IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Authentication and Data Repairing of Document Image using Steganography Method

Rahil Khan[1], Ruhina Quazi[2]

Assistant Professor, ETC Department, Anjuman College of Engg & Tech., Nagpur, India [1]

Assistant Professor, ETC Department, Anjuman College of Engg & Tech., Nagpur, India [2]

Abstract: This paper attempts to propose a novel technique of blind authentication based on the method of secret in addition to data repair capability for grayscale document images through the use of the Portable Network Graphics (PNG) image. For every block of a grayscale document image, an authentication signal is generated, which, along with the block content in binary, is transformed into numerous shares using the Shamir secret sharing scheme. The parameters involved are carefully selected so that as many shares as possible can be generated and embedded into an alpha channel plane. After this, the alpha channel plane is combined with the original grayscale image to yield a PNG image. During this process, the computed share values are recorded as a range of alpha channel values near their maximum value of 255 to return a transparent stego-image with a disguised effect. In the image authentication process, marking of an image block is done as tampered, if the authentication signal computed from the current block content does not match the one extracted from the shares embedded in the alpha channel plane. Each tampered block is then subjected to data repairing by a reverse Shamir scheme after collecting two shares from unmarked blocks. Procedures to protect the safety of the data that lies concealed in the alpha channel have been proposed. Decent experimental results demonstrate the efficiency of the proposed method.

Keywords: Data hiding, data repair, grayscale document image, image authentication, Portable Network Graphics (PNG) image, secret sharing.

I. INTRODUCTION

A novel blind authentication technique based on the secret sharing technique in addition to data repair capability for grayscale document images through the use of the Portable Network Graphics (PNG) image. For every block of a grayscale document image, an authentication signal is generated, which, along with the block content in binary, is transformed into numerous shares using the Shamir secret sharing scheme. The parameters involved are carefully selected so that as many shares as possible can be generated and embedded into an alpha channel plane. After this, the alpha channel plane is combined with the original grayscale image to yield a PNG image. During this process, the computed share values are recorded as a range of alpha channel values near their maximum value of 255 to return a transparent stego-image with a disguised effect. In the image authentication process, marking of an image block is done as tampered, if the authentication signal computed from the current block content does not match the one extracted from the shares embedded in the alpha channel plane. Each tampered block is then subjected to data repairing by a reverse Shamir scheme after collecting two shares from unmarked blocks. Procedures to protect the safety of the data that lies concealed in the alpha channel have been proposed. Decent experimental results demonstrate the efficiency of the proposed method.

Digital image is a way of preserving important information. However, with the advent of fast advances of digital imaging technologies, it is easy to make visually indiscernible modifications to the contents of digital images. Ensuring of the integrity and genuineness of a digital image is indeed a challenge. So it is needed to project such methods which prove to be effective to decipher this kind of image authentication issue, especially for images of documents whose security must not be compromised. It is also important to note that if some fraction of a document image is corroborated to have been altered illegitimately, the destructed content can be repaired. Such image content authentication and self-repair capabilities are beneficial for protection of security of digital documents in numerous fields, such as important certificates, signed documents, scanned cheques, testaments, art drawings, circuit schematics, design drafts, last will and so on.

Document images, which comprise of texts, tables, line arts, etc. as chief contents, are normally converted into their digital counterpart as grayscale images consisting of two major gray values, one being of the background (including mainly blank spaces) and the other of the foreground (including mainly texts). Such images, although gray-valued in nature, appear to be like binary. As an example, the two major gray values in the document image shown in Fig. 1 are 174 and 236, respectively. It gives the impression that such binary-like grayscale document images may be thresholded into binary ones for processing at a later stage, but such an operation distorts the smoothness of the boundaries of text characters, which causes visually displeasing stroke appearance with zigzag outlines. Therefore, in practical applications text documents are often converted into their digital

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

counterparts and kept as grayscale images for later visual inspection.

Institute of Multimedia and Engineering
College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.

As members of the Final Examination Committee, we certify that we have read the thesis prepared by Jheng-Kuei Huang entitled A Study on Learning and Guidance for Outdoor Autonomous Vehicle Navigation by Two-mirror Omni-directional Imaging and Ultrasonic Sensing Techniques and recommend that it be accepted as fulfilling the thesis requirement for the Degree of Master of Science.

Committee Members:

Thesis Advisor:

Director:

Date: June 18, 2010

II. LITERATURE SURVEY

In general, the problem of image authentication is quite challenging for a binary document image owing to its simple binary nature which causes certain alterations which are distinguishable after the authentication signals are implanted into the image pixels. Such changes have a great possibility of arousing likely suspicions from attackers. A worthy solution to such binary image authentication should take into consideration not only the issue of security to prevent tampering of image, but also the requirement of retaining the visual quality of the resulting image. Here, we intend to suggest an authentication method which deals with binary-like grayscale document images in place of pure binary images, and provides a solution to the complications of image tampering detection and visual quality retention.

