Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security and Authentication of Gray Scale Document Image by Secret Sharing Method with Data Repair Capability

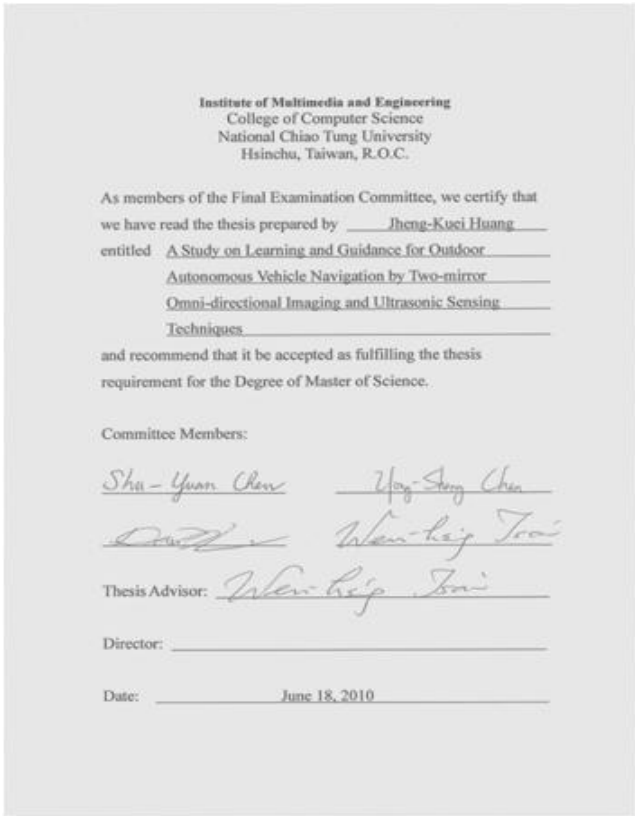
Vandana Navale, Archana Lomte
Computer Department & Pune University,
India

Abstract— For a Gray scale document image a new authentication method based on secret sharing technique with data repair capability use of Portable Network Graphics(PNG). For each block of gray scale document image an authentication signals are genrated, i.e. together with binarized block content. The Shamir secret sharing scheme is used to shares the authentication signals of Gray scale document image.Many shares are genrated and embedded in to an Alpha Channel Plane then alpha channel plane is combined with original Gray scale image to form a PNG image.In the embedding process, the computed share values are mapped into range of alpha channel values at maximum range. The maximum range of alpha channel value is 255.In the image authentication process the image block is marked as tampered. From the current block content the authentication signals are computed and i.e. not match that exrracted fom the shares embedded in alpha channel plane.Then the data repairing applied to each tampered block by reverse Shamir scheme after collecting shares from unmarked blocks.

Keywords— Data repair, Gray Scale document mage,Image Authentication,PNG,Secret Shairing.

I. INTRODUCTION

Important information is save in the form of digital image.However, advance of digital technologies it is easy to make modifications in digital image contents.There is challenge in security image.It is necessary to design methods to solve image authentication problem.[1][2].Self repair capabilities are useful for protection of digital documents in many fields.Image content authentication also useful for protection of digital documents.Such as signed checks, art drawing, important certificates so on.Gray scale images with two gray values,one value of the background and second for the foreground.Background including mainly blank spaces and foreground including mainly text for example shown in Fig1.



Institute of Multimedia and Engineering
College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.

As members of the Final Examination Committee, we certify that we have read the thesis prepared by Jheng-Kuei Huang entitled A Study on Learning and Guidance for Outdoor Autonomous Vehicle Navigation by Two-mirror Omni-directional Imaging and Ultrasonic Sensing Techniques and recommend that it be accepted as fulfilling the thesis requirement for the Degree of Master of Science.

Committee Members:

Thesis Advisor:

Director:

Date: June 18, 2010

Fig. 1. Binary-like grayscale document image with two major gray values.

