International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-5)

Research Article | **May 2014**

Authentication Method for Document Type Colour Images with Data Repair Capability

Miss. Ashwini V. Kurzekar, Dr. A. R. Mahajan
Department of CSE
Priyadarshini Institute of Engineering & Tech.
Nagpur, India

Abstract—

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

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 digital documents has the great interest due to their wide application areas such as important certificates, digital books, legal documents and engineering drawings. Important documents such as fax document, insurance copy and personal documents are digitized 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 wide range of values, 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, particularly for images of documents 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 signed documents, certificates, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Document images, which include texts, tables, line arts, etc.

B. Data Hiding

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

Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. Two important uses of data hiding in digital media are to provide proof of the copyright, and assurance of content integrity.

II. LITERATURE SURVEY

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 [1].

Yang and Kot 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) [2].

A new binary image authentication method with small distortion and low false negative rates system is proposed. It 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 [3].

Y. Lee, H. Kim and Y. Park proposes 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 $n\log_2((M\times N)/n + 1)$ by changing at most n pixels. This scheme can embed more data, as wel it maintain a better quality, and have wider applications. This data hiding scheme embed more amount of data and it will not affected the quality of the image [4].

Min Wu and Bede Liu propose a new method to embed data in binary images, the images contains scanned text, figures, and signatures. The data hiding method in which "flippable" pixels criterion is used to enforce specific blockbased relationship in order to embed a significant amount of data without causing noticeable changes. Shuffling of pixels is applied before embedding to equalize the uneven embedding capacity from region to region. The hidden data in image can be extracted without using the original image, and data can be extracted after high quality printing and scanning with the help of a few registration marks. The data embedding method can be used to detect unauthorized use of a digitized signature, and annotate or authenticate binary documents [7]

Min Wu and Bede Liu proposed in paper data hiding in image and video in that they addresses a number of fundamental issues of data hiding in image and video and propose general solutions to them. Also they propose a new multilevel embedding framework to allow the amount of extractable data to be adaptive according to the actual noise condition. As well as the issues of hiding multiple bits through a comparison of various modulation and multiplexing techniques. Finally, the nonstationary nature of visual signals leads to highly uneven distribution of embedding capacity and causes difficulty in data hiding. Min Wu and Bede Liu proposed an adaptive solution switching between using constant embedding rate with shuffling and using variable embedding rate with embedded control bits. They verify the effectiveness of their proposed solutions through analysis and simulation. And apply these solutions to specific design problems for embedding data in grayscale and color images and video [8].

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. To provide a well-developed intellectual property rights protection scheme, 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 and data repair capability for color document type images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a color document image which, together with the binarized block content, is 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 destruction will occur to the input 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.

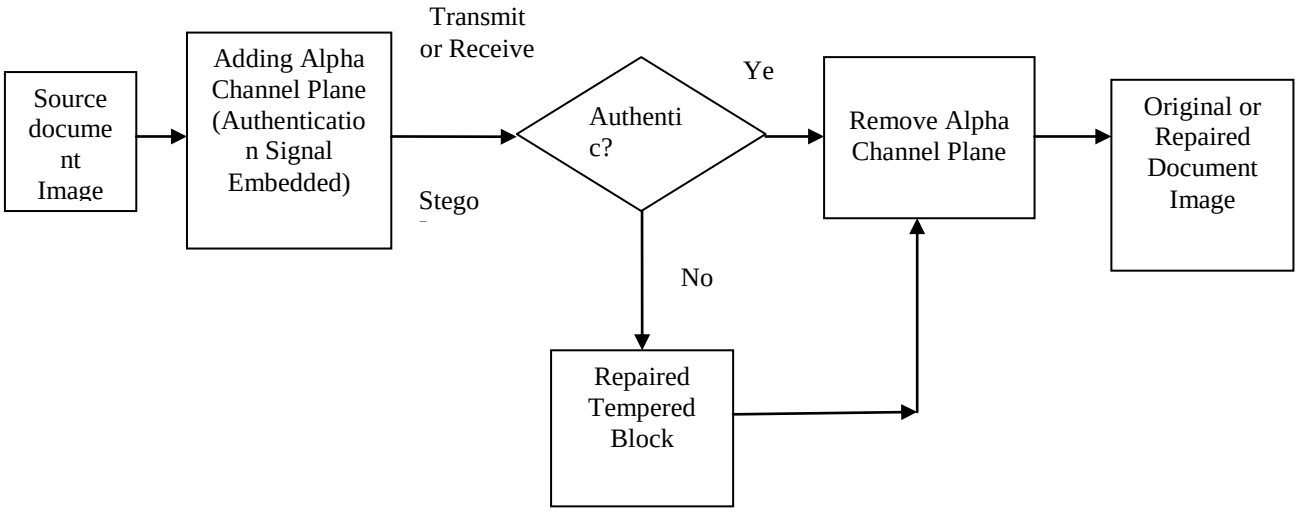

Fig.1. Framework of proposed document image authentication method

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. THE SECRET SHARING AND SECRET RECOVERY

A. Secret Sharing

Secret sharing algorithm is introduced by the Shamir [9]. In secret sharing algorithm, secret data d with n participant and threshold k which is passed as an input, Where k<= n. And getting n shares as output for the n participant. So for that we required the prime number p which is greater than d and k-1 coefficient i.e. $c_1, c_2 \ldots c_{k-1}$ and n real valus i.e. $x_1, x_2 \ldots x_n$. So shares are generated using the following formula,