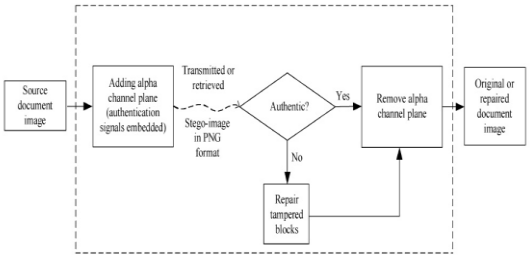
Quite a few approaches have been proposed for binary image authentication in the past. Yang and Kot [5] proposed a binary image authentication method consisting of two layers wherein one layer is utilized to check the image fidelity and the other layer to verify the image integrity. A connectivity-preserving transition criterion to determine the flippability of a pixel is used to embed the cryptographic signature and block identifier. Wu and Liu [4] worked on the so-called flippable pixels to generate specific associations to embed data for the purpose of authentication and annotation of binary images. Again, Yang and Kot [6] suggested a method of hiding the data based on pattern for authentication of binary image, in which three transition benchmarks are used to govern the flippabilities of pixels in each block, and the watermark is embedded in an adaptive manner into embeddable blocks for dealing with the condition of uneven embed ability in the host image.

Kim et al. [7] proposed a method in which a set of pseudo-random pixels present in a binary image are selected and cleared, and authentication codes are calculated accordingly and implanted into designated random pixels. In Tzeng and Tsai's method [8], image blocks are subjected to randomly-generated authentication codes for its use in image authentication, and a so-called code holder then reduces the distortion in image which is the result of data embedding. Lee et al. [9] proposed a data embedding method based on Hamming-code which flips a single pixel in each block of binary image in order to embed a watermark, resulting in minor distortions and low false negative rates.

Lee et al. [10] later on enhanced the method by employing an edge line resemblance measure to select flippable pixels so as to reduce distortion. In this study, a method of document image authentication with an additional self-repair capability to fix data of tampered image is discussed. The input cover image is presumed to be a like a binary grayscale image with two major gray values like the one shown in Fig. 1. After the proposed method is applied, the cover image is altered into a stego-image with the Portable Network Graphics format with an additional alpha channel for network transmission or archiving in the databases. The stego-image, when either received or retrieved, may be verified by the proposed method for its authenticity. Detection of integrity modifications of the stego-image can be done by the method at the block level and repaired at the pixel level. In case of removal of alpha channel from the stego-image entirely, the complete resulting image is considered as inauthentic, which means that the image fails the fidelity check. The proposed method is based on the (k, n)-scheme of threshold secret sharing proposed by Shamir [11] in which transformation of a secret message is done into n shares in order to keep by n participants; and when k of the n shares are collected, not necessarily all of them, we can have a lossless recovery of the secret message. Such a scheme of secret sharing is beneficial to reduce the risk of incidental partial data loss.

Usually, the concepts of "secret sharing" and "data hiding for image authentication" are two unrelated issues in the area of information security. But in the proposed method, we have combined them together for developing a novel image authentication technique. The secret sharing scheme is used in the developed technique not just to transmit authentication signals along with image content data, but also to assist towards repairing of the tampered data through the use of shares.

III.PROPOSED ALGORITHM



In this study, a method of document image authentication with an additional self-repair capability to fix data of tampered image is discussed. The input cover image is presumed to be a like a binary grayscale image with two major gray values like the one shown in Fig. 1. After the proposed method is applied, the cover image is altered into a stego-image with the Portable Network Graphics format with an additional alpha channel for network transmission or archiving in the databases. The stego-image, when

DOI 10.17148/IJARCCE.2016.56165

either received or retrieved, may be verified by the proposed method for its authenticity. Detection of integrity modifications of the stego-image can be done by the method at the block level and repaired at the pixel level. In case of removal of alpha channel from the stego-image entirely, the complete resulting image is considered as inauthentic, which means that the image fails the fidelity check. The proposed method is based on the (k, n)-scheme of threshold secret sharing proposed by Shamir [11] in which transformation of a secret message is done into n shares in order to keep by n participants; and when k of the n shares are collected, not necessarily all of them, we can have a lossless recovery of the secret message. Such a scheme of secret sharing is beneficial to reduce the risk of incidental partial data loss.

Usually, the concepts of "secret sharing" and "data hiding for image authentication" are two unrelated issues in the area of information security. But in the proposed method, we have combined them together for developing a novel image authentication technique. The secret sharing scheme is used in the developed technique not just to transmit authentication signals along with image content data, but also to assist towards repairing of the tampered data through the use of shares.