The two major gray values in Fig1.document image are 174 and 236. Because of simple binary nature the image authentication problem is difficult for binary document image. The problem regarding the binary image is visual quality of resulting image and issue of preventing image tampering. In this paper, I propose authentication method with self repairing capability of gray scale document images and overcome the problem of image tampering detection and keep visual quality.After applying the proposed method, the Gray scale image tranformed into Stego image i.e. in PNG format with scrambled form in a alpha channel for transmission on network.The input cover image with two major gray values shown in Fig.1.The stego image is received may be verified for its authenticity. The stego images integrity modifications can be detected by the method at block level and its repaired at pixel level. In case the alpha channel plane destroyed from the stego imge the entire resulting image is regarded as inauthentic that is nothing but fidelity check of the image failed. The proposed method is based on the (k,n) threshold. Secret sharing scheme that is of Shamir[3]. By secret shairing scheme the secret message is transformed into n shares, and when k of the n shares is collected the secret message can be recovered without data loss not necessary all of them are collected the secret message can be recovered.Such seheme is useful in reduce in reduce data loss.

The two issues in information security are secret sharing and data hinding.In the proposed method Icombine them together to developed method I combine them together to developed a new authentication method. The secret sharing scheme is used in modification to carry authentication singals and image contents data and also it help to repair tampered data through the use of shares self repairing of tamp data at attacked image parts is that after the orignal data of the cover image are embedded into the image itself. For use in later data repairing the cover image is removed in the first place and original data are no longer available for data repairing resulting is not accuration. To solve this problem embed the original image data other place without change in cover image itself to solve this problem use extra alpha channel plane will create random transparency in the formed PNG image. As proposed in this paper is to map the resulting alpha channel values into a small range near their extreme value of 255.Another problem is data embedded in carrier that is of larged sized for my case here with the alpha channel as the carrier,this is not a problem because the cover image that I deal with is binary like and thus may just embed into the carrier a binary version of cover image yhat contain much less data.

Several methods for image authentication have been proposed , authentication with embeding special codes Yang and Kot [5] proposed a two layer binary image authentication method in which one layer is used for checking image fidelity and the other for checking image fidelity and the other for checking image integrity . Latter Yang and Kot [6] proposed a patteren based data hiding method for binary image authentication in which three transition criteria are used to determine the flippabilities of pixels in each block and the watermark is adaptively embedded into embedded blocks to deal with host image.

II. RELATED WORK

Securing the image documents over the network is one of the important issue now days.
This method on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is design for the same.
In this system,
1) An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme.
2) The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane.
3) The alpha channel plane is then combined with the original grayscale image to form a PNG image. During the embedding process, the computed share values are mapped into a range of alpha channel values near their maximum value of 255 to yield a transparent stego-image with a disguise effect.
4) In the process of image authentication, an image block is marked as tampered if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane.
5) Data repairing is then applied to each tampered block by a reverse Shamir scheme after collecting two shares from unmarked blocks, which increase more security.

III. PROPOSED WORK

Following methods need to study and included in this project

A. The Shamir Method For Secret Sharing

Secret sharing was proposed by Shamir in 1979. [3]. In the (k,n) threshold secret sharing method secret in the form of integer is transform into shares which then distributed in to n participants for them to keep original secret can be recovered accordingly. and as long as k of then n shares are collected, the orig-inal secret can be accordingly recovered, where $k \leq n$. The detail of the method is reviewed in the following. In Shamir's secret sharing scheme, a secret is split among n participants using a polynomial of degree k.
1.Based on polynomial interpolation k points are needed to fully define a unique polynomial of degree k-1.
It's (k, n) threshold scheme Dealer D distribute a secret s to n players At least k participant's are required to construct a secret s Also known as unconditionally secure Shamir's (k, n) secret sharing Goal Share the secret s among n participants 1, P2, P3, ..., Pn such that at least k participants are required to reconstruct the secret s.
B.Sharing Protocol (cont.)
Step I : Dealer D constructs polynomial f(x) of degree (k-1)

f(x) = a0+ a1 x + a2x2+ a3x3+ ... + ak-1xk-1 Polynomial f(x) is constructed over finite field, a0= secret (s), and all other coefficients are random elements in the field .

Step II : Dealer D chooses n random distinct evaluation points: Xj!= 0 , and secretly distributes to each participants Pj the share share j(s) = (Xj, f(Xj)), j=1, 2, ..., n.

C. Reconstruction

reconstruct the secret from each subset of k shares out of n shares. i.e. To find s=a0 from f(1), f(2), f(3), ..., f(k).

