International Journal of Research in Advent Technology, Vol.2, No.7, July 2014
E-ISSN: 2321-9637

Survey of Digital Image Authentication Techniques

Reshma Vartak[1], Smita Deshmukh[2]
Information Technology[1], Mumbai University[1]
Email: reshma.vartak@gmail.com[1]

Abstract- Today internet is become a common communication medium to transfer multimedia data. This multimedia data includes digital images of text documents, scan copies of important certificates, circuit diagrams, design drafts, signed cheques. Providing integrity and authentication to these images is a challenging task as they are increasingly transmitted over insecure network such as internet and with the fast advancement of digital technologies, it is easy to make modifications to the contents of digital images; hence there is an urgent need to ensure the integrity and authenticity of digital images against various attempts to manipulate them and it is important to design effective methods to solve the problem of digital image authentication, particularly for important digital images whose security must be protected. In this paper we present requirements of digital image authentication system, types of digital image authentication and application of digital image authentication system.

Index Terms- Digital Image Authentication, Strict Image Authentication, Content based Image Authentication

1. INTRODUCTION

Digital images are used to preserve important information. But providing integrity and authentication to these images is a challenging task as they are increasingly transmitted over insecure network such as internet. In this era with the use of fast advanced technologies it is easy to modify the contents of these digital images. 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, particularly for document images such as important certificates, scanned cheques, art drawings, signed documents, circuit diagrams, design drafts etc.

2. DIGITAL IMAGE AUTHENTICATION SYSTEM REQUIREMENTS

Digital Image Authentication System should satisfy following requirements**.**

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

[2] ***Robustness*****:** Also called tolerance. The authentication system must tolerate content preserving manipulations. This property is valid just for algorithms that provide a selective authentication service.

[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.

[6] ***Portability:*** The authentication system must be able to carry the signature with the protected image during any transmission, storage or processing operation.

[7] ***Complexity:*** The authentication system must use real-time implemented algorithms that are neither complex nor slow.

3. DIGITAL IMAGE AUTHENTICATION TECHNIQUES

3.1 Strict Image Authentication

Strict image authentication methods do not tolerate any changes in the image data [5,6]. These methods can be further separated in two groups according to the techniques that are used:

3.1.1 Conventional cryptography
3.1.2 Fragile Watermarking

3.1.1 Conventional Cryptography

Image authentication methods based on *cryptography* compute a message authentication code (MAC) from images using a hash function. The resulting hash (h) is further encrypted using secret private key S of the sender and then appended to the image. For a more

secure exchange of data between subjects, the hash can be encrypted using public key K1 of the recipient. The verification process is depicted in Figure 1. At the receiver side receiver computes the hash from the received image. The hash that was appended to the received image is extracted and decrypted using private key K1. The extracted hash and the calculated one are then compared.

Techniques that are based on the hash computing of image lines and columns are known as line–column hash functions [7]. Separate hashes are obtained for each line and each column of an image. These hashes are stored, and compared afterwards with those obtained for each line and each column of the image to be tested. If any change in the hashes is found, the image is declared manipulated otherwise it is declared authentic.

Conventional cryptography was developed to solve the problem of message authentication. Algorithms based on conventional cryptography show satisfying results for strict image authentication with high tamper detection [5]. Localization performances are not very good but may be acceptable for some applications. Hash functions are very sensitive to any small change in the image pixels or even in the binary image data. In consequence the image is classified as manipulated, when just only one bit of this image is changed; this is very severe for most of applications.

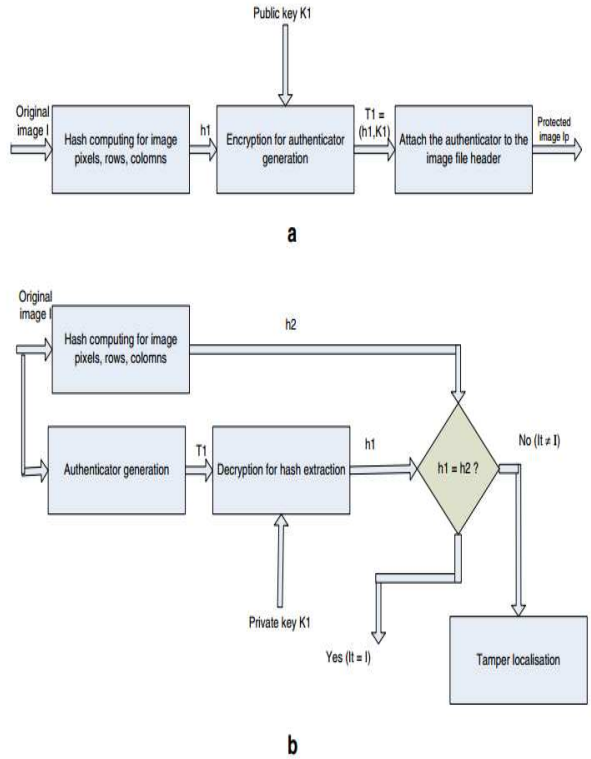

Fig. 1. Conventional Cryptography

3.1.2 Fragile Watermarking

Digital watermarking is a technique consists of calculating watermark and inserting watermark (authentication data) into an image, which can be extracted later or detected for variety of purposes including identification and authentication purposes. A digital watermark is called *fragile* if it is distorted or broken under slight changes. Fragile watermarks are commonly used for tamper detection (integrity proof) [3].