A major topic of discussion in the self-repairing of tampered data at attacked image parts is that, after the original cover image data is embedded into the image itself to use in data repairing later on, the cover image is itself destroyed in the first place and the original data is now no longer available for the purpose of data repairing, which results in a contradiction. A solution to this difficulty is to embed the original image data somewhere else without varying the cover image itself. The technique proposed in this paper to implement this solution is to utilize the extra alpha channel in a PNG image so as to embed the original image data. However, the use of alpha channel of the PNG image is done to create a desired degree of transparency for the image. Moreover, data embedding into the alpha channel will create random transparency in the resulting PNG image, which will produce an unwanted opaque effect. One way out, as proposed in this paper, is to map the resulting alpha channel values into a small range near their extreme value of 255, resulting in an almost undetectable transparency effect on the plane of alpha channel.

There is another difficulty faced during the self-repairing of the original image data, that the data to be embedded in the carrier are often large in size. This is not a problem for our case where with the alpha channel as the carrier, the cover image that is dealt with is basically binary-like, and hence, we may just embed into the carrier a binary version of the cover image, which includes much less data. Additionally, through a cautious design of authentication signals, an appropriate selection of the basic authentication unit (i.e., the unit of 2 x 3 image block) and a good parameter adjustment in the Shamir scheme, we can reduce the data volume of the generated shares commendably so that more shares can be embedded into the alpha channel plane. It is noted that, by the proposed method, the larger the number of shares is, the higher will be the resulting data repair capability. As a final point, we allocate the multiple shares in a random manner into the alpha channel to allow the share data to have great likelihoods of surviving attacks and to thus stimulate the data repair capability. To the best of our knowledge, this can be considered to be the first secret-sharing-based authentication method for binary-like grayscale document images. It is also the first authentication method for such document images through the use of the PNG image. It is also worth noting that this method is not a secret-sharing technique but a method of document image authentication.

IV. PROPOSED SOFTWARE DESCRIPTION

MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and FORTRAN" –

Over the years MATLAB as a tool has become more and more user friendly and today using MATLAB is quite easy and hence it is possible to implement our projects in MATLAB. MATLAB is an extensive software with possibilities for final year projects in many different domains. With MATLAB projects are possible in the following primary domains

- Image Processing Projects
- Digital Signal Processing Projects
- Electrical Projects
- Fuzzy Logic Projects
- Neural Network Projects
- ANFIS Projects
- Embedded Projects

MATLAB is one of the most widely used technology software in the world and hence naturally lots of IEEE papers based on MATLAB are published on a daily basis. One of the specific areas where MATLAB is at an advantage is Image processing. Image processing projects in MATLAB are a very good choice for project work, because of the extensive image processing capabilities of MATLAB.

V. FUTURE SCOPE

The probable future studies can take several directions, which include choice of alternative block sizes and connected parameters (prime value range, value for secret sharing, range of authentication signal bits, etc.) to enhance data repair effects.

Some security procedures to enhance the protection of the data embedded in the alpha channel plane is also specified. Applications of the proposed method for authentication and repairing of attacked color images, and block based owner validation may also be applied.

REFERENCES

[1] C. S. Lu and H. Y. M. Liao, Multipurpose watermarking for image authentication and protection, IEEE Trans. Image Process., vol. 10, no. 10, pp. 15791592, Oct. 2001.

[2] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, Hierarchical watermarking for secure image authentication with localization, IEEE Trans. Image Process., vol. 11, no.6, pp. 585595, Jun. 2002.

[3] Z. M. Lu, D. G. Xu, and S. H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, IEEE Trans. Image Process., vol. 14, no. 6, pp. 822831, Jun. 2005.

[4] M. Wu and B. Liu, Data hiding in binary images for authentication and annotation, IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528538, Aug. 2004.

[5] H. Yang and A. C. Kot, Binary image authentication with tampering localization by embedding cryptographic signature and block identifier, IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741744, Dec. 2006

[6] H. Yang and A. C. Kot, Pattern-based data hiding for binary images authentication by connectivity-preserving, IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475486, Apr. 2007

[7] H. Y. Kim and A, Secure authentication watermarking for halftone and binary images, Int. J. Imag. Syst. Technol., vol. 14, no. 4, pp. 147152, 2004.

[8] C. H. Tzeng and W. H. Tsai, A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement, IEEE Commun. Lett., vol. 7, no. 9, pp. 443445, Sep. 2003.

[9] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, A new binary image authentication scheme with small distortion and low false negative rates, IEICE Trans. Commun., vol. E90-B, no. 11, pp. 32593262, Nov. 2007.

[10] Y. Lee, H. Kim, and Y. Park, A new data hiding scheme for binary image authentication with small image distortion, Inf. Sci., vol. 179, no. 22, pp. 38663884, Nov. 2009.

[11] A. Shamir, How to share a secret, Commun. ACM, vol. 22, no. 11, pp. 612613, Nov.1979.

[12] C. C. Lin and W. H. Tsai, Secret image sharing with steganography and authentication, J. Syst. Softw., vol. 73, no. 3, pp. 405414, Nov./ Dec. 2004.

[13] W. H. Tsai, Moment-preserving thresholding: A new approach, Comput. Vis. Graph

DOI 10.17148/IJARCCE.2016.56165