Authentication Scheme for Document Type Image

Mona Mulchandani
Department of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India.

Sonia Bajaj
Department of Computer Science and Engineering
Jhulelal Institute of Technology
Nagpur, India

***Abstract*: Nowadays, Internet has become a common communication medium to transfer multimedia data. This multimedia data includes digital images of text documents, scan copies of certificates, circuit diagrams, design drafts, signed cheques. It is a challenging task to maintain integrity and authentication of these images as they are transmitted over insecure network-Internet. The fast evolution of digital technologies has made it easy to make modifications to the contents of digital images leading to an urgent need to ensure the integrity and authenticity against various attempts to manipulate them.**

There are various digital images whose security must be protected and hence it is important to design effective image authentication schemes to maintain integrity and authenticity of such images. The aim of this paper is to present a comparison of various techniques for image authentication such as Robust Hashing scheme, Shamir Secret scheme, Image based authentication over wireless transmission with AWGN. Methods are classified according to the service they provide whether strict or selective authentication. The performances of various schemes are discussed based on factors such as localization of tampered region and robustness against the various operations performed on the image. Furthermore, we discuss the concept of Secret Sharing technique for Image Authentication and discuss the most important requirements for an effective image authentication system design.

Keywords- Robust hashing scheme, Shamir secret scheme, image authentication.

1. INTRODUCTION:

1.1 Image Authentication: Image authentication varies the originality of an image by detecting malicious manipulations. The adage that “the photograph doesn't lie" is no longer true because of the powerful image manipulation software. It is very difficult to analyze the difference between original and manipulated image. The technical advancement has reduced the importance that the photography was use to achieve.

Image authentication techniques are employed to detect the changes obtained from manipulation at different stages from transmission to the storage. An Image authentication technique is said to be reliable if the image obtained is the same as it was at the original stage of use. Authentication of digital images/ documents has recently gained great importance due to its requirements for numerous applications. The various Government/ commercial departments like Military, Medical, Accounting, Engineering etc .have important documents that are stored in a digitized form and need to be protected against any manipulations because digital images are increasingly transmitted over Internet. These manipulations can violate the decisions based on these images. The preservation of authenticity of these images is the main purpose behind the various proposed approaches. A good image authentication should not only consider the security issues but also be able to prevent image tampering and also maintaining the visual quality of the image.

2. DIFFERENT TECHNIQUES FOR IMAGE AUTHENTICATION

1. Strict Image Authentication
2. Content-based Authentication

2.1 Strict image authentication does not take any changes to the image. These methods can be further categorised in two groups:

i. Conventional cryptography
ii. Fragile Watermarking.

Cryptography is the main key to Image authentication methods. It computes 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.

Techniques that are based on the hash computing of image lines and columns are known as line–column hash functions. Separate hashes are obtained for each line and each column of an image. The authentication of image is obtained after comparing the existing hashes with those obtained while the image is 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 produces satisfying results with high tamper detection. 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, hence localization performance of these algorithms are not very good.

Fragile watermarking is a technique consists inserting the computed watermark (authentication data) into an image. A digital watermark is called *fragile* if it has undergone slight changes (broken or distorted). Fragile watermarking techniques first generates a watermark for a set of image pixels then it inserts it in the image to be protected. This watermark serves as a measure to check authenticity, if any changes are made in the image then it clearly reflects onto this watermark. It also helps in detecting the tampered regions of the image. 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 features supporting the reconstruction of the image regions that have been tampered.

2.2 Content-based authentication as the name says is capable of tolerating any changes made in the content of the image. The content of the image can be preserved by two ways:

i. Digital signature/ content-based signature method.
ii. Watermark method.

A digital signature method involves extraction of various unique features from the image at transmission side from which then the digital signatures are encoded. These signatures are stored for later use. Upon the receiving side, these digital signatures are decoded back and then these two signatures are compared to verify the image authenticity. Signature-based methods can work on both the integrity protection of the image and repudiation prevention of the sender. Watermarking, on the other hand, really embeds a message into an image data and the hidden message is later extracted to verify the authenticity of image content. Watermark-based approaches work only for protecting the integrity of the image. The major difference between a watermark and a digital signature is that embedding process of the former requires the content of the media to change.

3. RELATED WORK

Yan Zhao, Shuoz Hong Wang,, Pinang Zhang, and Hang Yao [4], proposed a system in which an image hashing method. This system integrates both the local and global features. The Zernike moments represents the global features such as luminance and chrominance characteristics of the image. The position and texture of the image comprises the local features. Hashes produced with the proposed method are robust against common image processing operations. Collision probability between hashes of different images is not high. The proposed system has certain advantages such as:

- Good ROC performance.
- Supports noise contamination.
- Provides Jpeg coding.

Despite of the various advantages the success of this proposed system is dependent on the accuracy of saliency detection for improved performance and as well as to enhance the hash's sensitivity to small area tampering while maintaining good robustness against normal image processing.

