Asian Journal of Engineering and Technology Innovation 02 (05) 2014 (30-32)

Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Received on: 01-12-2014
Accepted on: 10-12-2014
Published on: 22-12-2014

Vaibhav Malave, Sarika Deokate, Vikas Nagargoje, Namdev Kadam, Sourabh Aglave
Computer Engineering Department, Indira college of engineering and Management Pune University, Maharashtra, India
vabhav.malave2012@gmail.com
sarikajaankar@gamil.com
vikasnagargoje1@gmail.com
namdev.kadam1993@gmagm.com
sraglave@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared !

Color Image Tampering Detection And Repairing of Tampered Block

Vaibhav Malave, Sarika Deokate, Vikas Nagargoje, Namdev Kadam, Sourabh Aglave
Computer Engineering Department, Indira College of Engineering and Management Parandwadi, Pune.

Abstract:
This is new authentication scheme based on the secret sharing technique with a data repair capability for document type color image via the use of PNG image i.e. portable network graphics images. An authentication signal i.e. a1 and a2 are generated for each block of document type color images, which is transformed into a several shares using the secret sharing Scheme. The characters which is involves are carefully chosen so that many shares as possible are generated and embedded into an alpha channel plane. The alpha channel is then combined with the original image to form a stego image in the PNG format. During the embedding process, the shares which are computed from secret sharing, values of this computed shares are mapped into a range of alpha channel value near their maximum value of 255 to yield a transparent stego image in the PNG format. In the process of image authentication, an image block is marked as a tampered if the authentication signal computed from the current block content does not match that extracted from the share embedded in the alpha channel plane. Data repair scheme is applied to each tampered block after collecting two shares from unmark block.

Keywords: Authentication, Data Hiding, Secret Sharing, Data Repair.

Cite this article as:
Vaibhav Malave, Sarika Deokate, Vikas Nagargoje, Namdev Kadam, Sourabh aglave. color image tampering detection and repairing of tampered block, Asian Journal of Engineering and Technology Innovation 02 (05); 2014; 30-32.

INTRODUCTION:

Digital image is a form for preserving important information. However, with the fast advance of digital technologies, it is easy to make visually unnoticeable modifications to the contents of digital images. How to ensure the integrity and the authenticity of a digital image is thus a challenge. It is desirable to develop methods to solve this kind of image authentication problem, particularly for images of documents whose security is important. If part of a document image is verified to have been illegally altered, the destroyed content can be repaired. Such image content authentication and self-repair capabilities are useful for the security protection of digital documents in many fields, such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Thus we are going to develop an authentication method for color image to solve the problem of image tampering detection and visual quality keeping.

SCOPE:

Most techniques are available for image authentication. They also provide detection of tampered block. Some techniques are available to repair tamper block. These techniques are restricted to some image formats such as binary documented image or gray-scale image. Current market demands an efficient technique for color image authentication and detection of tampered block and repairing detected tampered block.

RELATED WORK DONE:

The paper [1], proposed a method which scanned text, figures, and signatures are embed in binary images. In order to embed a data without causing perceptible artifacts the method manipulates “flippable” pixels. Shuffling is applied before embedding to equalize the uneven embedding capacity from region to region.The proposed data embedding method can be used to detect unauthorized use of a digitized signature, and comment or authenticate binary documents. Data hiding techniques for these authentication and annotation purposes are discussed in this paper, this method is alternative to the cryptographic authentication approach. Such targeted applications calls for fragile or semi fragile embedding of many bits. It should be stressed that while it is desirable for the embedded data to have some robustness against minor distortion and preferably to withstand printing and scanning, the robustness of embedded data against intentional removal or other obliteration is not a primary concern. Advantage of this scheme is that this method can be applied to detect unauthorized use of signatures in binary image format, to detect alterations on documents, and to annotate signatures and drawings. Disadvantage of this scheme is that this method is applicable to binary images only i.e. it is not applicable to binary images such as text, binary drawings.

In paper [2], author proposed the method in which semi-fragile watermark and the robust watermark are embedded in different VQ stages using different techniques, and both of them can be extracted without the original image. In the proposed algorithm, in the first stage by using the embedding method presented the robust watermark is embedded, and in the second stage by using a novel index constrained method the semi-fragile watermark is embedded. Although the encoded indices of the attacked watermarked image may be very different from the original ones, the variance of neighboring indices does not vary too much. The first-stage watermarking method is robust. The second-stage watermarking method can tolerate few modifications, so it is fragile to most intentional attacks. The proposed method can be used for copyright protection by extracting the first-stage watermark, and it can also be used for image authentication by extracting the second-stage watermark. Advantages of given system are, the proposed algorithm can tolerate rotation attacks with relatively larger angles. The semi-fragile and robust watermarks are extracted independently and blindly. In the embedding and the extraction processes different codebooks are used. The extraction process sometimes can be performed publicly for special applications as the final product codebook can be public for users. The proposed algorithm can be extended to be used in e.g., digital fingerprint, copyright protection and image authentication, by embedding three watermarks in a three-stage VQ. The amount of the data transmitted can be reduced by using VQ-based watermarking algorithm. Disadvantages of system are, the quality of the watermarked image obtained is not high enough for copyright protection. Proposed algorithm cannot tell what kind of attack the watermarked image suffers from. The human visual characteristics are not adopted in the VQ-based watermarking systems. This is time consuming process if we use the full-search encoding algorithm.

