SECURING DOCUMENT IMAGES USING SECRET SHARING

Manjusha R. Gaikkwad[1], Dr. Savita R. Bhosale[2]

[1]PG scholar, Department of Computer Engineering, MGMCET, Kamothe, Navi-Mumbai (India)

[2] Professor, Department of Electronics and Telecommunication, MGMCET, Kamothe, Navi-mumbai (India)

ABSTRACT

A visionless authentication method is based on secret sharing technique with additional data repairing ability for the gray-scale document images by using Portable Network Graphics (PNG) is presented. For each data block of gray-scale document images authentication signal is produced then this produced authentication signal and binarized data block content is transmute by using the secret Shamir scheme ,the contributed values are selected such that as many shares can produced and place in to the alpha channel plane. To create PNG image the alpha channel plane is added with the gray-scale document image at the time of placing the values, computed shares are correlated to the range of alpha channel values extent up to 255 to get the stego-image. An image block is patent as damaged if the authentication signal calculated from the present block that does not matches which is calculated from the placed values of alpha channel plane. The reverse Shamir scheme is applied to repair the damaged data block content by collecting two shares from unobtrusive data block. The proposed method can survive malicious attacks of common content modification, such as super imposition, painting etc.

Keywords: Binarized Data, Data Repairing, Gray-Scale Images, Portable Graphics Network (PNG), Secret, Stego Image

I. INTRODUCTION

Digital Imaging has substantiated its estimable value in the various fields of science and technology with great increase of many applications in number of different fields. Digital images play a vital role for saving and maintaining credential data from the malicious attacks, it also provides a security by authentication. Optical cryptography(OC) intern also called as optical secret sharing encryption is done during the transformation of secret in to number of shares and decryption is performed after collecting all the shares [1][2].with the furtherance of digital technologies ,it's very simple for anybody to change the original content without affecting its originality , so to solve these type of image authentication problem specifically those documents which are very important like bank cheque ,insurance documents etc. there are many methods have been proposed in the past on authentication of gray scale document images[3][4][5].The problem found in our existing system as, it does not provide optimum transparency to the documents because there is no use of alpha channel plane so because of this anyone can tamper the credential data, important documents and it also harms the visual quality of documents[5][6][7]. here secret sharing method for creation of stego image and generating authentication signal by extracting two shares which was embedded previously in the alpha channel plane again matching the

current calculated authentication signal with the hidden authentication signal which is embedded in alpha channel plane[8][9].

Our Contribution

To solve challenges of security of images with authentication and their visual quality keeping problem ,we propose here one algorithm i.e. Algorithm for generation of stego image using alpha channel plane & authentication of it by using two shares of untampered blocks and then repairing of the damaged block using two untampered blocks of shares

Proposed system also provides efficiency with security and better visual image quality & authentication.

II. RELATED WORK

- **M. Wu and B. Liu [2]** implemented connectivity preserving criterion for accessing the flippability of a pixel for getting better visual quality result of the images this criterion is defined that is based on connectivity among the pixels, to make sure authenticity and integrity of the document images they designed cryptographic signature.

- **H. Yang and A.C. Kot [3]** propounded two layer binary image authentication method in which first layer is used for testing the image constancy and the second layer is used for testing the image integrity. here it is also used connectivity preserving transition criterion for calculating flippability of pixel.

- **H. Yang and A.C. Kot [4]** proposed a pattern-based data hiding method for binary image authentication in which three transition criterion is used for calculating the flippabilities of the pixels in each block.

- **C. C. Lin and W .H. Tsai [5]** they developed a secret image sharing with authentication and steganography. Here (t, n) threshold function is used for sharing the secret and data hiding is used for embedding the shares before sending to n number of participants .proposed system also provides high level of security and efficiency.

- **M. u. Celik, G. Sharma, E. Saber, and A. M. Tekalp [6]** proposed that for calculation of block signature they divide the image in to number of blocks in multilevel hierarchical manner to achieve localization .they also used Sliding window for searching and enabling of the untampered blocks.

- **Y. Lee, H. Kim, & Y. Park [10]** they proposed thresholding technique i.e. bi-level and multilevel thresholding they also proposed the method for quality of selected threshold and threshold selection method based on the concept of moment preserving principle.

