MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

AUTHENTICATION OF GRAYSCALE DOCUMENT IMAGES

Harsha Karpe[1], Pallavi Gadekar[2], Swati Kale[3], Snehal Shinalkar[4]
Department of Information Technology
JSPM's Imperial College of Engineering & Research
Pune, India

[1]harshakarpe31@gmail.com, [2]gadekarpallavi07@gmail.com
[3]kale.swati96@gmail.com, [4]snehalshinalkar30@gmail.com

Abstract: *In this paper an authentication method for grayscale document images which is based on secret sharing technique with self repairing capability via the use of the Portable Network Graphics image has been described. In this approach the original grayscale document image is converted into stego image by adding the alpha channel plane. The stego image is in the Portable Network Graphics (PNG) format. This stego image is transmitted over the network. The authentication process is applied on the stego image on the receiver side. In the authentication process the data extracted from this stego image is compared with the data computed from the binary version of the stego image. If the data is matched the image is considered to be authentic. Else the tampered blocks are marked and the image is self repaired using inverse secret sharing scheme.*

Keywords*: Image Authentication, Grayscale Image, PNG Image, Secret Sharing.*

1. INTRODUCTION

Digital image is a binary representation of an image. The image can be of raster or vector type. Important information can be preserved in the form of digital images. But with the modernization of technology it is easy to make changes to the contents of digital image. Digital images can be important documents such as scanned checks, university results, last will, etc. Thus the issue of integrity and authenticity of digital images arises. To secure these images and to solve the problem of image authentication we need to develop effective authentication methods. A new blind authentication method is suggested in this paper. First we will have a overlook on the existing methods and their disadvantages.

2. RELATED WORK

In 2003, in Tzeng and Tsai's method [3], for the image authentication randomly-generated authentication codes are embedded into image blocks. The concept of Code holder is used to reduce image distortion which results from data embedding by using more than one pixel group. The main drawback of this method is that pixel replacement for data embedding, generate noise pixels, distortion in stego-image and no repair capability.

In 2004 Wu and Liu [4] operated the flippable pixels. The binary image can be manipulated in two ways. In the first way the pixels of the image are changed. In the second way thickness of strokes, curvature and relative positions are changed. In this method the image is partitioned into multiple blocks and fixed number of bits is embedded in each block by changing the pixels of the block. Here embedding is done by manipulating the pixels with high flippability scores. The main drawback of this method is that, noise is robust, only limited amount of data can be hidden.

Later in 2006, Yang and Kot [6] proposed a two-layer binary image authentication method. In this method one layer is used for checking the image fidelity. The other layer is used for checking image integrity. The disadvantages of this method are distortion in stego image needs larger macro blocks to yield pixel flippabilities for embedding authentication data.

Thus in the above methods we encounter the problems of distortion and repair capability. To overcome this problem a new blind authentication method is proposed.

3. PROPOSED METHOD

This paper focuses on authentication of grayscale document images with an additional self repair capability. The original image is binary like grayscale image. This image is transformed into a stego image which is in the PNG format. PNG is an extension to the stego image. This image is then sent to the receiver. The stego image is then verified by the proposed authentication method. If the image has not undergone any attack it is verified. Otherwise, the tampered blocks are identified and the image is repaired using reverse Shamir secret sharing scheme.

To understand the proposed method we first need to have the base of Shamir secret sharing algorithm.

3.1. Shamir Secret Sharing Algorithm

In this algorithm, the secret or the image is transformed into several shares. These shares are distributed to n participants. And if we manage to collect any of the k shares such that k<n, we can recover the image easily. But the knowledge of k-1 shares makes the recovery of image impossible. Here k is called the threshold value and therefore the algorithm is also called (k,n) threshold algorithm. This algorithm is used as a base in the formation of stego image.

3.2. Formation of Stego Image

Firstly, the input grayscale binary image is binarized with two major gray values. Then data for authentication and repairing is computed from the binarized image. This is given as an input to the Shamir secret sharing scheme to get n shares. These share values are mapped into alpha channel values. Finally the mapped secret shares are embedded into the alpha channel plane to form the stego image as shown in Fig.1 and instead of sending the original grayscale image, the stego image is sent.