Fouzia Sultana, Stephen Charles and A.Govardhan [6], introduced a content-based authentication scheme that exploits the scalability of a structural digital signature. This scheme is mainly used to produce good authentication rate over wireless media. This proposed work uses a technique for secured transmission over wireless channel using image features extracted depending upon wavelet transform . The various advantages of this scheme is as follows:

- It produces good authentication rate even when the channel error and tampering attempts are more.
- Useful for networked image applications.
- AES encryption technique is used for protection.

This scheme however faces certain drawbacks such as generating one fixed-length digital signature per image regardless of the image size and packet loss during the transmission. In order to achieve security this scheme demands adoption of a filter parameterisation technique.

Mrs G Niranjana and Ms K Siva Shalini [5], proposed a method based on the shares which are like secret messages capable of providing data security for binary documents. These binary documents are in the portable network graphics form. It is necessary to hide the important regions of our image by such secret messages so that the data is not easily available to the unauthorized user .Each pixel value of a secret image is a secret message. A block of document image is responsible for generating authentication signals. These signals are merged with the binaries block content to transform into several shares using the Shamir secret sharing Scheme.

4. PROPOSED RESEARCH METHODOLOGY

The authentication methods developed to copyright/protect the information contained in the digital images are helpless by a common drawback. The fast growth of the internet technology development has made it possible to get lots of duplicated information and hence the copyrighted material is no more authenticated.

To provide information security, an innovative approach has been proposed. This method is useful in preserving authentication of the image by hiding the secret information on an alpha channel plane which overcomes the drawback of a single- information carrier that can be destroyed or lost by an attacker easily thereby disappearing the secret information.

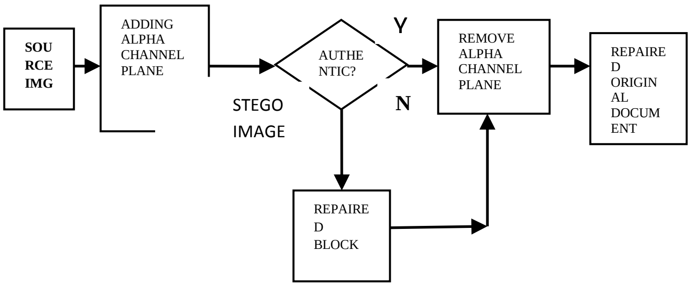

Fig: Framework of proposed document image authentication method

An Authentication method providing data security based on secret sharing technique is proposed and its framework is as shown in the figure above. This technique provides data repair capability for image by using Portable Network Graphics. . A block of document image is responsible for generating authentication signals. These signals are merged with the binarised block content to transform into several shares using the Shamir secret sharing scheme. This binary document with an alpha channel plane is employed to create a PNG image. This methodology aims to distribute the secret information by collecting enough numbers of multiple carriers. Hence this methodology combines both the features of "data hiding" and "secret sharing" together to provide information security to the image.

The source document ie; the gray scale document is combined with the binarized block content and is converted into several shares with secret Shamir scheme. A portable network graphics is the resultant we obtain from binary document. This is then integrated onto the alpha channel plane. The original image may be thought of as a gray scale channel plane of the PNG image. The alpha channel provides destruction-free carrying of the input image for authentication and repair.

The secret sharing scheme is used in the proposed methodology to carry authentication signals as well as for repairing the violated image content through use of shares. To data repair the image content the cover image is destroyed first so that the original data are not available for data repairing.

5. CONCLUSION

The proposed methodology involves both data repair capability and security for gray-scale images which are binary like, where alpha channel plane plays the most important role in maintaining security and the use of secret sharing methods is responsible for maintaining the authentication of image. Stego-Image has the capability of repairing the tampered parts of an authenticated image. Reverse Shamir scheme can also be implemented to provide self-repairing provision for the content of tampered block and also to compute the original content of block from any two un-tampered shares. Measures for enhancing the security of the data embedded in the alpha channel plane have been also proposed.

REFERENCES:

[1] Chih-HsuanTzeng and Wend-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.

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

[3] Meng Guo, Hongbin Zhang, "High capacity data hiding for binary image authentication,'' International Conference on System Science and Engineering (ICSSE), 2010.

[4] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust Hashing for Image Authentication Using Zernike Moments and Local Features," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 1, JANUARY 2013

[5] Mrs.G.Niranjana, Ms.K.Siva Shalini, " Authentication of grayscale document images using shamir secret sharing scheme," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VII (Mar-Apr. 2014), PP 75-79 www.iosrjournals.org

[6] Fouzia Sultana, Stephen Charles, A. Govardhan, " A Tamper Proof Noise Resilient End to End Image Based Authentication System over Wireless Transmission with AWGN Channel using Wavelet Based Templates and AES," IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.7, July 2014 58.

[7] Reshma Varta, Smita Deshmukh, "Survey of Digital Image Authentication Techniques," International Journal of Research in Advent Technology, Vol.2, No.7, July 2014 E-ISSN: 2321-9637.