III.PROPOSED SYSTEM

3.1 Flowchart of Proposed System

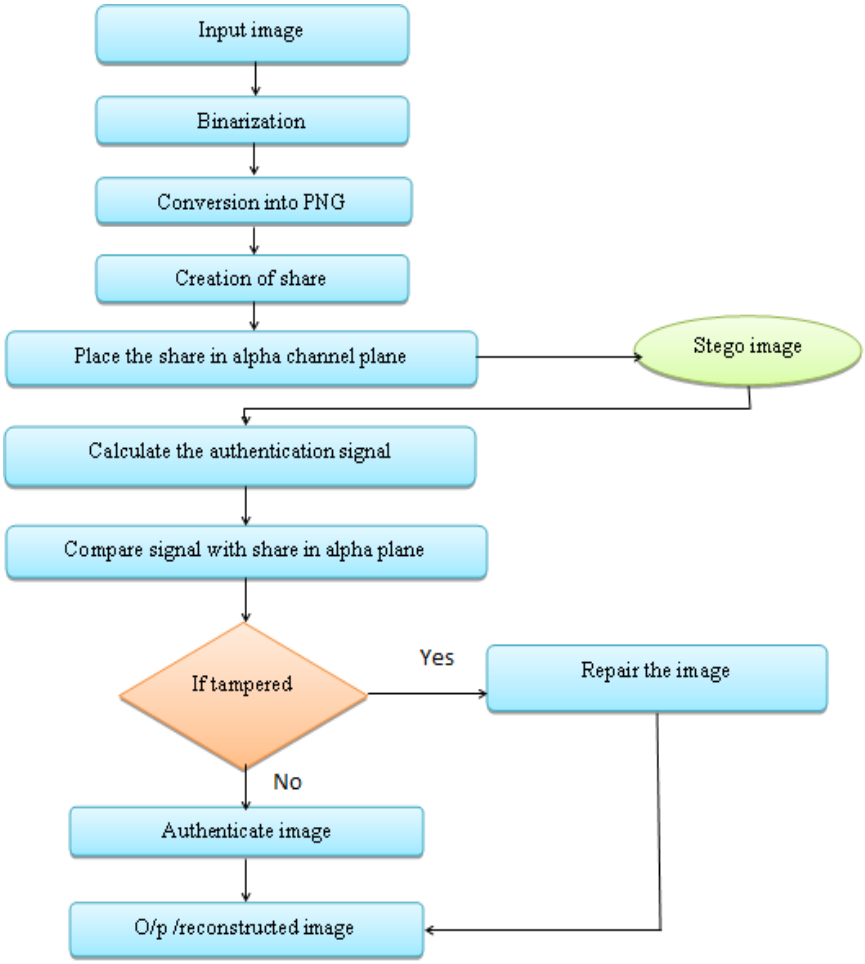


Fig 1.Flowchart of proposed system

Fig.1 representing the flowchart of the proposed system first the input image is given for Binarization and after it get convert in to PNG format, then place the shares in alpha channel plane to create stego image then by using the shares of alpha channel plane authentication signal is generated, compare this current signal with shares which was already embedded in the alpha channel plane, if the image is tampered then repair & reconstruct it otherwise it is authentic image.

3.2 Alpha Channel Plane

The alpha channel of an RGB image defines its transparency when it is amalgamated with another image. If a pixel has an alpha channel of 0 it is considered completely transparent when placed onto another image. If pixels of alpha channel are set to value 255 it is considered as completely equivocal.

Fig.2 Infrastructure of Proposed System

Fig.2 represents a Infrastructure of Proposed System in the first stage input source document image is inserted with alpha channel plane after some processing is done the stego image is created in the PNG format then it is given for checking whether it is certified i.e. for authentication. If the calculated share is matched with the share which extracted from the embedding process then only authentication is possible there are some blocks which marked as tampered and that can be repaired by using two shares of untampered block.

3.3 Algorithm for Generation of Stego Image in the PNG Format, Authentication, Repairing.

Part 1: carrying two gray values which is placed in alpha channel plane.

Step 1: conversion of stego image in to binary form (Binarization).

Calculate T= (gr1+gr2)/2, use this threshold to convert stego image i.e. Is in to binary form Ib with 0 denoting gr1 and 1 denoting gr2.

Part 2: Authentication of stego image.

Srep2 :(start loop) taking unprocessed block Bu of stego image Is with pixel values P1 to P6 and find the corresponding values q1 to q6 of block Bu in alpha channel plane of stego image Is.

x1=1, x2=2,x3=3…..x6=6.

Calculate threshold (T, n) to get six shares by using the below formula,

$qi= F(xi)=(d+c1xi) mod\ p$ where i= 1,2,….6.