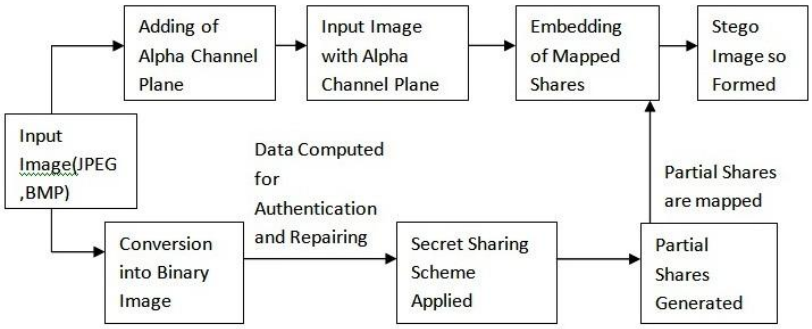

Fig.1: Stego Image Formation (Source: IEEE Transactions on Image Processing, Vol 21. No.1, Jan 2012)

3.3. Authentication Process

The authentication process is applied on the stego image. Firstly the shares are extracted from the alpha channel plane of the stego image and inverse secret sharing scheme is applied on it. The extracted data is used for authentication and repairing. On the other hand, the stego image is also binarized. The authentication data is computed from the image. These computed data is compared with the extracted data which is a result of inverse Shamir secret sharing scheme. If the data is matched, the image is authentic. And if the data is not matched, that is the image is unauthentic, the tampered blocks are marked. Then k partial shares from the alpha channel plane are collected and the image is repaired. If it is not possible to collect k shares then the image cannot be repaired. This is shown in Fig.2. It is necessary to collect minimum k untampered shares. Thus the original image is obtained even if it is attacked or changes are made to it and hence the security is maintained.

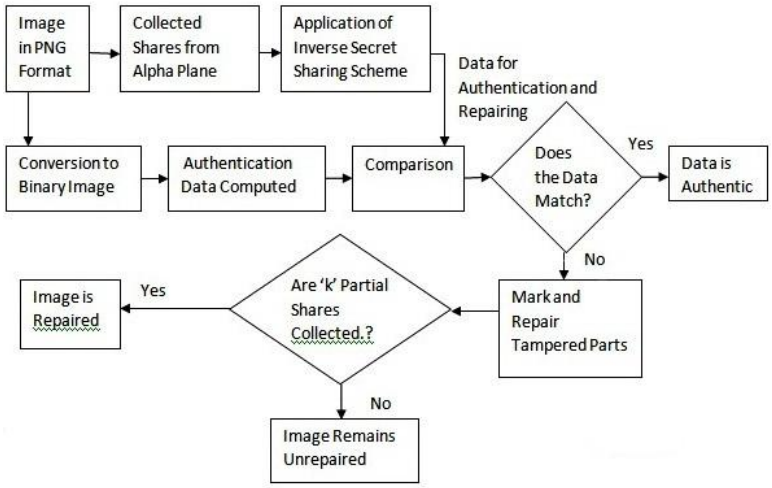

Fig.2: Authentication Process (Source: IEEE Transactions on Image Processing, Vol 21. No.1, Jan 2012)

4. ADVANTAGES

The proposed method is blind. That is it does not require any overhead for transmission other than stego image. This marks the different feature in this method.

The method provides repair of the image at the pixel level. This gives a better repair effect to the text images. Also text characters are smaller in size with curved strokes. This method enhances the data security by using the secret sharing scheme. Data is not directly hidden into the document image pixels. It is embedded in the form of shares in the alpha channel plane. The authentication method has the ability to survive image content attacks. This happens because of combining Shamir scheme, authentication signal generation, and random embedding of multiple shares.

5. CONCLUSION

Thus a new blind authentication method for grayscale document images via the use of PNG with an additional self repair capability has been proposed. This is the only method as compared to earlier methods which uses the concept of alpha channel plane. It is basically used as a carrier for authentication signals. Also the Shamir secret sharing scheme is used which helps in repairing tampered block images. This method solves the problem of image security and authentication. Hence the data can be stored and transmitted through digital image safely.

6. FUTURE SCOPE

The proposed method is useful for the security of digital images. Also the method can be used in future to apply on colored images. In this method the shares generated by Shamir secret sharing method are of fixed size. Future improvements can be done to generate shares of alternative size for better data repair effects. Hence the proposed method has immense scope in authentication and security of digital images.

ACKNOWLEGEMENT

We would like to express our gratitude towards Prof. S.R. Todmal, our guide, for his immense support and encouragement. We are also thankful to our department for providing necessary resources.

REFERENCES

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

[2]. W. H. Tsai, "Moment-preserving thresholding: A new approach," Comput. Vis. Graph. Image Process., vol. 29, no. 3, pp. 377–393, Mar.1985.

[3]. 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 443–445, Sep. 2003.

[4]. M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, 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. 741–744, Dec.2006.