ISSN: 2321-7782 (Online)
Volume 2, Issue 4, April 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

A Blind Authentication Scheme for Document Type Color Images with Data Repair Capability

Ashwini V. Kurzekar[1]
Department of CSE
Priyadarshini Institute of Engineering & Tech.
Nagpur – India

Dr. A. R. Mahajan[2]
Department of CSE
Priyadarshini Institute of Engineering & Tech.
Nagpur – India

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 together with the binarized block content, 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: Image Authentication, Data Hiding, Secret Sharing, Portable Network Graphics, Data Repair.

I. INTRODUCTION

Image transmission is a major activity in today's communication. Digital images are now widely distributed via the internet and various public channels. With the advance of digital technologies; it is now easy to modify digital images without causing noticeable changes, resulting possibly in tampering of transmitted images. It is desirable to design effective method for image authentication, aiming to check the fidelity and integrity of received images. There is an urgent need for copyright protection against the unauthorized data reproduction.

The conventional copyright protection technologies such as authentication mechanism that is employed for digital content applications are helpless by a common drawback. The illegal reproduction of the copyrighted material can no longer be prevented. Once the image is authenticated and if someone can make some modification in that image, that time we cannot say that the image is authenticated.

A. Image Authentication

Authentication of any digital type documents has the great interest due to their wide application areas such as important certificates, digital books, important legal documents and engineering drawings. Important documents such as fax document, insurance copy and personal documents in the digitized form and stored. It is very important that how to ensure the authenticity and integrity of the documents. And on the other hand, the powerful image editing software tool is available which copying and editing an image more easily with less noticeable changes. Authentication and detection of tampering are thus main goal. Data hiding or watermarking for binary images authentication has been a promising approach to alleviate these concerns. Most prior

works on data hiding with watermarking focus on grayscale or color images in which the pixel takes a different range of values, which is slightly perturbing the pixel value by a small amount causes no perceptible distortions.

Digital Image is used to preserving important information. But, with the advance of digital technologies, it is easy to make modifications to the contents of digital images. So, How to ensure the integrity and the authenticity of a digital image is thus a big challenge. It is desirable to design effective methods to solve this kind of image authentication problem which comes particularly for document type images whose security must be protected. And, if some part of a document image is verified to have been illicitly altered, then 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 a certificates, signed documents, art drawings, scanned checks, design drafts, circuit diagrams, last will and testaments, and so on. Document images, which include texts, line arts, tables etc.

B. Data Hiding

Data hiding represents is a processes which is used to embed data into an image, like as different copyright information, which is hide into the various forms of media such as image, audio, text with a minimum amount of perceivable degradation to the "host" signal; i.e., the data which is embedded into an image should be invisible and inaudible to a human.

Data hiding is a one of the form of steganography, in which embeds data into digital media for the purpose of annotation, identification and copyright. Several constraints which is affect to this process i.e. the quantity of data to be hidden into an image, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, As well as the degree to which the data modification, or data removal by a third party. So for that the two important data hiding in digital media are to provide proof of the copyright, and assurance of image content integrity.

II. LITERATURE SURVEY

H. Yang and A. C. Kot *et al.* [1] proposed a novel blind data hiding method for binary images authentication aims at preserving the connectivity of pixels in a local neighborhood. Data hiding method which is pattern based for binary image authentication in which three transition criteria are used to determine the flippabilities of pixels in each block, the watermark is embedded into embeddable blocks that deal with the uneven embeddability condition which present in the host image.

The "flippability" of a pixel is determined by imposing three transition criteria in a 3*3 moving window centered at the pixel. The "embeddability" of a block is invariant in the watermark embedding process; hence if want to extract watermark then it can be extracted without referring to the originl image. The "uneven embeddability" of the host image is handled by embedding the watermark in only those "embeddable" blocks in an image.

Yang and Kot et al. [2] proposed a two-layer binary image authentication method in which one layer is used for checking the image fidelity and the other layer is for checking image integrity. In this two layer binary image authentication method, a connectivity- preserving transition of pixel criterion is used for determining the flippability of a pixel for embedding the cryptographic signature and for the block identifier. A novel two-layer blind binary image authentication scheme, in which the first layer is design for overall authentication and the second layer, is design for ientifying the tampering locations. The "flippability" of a pixel is determined by the "connectivity-preserving" transition criterion.