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + \ldots + c_{k-1} x_i^{k-1}) \bmod p \qquad (a)$$

B. Secret Recovery

The Secret recovery algorithm is also introduces by Shamir. Secret recovery algorithm which is used for recover the secret at the time of authentication and data repairing. So input to the secret recover algorithm is k shares wich is collected from the secret sharing algorithm with prime number p and threshold k. And output as secret data d which is present in the shares and coefficient. So for extracting d from shares with the use of following formula,

$$\begin{aligned} d = (-1)^{k-1} [&F(x_1) * x_2 x_3 \ldots x_k / (x_1 - x_2)(x_1 - x_3) \ldots (x_1 - x_k) \\ &+ F(x_2) * x_1 x_3 \ldots x_k / (x_2 - x_1)(x_2 - x_3) \ldots (x_2 - x_k) + \ldots \\ &+ F(x_k) * x_1 x_2 \ldots x_{k-1} / (x_k - x_1)(x_k - x_2) \ldots (x_k - x_{k-1})] \bmod p \end{aligned} \qquad (b)$$

V. IMAGE AUTHENTICATION

In this proposed scheme, The Stego image I' is generated which is present in PNG format from the simple document type color image I with an alpha channel plane. The alpha channel is used for carrying the data, which is used at the time of authentication and data repairing. PNG image is generated with passing the alpha channel to binary color document type image. Then embed the shares, which are generated by the secret sharing algorithm into document type PNG image. After embedding the shares into an image this is called as Stego image I'.

In this algorithm we give input as the stego image I' with threshold value k and the output is tampered image I_t, with tampered block marked. The following block diagram shows the authentication process,

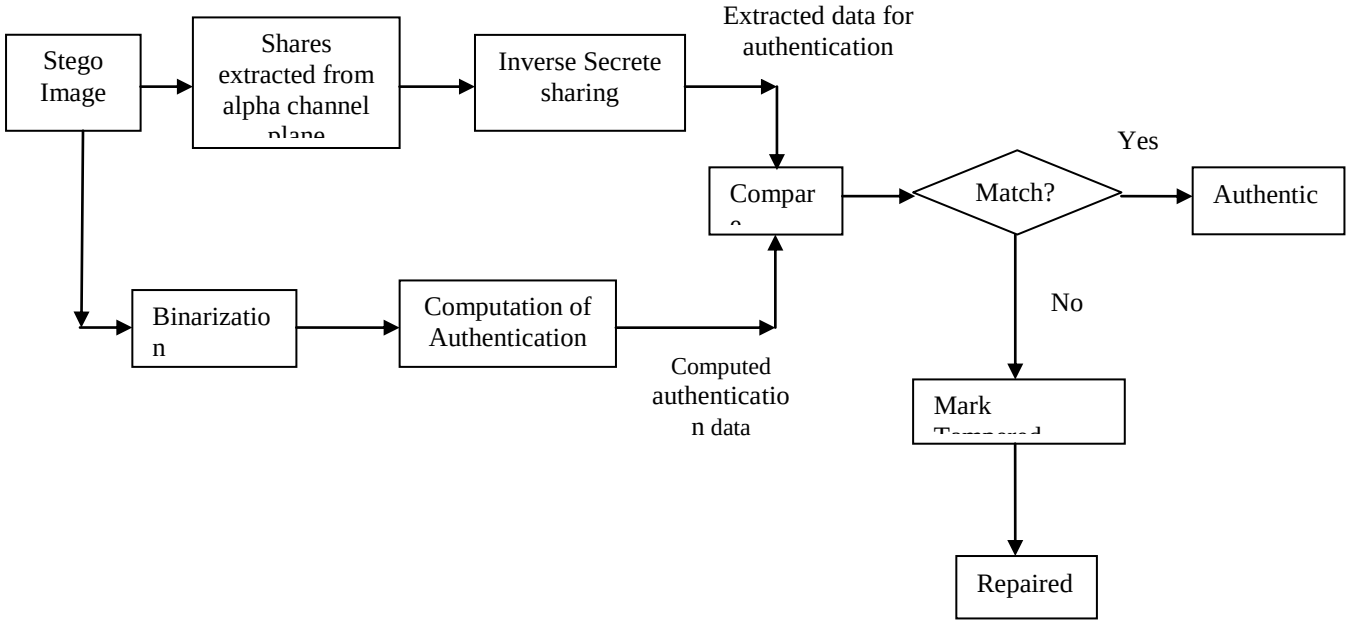

Fig.2. Authentication process for document type color image in PNG format

After giving input as a stego image, extract the shares from alpha channel plane then applying the reverse secret sharing algorithm for extracting data for authentication. at the same time binarized the given image and compute the authentication data from current block of image. Then compare extracted authentication data from alpha channel and computational authentication data, if match is occurred then image is authentic and match not occurred then marked as a tampered image and then repairing this block of an image.

VI. 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. Commun.*, 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
[9] A. Shamir, "How to share a secret,"*Commun. ACM*, vol. 22, no. 11,pp. 612–613, Nov. 1979.