International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Authentication of Colored Document Image with Data Repair Capability

Pradnya Kadam[1], Nishigandha Khandagale[2], Poonam Yadav[3]

Abstract: ***In this paper we proposed a new authentication method based on secret sharing technique with data repair capability for colored document image with use of Portable Network Graphics (PNG) image. An authentication signal is generated for each block of colored document image. This block is transformed into several shares using the Shamir secret sharing scheme. Many shares are generated and embedded into alpha channel plane. The alpha channel plane is combined with the original colored image to form PNG image. This PNG image is encrypted by using the chaotic logistic map and forms the stego image.Stego image is received in receiver side and checks for the authentication. If the authentication is fails, then use the reverse shamir secret algorithm. This algorithm having the data repair capability.***

Keywords: Image authentication, Secret sharing, Data repair, PNG, Encryption, Logistic map.

1. Introduction

1.1 About the Project

Digital images are used to preserve important information. But providing authentication to this image is challenging task. In this paper we use of fast technology it is easy to modify the contents of this digital images. Particularly for document images such as important certificates, scanned checks, art drawings, signed documents, circuit diagram etc.

In this approach, we take input as colored document images then each block of colored image generate an authentication signal which combines with binarized block content, is transformed into several shares using shamir secret sharing. After this using alpha channel plane it forms the PNG image. This PNG image is transformed into stego image using chaotic logistic map. By using proposed method the stego image is received at the receiver side and check for authentication. Integrity modification of the stego image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is totally destroyed from the stego image. The proposed method is based on (t,n)threshold secret shamir sharing scheme and encryption based on chaotic logistic map. By secret sharing the secret message is transformed into n shares, when t of the n shares is collected the secret message can be recovered without the data loss. Using logistic map we generate a random key, by this key the PNG image formed with alpha channel plane is scrambled, and made ready for transmission. This method provides two layers of security to the document by keeping shares in the alpha channel and encrypting the PNG image. Reverse Shamir secret is used to reconstruct the tampered image and providing the security.

1.2 Existing System

In recent year we use the Watermarking technique. But it found that watermarking technique are not as reliable to use for authentication because this can be removed by software available. Hence we are using the colored technique which helps in digitally identifying and preventing image with data repair capability. This technique having visual quality problem so, we use this proposed system.

1.3 Proposed System

Proposes a new authentication method which is based on secret sharing techniques and logistic map with repairing capability of data with PNG image. In this approach each block of colored document image generate authentication signal using a shamir secret algorithm it transfer into the several shares. Alpha channel plane forms PNG image.PNG image encrypted by the chaotic logistic map to forms the stego-image. Stego image is received at receiver side and check authentication signal. If the authentication process failed then repairing is done using reverse shamir secret.

2. Algorithm for Creating Secret Shares

2.1 Algorithm 1-(t,n) threshold secret sharing

Input: Take secret c in the forms of an integer, number n of participants and threshold t<=n.

Output: n shares in the form of integer for the n participants to keep.

2.2 Algorithm 3-Generating stego image in PNG format form a given colored image.

Input: A colored image document E with two major color values and secret key K.

Output: Stego image E' in PNG with encrypted format, relevant data embedded, including the authentication signal and the data used for repairing.

2.3 Algorithm 2-Secret recovery of shares

Input: Select t shares from the n participants and the prime number p with both t and p

Output: Secret c hidden in the shares and coefficients mj used in 2.1 where m is integer values and j=1,2,3....m-1

3. System Architecture

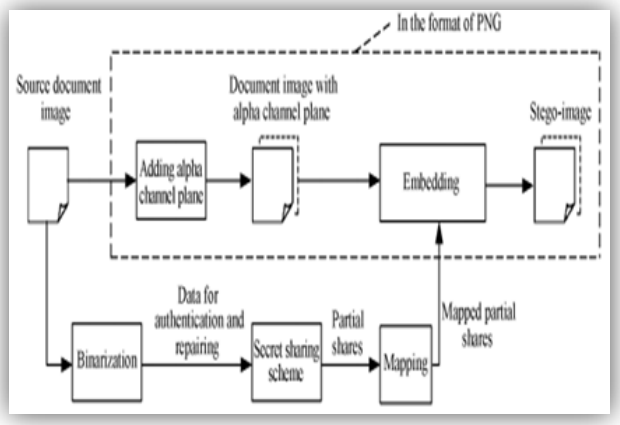

Figure: sender side image

Take the input cover image is the colored image. Add the alpha channel plane to this source image and embed with shamir secret shares. Stego image is formed which is ready to share in the network or in database. The original image is combined with alpha channel plane to generate the PNG (Portable Network Graphics) image. Using shamir secret scheme it send the data to the partial shares.