The authentication is achieved in the first layer by hiding the cryptographic signature (CS) of the image. The detection of tampering is achieved in the next layer i.e. in second layer by embedding the block identifier (BI).

Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon et al. [3] proposed a new binary image authentication method with small distortion and low false negative rates scheme. Which is based on Hamming-code- data embedding method that flips one pixel in each binary image block for embedding a watermark, which yielding small distortions and low false negative rates.

Y. Lee, H. Kim and Y. Park et al. [4] proposed a data hiding scheme for binary images, which includes the document type images, scanned figures text and signatures. In this data hiding scheme, embedding efficiency and the placement of embedding changes are perform simultaneously. Take M×N image block, the upper bound of the amount of bits that can be embedded of the scheme is nlog2((M×N)/ n +1) by changing n pixels. This scheme is used for embed more amount of data, as well as it maintain a better quality of image, and it has the wider applications. This data hiding scheme embed more amount of data and it will not affected the quality of the image.

Min Wu and Bede Liu et al. [7] proposed a method to embed data into binary images, the images which are scanned text, figures or diagrams, and signatures. It is a data hiding method in which "flippability" of pixels criterion is used to enforce specific block of image in order to embed a significant amount of data without causing noticeable changes into an image. The shuffling of pixels is then applied before embedding data. The hidden data in image can be extracted without using the original image, and data can be extracted from the image after high quality printing and scanning with the help of some registration marks into an image. This data hiding technique which used to detect unauthorized uses of a digitized signature as well as annotate or authenticate binary documents type image.

Min Wu and Bede Liu et al. [8] proposed data hiding in image and video in that they addresses a number of fundamental issues which is related to the data hiding in image and video and proposed the general solutions to them. They proposed a multilevel embedding scheme to allow the extractable data to be adaptive according to the actual noise condition. And the issues related to hiding multiple bits through a comparison of various multiplexing and modulation schemes. As well as the non-stationary nature of visual signals which leads to highly uneven distribution of embedding capacity and causes difficulty in data hiding. Min Wu and Bede Liu proposed solution switching between using constant embedding rate with shuffling and using variable embedding rate with embedded control bits. And apply these different solutions to specific problems for embedding data in grayscale and color images and video.

III. PROPOSED RESEARCH METHODOLOGY

The conventional copyright protection technologies such as authentication mechanism that is employed for digital content applications are helpless by a common drawback. The illegal reproduction of the copyrighted material can no longer be prevented. Once the image is authenticated and if someone can make some modification in that image, that time we cannot say that the image is authenticated.

A well-developed intellectual property rights protection scheme is provided, so for that an innovative approach has been proposed. The proposed method preserves image authentication whatever modification has been made in that image.

Authentication method based on the secret sharing technique with detection of tampering region and data repair capability for color document type images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal i.e. a1 and a2 is generated for each block of a color document image which is together with the binarized block content of an image, is then transformed into several shares using the Shamir secret sharing scheme. PNG image is created from a binary document image with an alpha channel plane. The alpha channel is act like a carrier. The original image may be thought as a grayscale channel plane of the PNG image. Since the alpha channel plane is used for carrying data for authentication and repairing, no any destruction will occur to the input document type color image in the process of authentication. So, first we add the alpha channel to the original color image. Now the image containing the four channels i.e. ARGB. In that 'A' stands for alpha. Alpha channel is used for carrying the authentication signals.