The basic idea behind fragile watermarking techniques is to generate a watermark for a set of image pixels and to insert it in the image to be protected in such a way that any modification made to the image is also reflected in the inserted watermark. Simply verifying the presence of the inserted watermark allows the image authenticity verification and eventually localization of tampered regions. This type of watermarking does not tolerate any image distortion. The image is considered authentic if and only if all its pixels remain unchanged. The main objective is to determine whether the image has been modified or not, with the possibility of locating and reconstructing image regions that have been tampered. A fragile marking system should be able to detect any changes made in a cover image. The fragile watermark should not be visible under normal viewing conditions, that is the watermark should not alter the quality of the image in a large extent. In fragile watermarking the detector should be able to locate and characterize alterations made to an image by the provision of the correct key. Otherwise the detector should resemble random noise or provide an image which is commercially valueless.

3.2 Content-based Image Authentication or Selective Authentications

Content modification is defined as an object appearance or disappearance, a modification to an object position, or changes to texture, color or edges. Lot of applications that base their decisions on images, need authentication methods that can tolerate content preserving manipulations while at the same time detect any manipulation that change the image content. This leads to new watermarking methods known as semi fragile watermarking, and to new approaches known as content-based signatures. Content-based image authentication technique consists of following techniques.

3.2.1 Semi-fragile watermarking

3.2.2 Image authentication by digital signatures based on the image content

3.2.1 Semi-fragile watermarking

Robust watermarking is designed to resist all attempts to destroy the watermark. Its main application includes the intellectual property protection and owner identification [2]. The robustness of the

embedded watermark is crucial to resist any intentional and even unintentional manipulation. The goal of these techniques is not the verification of the image authenticity, but rather the verification of their origins. Conversely, fragile watermarking is designed to easily destroy the embedded watermark following any kind of manipulations of the protected image. It is useful for applications where strict authentication is needed, that is where the main objective is to determine whether the image has been modified or not, with the possibility of locating and reconstructing image regions that have been tampered.

Semi-fragile watermarking combines characteristics of fragile and robust watermarking techniques. Basically, the idea of semi-fragile watermarking is to insert a watermark in the original image in such a way that the protected image can undergo some specific image processing operations while it is still possible to detect alterations and to locate and restore image regions that have been altered [4]. Semi fragile watermark is a watermark which is designed to break under all changes that exceed a user specified threshold value. Semi fragile watermarking system accepts some acceptable manipulations such as JPEG lossy compression and reasonable brightness adjustment on the watermark image. Images with excessive compression rate are considered as unauthenticated image due to poor quality. Semi fragile watermarking identifies the position of corrupted blocks and recovers them with approximation of the original image content.

3.2.3 Image authentication by digital signatures based on the image content

Most recent investigations in image authentication domain were concentrated on digital signatures applied to the digital image content; these approaches offer high performance. The digital signature consists of extracting unique features from the image at the source side and encoding these features to create digital signatures. Afterwards signatures are used to verify the image integrity by signature comparison at the detection side.

Such systems consist of;

- Extracting specific high level characteristics from the original image;
- Applying a hash function to these characteristics in order to reduce their size;
- Digitally signing the hash value using an existing digital signature algorithm such as a private or public key system to increase the overall security;
- Attaching the signature to the original image or inserting it in the image using techniques for data dissimulation.

Likewise, the verifying procedure of an image authenticity consists of;

- Generating the image signature using the same algorithm;
- Extracting the attached or dissimulated signature;
- Comparing these two signatures using a comparison algorithm to decide whether the image was altered or not;
- Determining the image regions that were manipulated.

4. Application of Image authentication system

[1] Image authentication system verifies the originality of an image by detecting malicious manipulations.

[2] image authentication system are used to ensure the integrity of an image, particularly for document images such as important certificates, scanned checks, art drawings, signed documents, circuit diagrams, design drafts etc.

[3] For highly confidential document image transmission various image authentication methods can be used.

5. CONCLUSION

In this paper we categorize digital image authentication techniques into strict image authentication and content based or selective image authentication.

Strict image authentication technique does not tolerate any changes in the image data. Strict image authentication again categorized in to conventional cryptography and fragile watermarking. Conventional cryptography compute authentication data using hash function and then this hash is encrypted and appended to image. The receiver computes the hash from the received image. The hash that was appended to the received image is extracted and decrypted. The extracted hash and the calculated one are then compared. Fragile watermarking techniques generate a watermark for a set of image pixels and insert it in the image to be protected in such a way that any modification made to the image is also reflected in the inserted watermark. Verifying the presence of the inserted watermark allows the image authenticity verification and eventually localization of tampered regions.

Content based image authentication technique authenticate image based on change in image content and can tolerate content preserving manipulations. Content based image authentication again categorized in to semi fragile watermarking and authentication using digital signature. The digital signature extracts unique features from the image at the source side and encoding these features to create digital signatures. At the detection side signatures are used to verify the image integrity by signature comparison. Semi-fragile watermarking is to insert a watermark in the original image in such a way that the protected image can undergo some specific image processing operations while it is still possible to detect alterations and to locate and restore image regions that have been altered.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] Chih-HsuanTzeng and Wen-Hsiang Tsai, “A new approach to authentication of Binary image for multimedia communication with distortion reduction and security enhancement,” IEEE communication letters, VOL.7.NO.9, 2003.
[6] C Yu, X Zhang “Watermark embedding in binary images for authentication”, IEEE Trans. Signal Processing, VOL.01, no.07, pp.865-868, September. 2004.
[7] 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