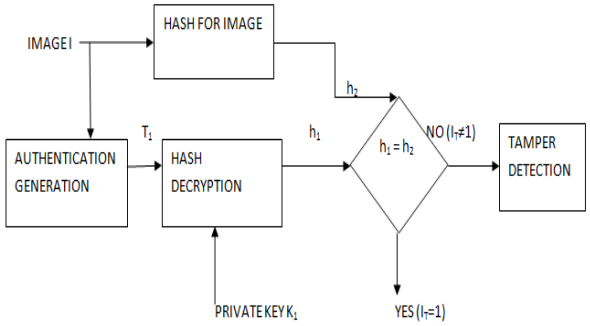

Fig.2 Verification of Authenticity

B. Cryptography Based Authentication

Cryptography based authentication [7] is the methods in which the images or documents are transformed into another form by encryption and decryption. Conventional cryptography is one of the cryptography based authentication for image authentication with high tamper detection, which computes a message authentication code (MAC) from image using a hash function. The hash function (H) is the encrypted using senders secret private key (S) which is added to the image, by using the public key K_1 of the receiver the hash can be again encrypted for more secure exchange.

The hash from the received image at the receiver is extracted and is decrypted using private key K_1, which is then compared with calculated one. In conventional cryptography, the manipulations in the image are detected by calculating separate hashes for each lines and columns of an image, which is then compared with each line and column of the image to be tested. At the same time, these hashes obtained are very sensitive to even a small variation in image pixels [8]. The main objective of cryptography based authentication is to solve the problem of message authentication. Some of the drawback of this authentication method are delay in transmission and its difficult to differentiate between malicious and innocuous modifications.

C. Robust Image Hashing –Based Authentication

Another important method for image authentication method is image hashing - derived from cryptographic hashing. Robust image hashing based authentication [9] includes the selection of a set of features from a given image for a compact representation. For image authentication, the image hashing must be robust, fragile and secured. A robust image hashing method should be constant towards normal modification including brightness or contrast adjustment, JPEG compression and so on. The images can be differentiated by human visual perception, which means that the image hashing method is fragile. A secured hashing

method is needed to detect maliciously tampered regions. The image hashing can be viewed in two steps [10]. In first step, an intermediate hash is obtained through feature extraction and in second step; a final hash is produced by compressing the intermediate hash.

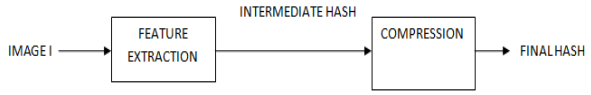

Figure .3 Image Hashing Scheme

A robust hashing method based on global and local features of the image, can provide a better authentication to the images. The global features include the zernike moment, which is a well- known Orthogonal Rotation - Invariant Moment (ORIM) [11] to recognize the shapes of the objects in the image. The perceptual texture features constitute the local features of an image. Compared with the existing method for authentication the robust image hashing method based on global and local features provide better performance. Some of the benefits of this methods are it has low collision probability, short hash length and good Receiver Operating Characteristics (ROC).

III. COMPARISON OF EXISTING IMAGE AUTHENTICATION METHOD

Method	Robust Image Hashing Based Authentication	Water-Marking 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	Identify the author of copyright work, Image tampering detection	Tamper detection
Demerits	Large area cropping	Re-sizing, Compressing image from one file type to another may diminish the watermark.	Hash functions are very sensitive.

Table 1: Comparative view of different authentication methods

IV. CONCLUSION

In this paper we present a literature review, which concludes that robust image hashing based authentication is more efficient compared to other techniques because it provides short hash length, good receiver operating characteristics (ROC) performance, low collision probability. Image hash is developed as a result of feature extraction and the coding of intermediate result. That hash is beneficial in image databases, watermarking, authentication etc.

REFERENCES

[1] K.M.M. Rao, ―Overview Of Image Processing , Medical Image Processing, Proc. of workshop on Medical Image Processing and Applications, 8th October 1995 @ NRSA, Hyderabad-37. 4.

[2] Adil Haouzia & Rita Noumeir, , “Methods of Image Authentication : a Survey,” Published online: 1 August 2007, # Springer Science and Business Media, LLC 2007,Multimedia Tools Appl (2008) 39:1–4.

[3] Reshma Vartak, Smita Deshmukh , “Survey of DigitalImage Authentication Techniques ,” International Journal of Research in Advent Technology, Vol.2, No.7, July 2014 E-ISSN: 2321-9637 .

[4] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark," in Security and Watermarking of Multimedia content, VOL.3657of SPIE proceedings, January 1999.

[5] C.Y. Lin and S.F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content," in Proc. SPIE International Conf. on Security and Watermarking of Multimedia Contents, VOL. 3971, January 2000.

[6] Book of Angela D’Angelo, Giacomo Cancelli, and Mauro Barni, “Watermark-based Authentication,” .

[7] Gaurav A. Hiware, Rahul D. Chopade, Prof. Manish S. Nimkar , “A Cryptographic Technique using image based Authentication,” http: // www.ijfeat.org (C) International Journal For Engineering Applications and Technology [62-70] , March ISSN 2321-8134.

[8] 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 .

[9] S.Jothimani, P.Betty , “Survey of Image Authentication Techniques,” International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 4- Jan 2014 .

[10] Yan Zhao, Shuozhong Wang, Guorui Feng, Zhenjun Tang,"A Robust Image Hashing Method Based on Zernike Moments ," Journal of Computational Information Systems6:3(2010) 717-725 .

[11] F. Zernike, Beugungstheorie des schneidenverfahresund seiner verbesserten form[J], der phasenkontrastmethode, Physica, 1934, 1, pp.689-704