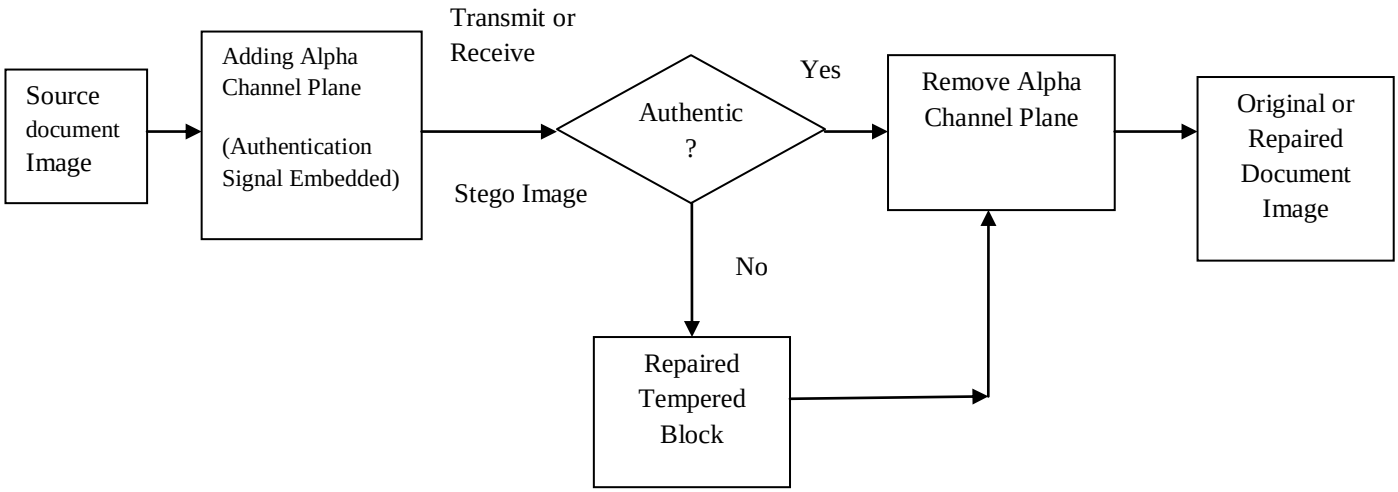

Fig.1 Framework of proposed document image authentication method

The concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security. However, in the proposed method, combine them together to develop a new image authentication technique. The secret sharing scheme is used in the developed technique not only to carry authentication signals and image content data but also to help repair tampered data through the use of shares.

The self-repairing of tampered data in an attack image, after the original data of the cover image are embedded into the image itself for use in later data repairing, but if the cover image is destroyed and the original data which is embedded in that image are no longer available for data repairing, resulting in a contradiction. So in the proposed system to embed the original image data somewhere else without altering the cover image itself. So we proposed the solution for that is using the extra alpha channel in PNG image to embed the original image data. Alpha channel is used for creating transparency in the PNG image. In proposed system is to map the resulting Alpha channel value into small range near their value of 255 yielding an imperceptible transparency effect on the alpha channel plane.

So, in the proposed system, a PNG image is created from binary type color document image, the image containing the alpha channel plane. First change this color image into the grayscale image. Then we get grayscale image, and we consider this grayscale image is original image may thought as a gray scale channel plane of the PNG image. Alpha channel is used for carrying data, which is used for authentication method and for repairing process.

Authentication method causes the destruction in original image to overcome this problem we proposed secret sharing authentication method for document type color image as well as provide the data repairing capacity.

IV. CONCLUSION

An effective image authentication method with data repair capabilities for document type color image based on the secret sharing method has been proposed. The authentication signals are generated and these generated signals and the block of image is then transformed into partial shares by secret sharing method. The alpha channel plane is used to create the stego image in a form of the PNG image. So the shares are embedded into the stego image.

The authentication signals are used to find out the tampered block which is present in that image when the authentication signal are not match to that of extracted partial shares. Self repairing capability is provided to repair original content of the block of image.

References

1. 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. 475–486, Apr. 2007.
2. 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. 741–744, Dec. 2006.
3. 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. Communication., vol. E90-B, no.11, pp. 3259–3262, Nov. 2007.
4. Meng Guo, Hongbin Zhang, "High capacity data hiding for binary image authentication," International Conference on System Science and Engineering (ICSSE), 2010.
5. 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. 3866–3884, Nov. 2009.
6. 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. 3259–3262, Nov. 2007.
7. Min Wu, Bede Liu, "Data Hiding in Binary Image for Authentication and Annotation," IEEE TRANSACTIONS ON MULTIMEDIA, vol. 6, no. 4, August2004.
8. Min Wu and Bede Liu," Data Hiding in Image and Video: Part II—Designs and Applications," IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 12, no. 6, June 2003

AUTHOR(S) PROFILE

Ashwini Kurzekar received the bachelor degree in Computer Science and Engineering from Hanuman Vyayam Prasarak Mandal College of Engineering and Technology, Amravati University in 2011. Her main area of interest includes image processing and data mining. She is now pursuing masters in computer science and engineering from Priyadarshini Institute of Engineering and Technology, Nagpur University.