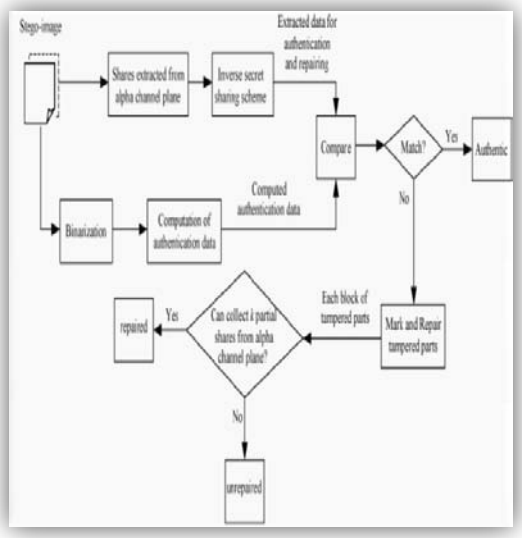

Figure: Receiver side

Stego image is send to the receiver side. Receiver receives this image and checks for the authentication. Extract secret share image and apply inverse secret sharing if the authentication is fails and compare it with original image. In authentication repairing is done in each tampered block, after collecting two shares from unmarked block using reverse shamir scheme. Security of data provided by sharing of data in the alpha channel an encrypting the stego image.

4. Merits of proposed system

The proposed method has several merits which are described as following:

1) Higher data security and possibility to survive image content attacks:
   Due to the use of encryption the data become scrambled, therefore the hackers does not see the document data, and also by the use of sharing method, the proposed method can survive malicious attacks of common content modification, such as super imposition and painting.
2) Providing pixel level repairing of tampered image parts:
   After collecting two non tampered partial shares, we can repair the tampered block at the pixel level.
3) Making the use of new type of image channel for data sharing:
   Rather than common type of image a PNG image has the extra alpha channel plane, which is normally use to produce transparency of the image.

5. Future Enhancements

We have proposed a secure authentication scheme for colored document images by the use of secret sharing method and chaotic logistic map. In this scheme security is provided by, secret sharing and encryption. Using Shamir secret sharing method both the generated authentication signal and the content of a block are transformed into partial shares.

Which are then distributed in an elegant manner into an alpha channel plane to create a PNG image. This image is encrypted by using chaotic logistic map and forms a stego image. In the authentication process, if it seen that the data is tampered then self-repairing is done in the content of the tampered block by reverse Shamir scheme. This method enhances the security by embedding the data in the alpha channel plane and encrypting the PNG image.

6. Acknowledgment

We thank Dr. R.S. Jahagirdar (Principal IOKCOE Pune) for providing necessary facilities to carry out the work. We are very thankful to Prof. Sarla A. Chimegawe (Assistant Professor) for her useful guidance.

7. Conclusion

We have proposed a secure authentication scheme for colored document images by the use of secret sharing method and chaotic logistic map. In this scheme security is provided by, secret sharing and encryption. Using shamir secret sharing method both the generated authentication signal and the content of block are transformed into partial shares. Then these shares are embedded into alpha channel plane to create PNG image. This image is encrypted by chaotic logistic map and forms a stego image. In the receiver side stego image is receive and check for authentication. In authentication process if the data is tampered then self repairing is done in the content of tampered by reverse shamir scheme. This method enhances the security by embedding the data in the alpha channel plane and encrypting the PNG image.

References

[1] M. U. Celik, G. Sharma, E. Saber, and A.M. Tekalp, "Hierarchical watermarking for secure image

authentication with localization," IEEE Trans. Image Processing, vol.11, no.6, pp.585-595, june.2002.
[2] C Yu, X Zhang "Watermark embedding in binary images for authentication", IEEE Trans. Signal Processing, vol.01, no.07, pp.865-868, September. 2004.
[3] A. Shamir, "How to share a secret," Commun.ACM, vol.22, no.11, pp.612-613, Nov, 1979.
[4] P.Jhansi Rani, S. DurgaBhavani1stInt'1Conf on Recent Advances in Information Technology RAIT-2012. [5] Chih-HsuanTzeng and Wen-Hsiang Tsai, "A new approach to authentication of Binary image for multimedia communication with distortion reduction and security enhancement. IEEE communication letters VOL.7.NO.9 2003
[5] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, vol. 13.
[6] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," IEEE Trans.on Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[7] Che- Wei Lee and Wen-Hsiang Tsai "A secret-sharing-based method for authentication of grayscale document images via the use of the png image with data repair capability" IEEE Trans. Image Processing., vol.21, no.1, january.2012.
[8] Niladri B. Puhan, Anthony T. S. Ho "Binary Document Image Watermarking for Secure Authentication Using Perceptual Modeling" IEEE International Symposium on Signal Processing and Information Technology2005.
[9] W.H. Tsai, "Moment-Preserving thresholding: a new approach." Computer Vision, Graphics, and Image Processing, vol. 29, no.3, pp.377-393, 1985.

Author Profile

Miss. Pradnya D. Kadam is pursuing BE Computer Engineering, Institute of Knowledge College of Engineering, Pune, Maharashtra, India

Miss. Nishigandha K. Khandagale is pursuing BE Computer Engineering, Institute of Knowledge College of Engineering, Pune, Maharashtra, India

Miss. Poonam E. Yadav is pursuing BE Computer Engineering, Institute of Knowledge College of Engineering, Pune, Maharashtra, India