In paper[3], author proposes two layer authentication techniques for binary image. In the first layer overall authentication is achieved. In the second layer tampering is detected. The “connectivity- reserving” transition criterion is used to determine the “flip ability” of a pixel. The image is divided into multiple macro-blocks that are classified into eight categories. For each class block identifier is defined adaptively and in order to identify the tampered locations they areembedded in those “qualified” and “self-detecting” macro-blocks. In the first layerby hiding the cryptographic signature of the image overall authentication is achieved. In the second layerby embedding the block identifier in the “qualified” or “self-detecting” macro-blocks the localization of the tampering is detected. Specifically, they group multiple overlapping 3X3 blocks and MBs are formed and MBs are classified to “qualified” macro-blocks and based on the number of “flippable” pixels Nf “unqualified” macro-blocks. The QMBs are chained, and to identify the tampering occurred both to the QMB and its neighboring UMB the BI that is usedis embedded. Advantage of this system is effective in detecting tampering, and the tampered locations can be identified. Disadvantage is the MB size should be chosen such that a good balance can be made between the capacity required for the localization accuracyand embedding CS. If MBs that do not have enough “flippable” pixels to embed a complete BIMismatch detection and the false alarm are most likely occurred.

In paper [4], author presented a different blind data hiding schemebased on connectivity-preserving of pixels for binary images authentication. To assess the “flip ability” of a pixel in a block a window of size 3 X 3 is selected. No side information is required for the water-mark retrieval due to the feature of the data embedding process. Based on the three transition criteria embedding the watermark is handle by the “uneven embed ability” of the input binary image. A smaller block size is chosen.

For different applications different types and sizes of block can be chosen to increasing the data hiding capacity. Also address the problem in a block for different block schemes that how to locate the "embeddable" pixels, which facilitates authenticity and integrity of the image. Advantage of the proposed scheme is that it can be applied to a wide variety of binary images authentication. Disadvantage is the interlaced block scheme is the most time-consuming due to the largest number of blocks.

In paper [5], a method for authentication of grayscale document image is proposed. It provides capability of detection of tampered block and recovery of tampered block if any found. Authentication signal is calculated for each block of garyscale document image. By using Shamir's secrete sharing algorithm binarized block contents which are transformed into some partial shares. Alpha channel contains both authentication signal calculated and partial shares. The alpha channel plane is then added with the original grayscale image to form a PNG image. During the embedding process, the computed share values are mapped into a range of alpha channel. Stego-image is verified by the proposed method for its authenticity. Authentication of the stego-image can be done by the method at the block level and repairing of tampered block at the pixel level. When the alpha channel is totally removed from the stego-image, the entire resulting image is marked as inauthentic. In the process of image authentication, if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane an image block is marked as tampered. The proposed method is based on the Shamir's so-called –(k, n) threshold secret sharing scheme in which for keeping by participants a secret message is transformed into shares, and when shares are collected, not necessarily all of them, the secret message can be losslessly recovered. To repair data reverse secret sharing scheme is applied. Advantage of this method is that it is able to authenticate the image and also provide capability of tamper detection and recovery of tampered block. Disadvantage of the method is that it is applicable to grayscale image only.

CONCLUSION:

Different image authentication techniques some with tamper detection are studied. All this methods are applied to binary images only. All methodsare capable of checking authenticity of image, but only few of them are able to mark tampered block. Only method proposed by Lee and Tai is able to repair tampered blocks to some extent. Future work can be detection of tampered block and repairing them for color image.

REFERENCES:

1. Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving, Huijuan Yang and Alex C. Kot, Fellow, April 2007.
2. Efficient Image Tamper Detection and Recovery Technique using Dual Watermark, Surya BhagavanChaluvadi and Munaga V. N. K. Prasad, 2009.
3. A RESTORATIVE IMAGE AUTHENTICATION SCHEME WITH DISCRIMINATION OF TAMPERS ON IMAGE OR WATERMARK, Ke KE, Tao Zao and Ou Li, 2010.
4. Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving, Huijuan Yang and Alex C. Kot, Fellow, April 2007.
5. A Secret-Sharing-based Method For Authentication Of Gray-scale Document Image Via The Use Of The PNG With Data Repair Capability , Che-Wei Lee and Wen-Hsiang Tai, January 2012.