Step 3: extracting hidden authentication signal.

1. Subtract 238 from each qi value of untampered block and also add partial shares to get the values of d and C1.

2. Here in this step convert value of d and c1 in to four bit binary form and concatenate these two values to get 8 bit string.

Step 4: map the authentication signal & mark the damaged/tampered blocks

1. Calculate the values q1 to q6 2×3 block of Ib.

2. Match the newly calculated q1 to q6 shares with the previously placed shares in Bu (unprocessed block) i.e. tampered/damaged.

Part 3: repairing of the damaged block/part.

1. Find the pixels p1 to p6 using the binary values of d and c1, if there are any tampered blocks of pixels then repair those values using binary values of b & c.

2. Assign pixel value for gr1 is 1 and for gr2 is 0 which is retrieved from image Is.

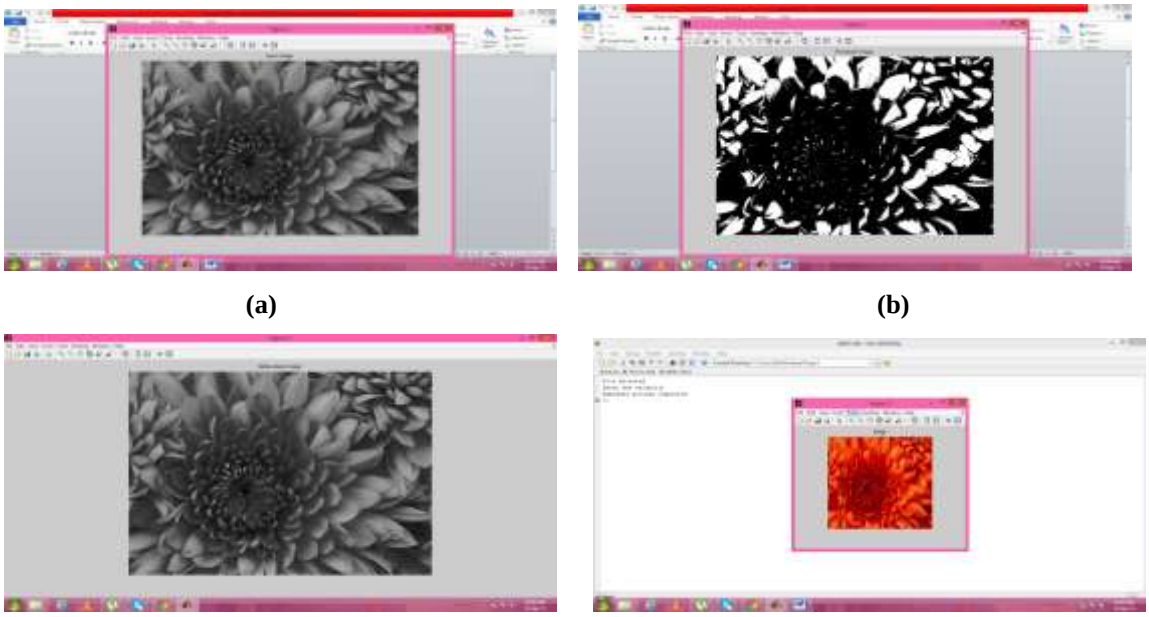
Here repairing is done only when two untampered block of share is available .if there is no untampered shares then repairing fail.

Step 5: end loop

If there is any unprocessed blocks of Bu then go to step 2.

3.4 Experimental Results

Following are the results of first and second module.



(a) **(b)**

(c) **(d)**

Fig.3 (a) Input image; (b) Threshold image; (c) Alpha plane image; (d) Stego image.

IV. CONCLUSION

We proposed here A Secure authentication scheme for grayscale document images by using secret sharing method. By using two gray values of grayscale document image the stego image is created. 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. 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. It provides advance level of security to the documents and credential data.

REFERENCES

[1]. Che-Wei Lee, IEEE Transaction on Image processing January 2012, and Wen-Hsiang Tsai Senior Member, IEEE "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability ".

[2]. M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation", IEEETrans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[3]. 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.

[4]. 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.

[5]. C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," J. Syst. Softw., vol. 73, no. 3, pp. 405–414, Nov./Dec. 2004.

[6]. M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchical watermarking for secure image Authentication with localization," IEEE Trans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.

[7]. C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Trans. Image Process, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

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

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

[10]. 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.