D. Interpolation property

Given k pairs of (i, f(i)), with i's all distinct, there is unique polynomial f(X) of degree k-1, passing through all the points. This polynomial can be computed from the pairs (i, f(i)).

E.Lagrange interpolation

Lagrange interpolation is used to find the unique polynomial f(x) such that degree f(x) < k
and f(j) = share j(s) for j=1, 2, 3, ..., k

Lagrange Interpolation Formula:

$$L(x) := \sum_{j=0}^{k} y_j \ell_j(x)$$

E. Image Authentication and Data Repairing

In the proposed method , I creat a PNG image from a binary type Gray scale document image with alpha channel plane.The original image is thought as Gray scale channel plane of the PNG image .PNG image creation in Fig.2.

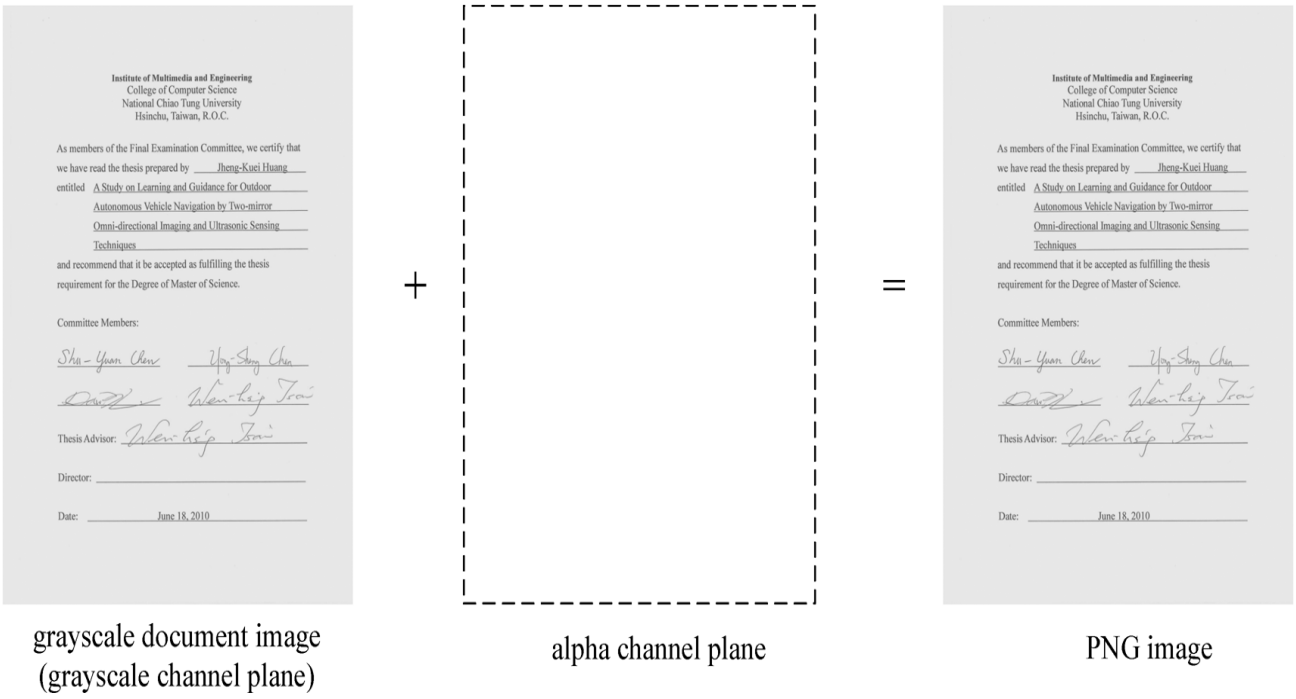


Fig. 2 Illustration of creation of a PNG image from a grayscale document image and an additional alpha channel plane.

Secondly the PNG image is binarized by moment preserving thresholding[7]. Data for authentication and repairing are then computed from binary version of image and takes as input to the Shamir secret sharing scheme to genrates secret shares.Finally the mapped secret shares embedded into the alpha channel plane for protection and data repair capabilities and find the stego image using stego method. Fig.3 and Fig.4 shows the block diagram of proposed method.

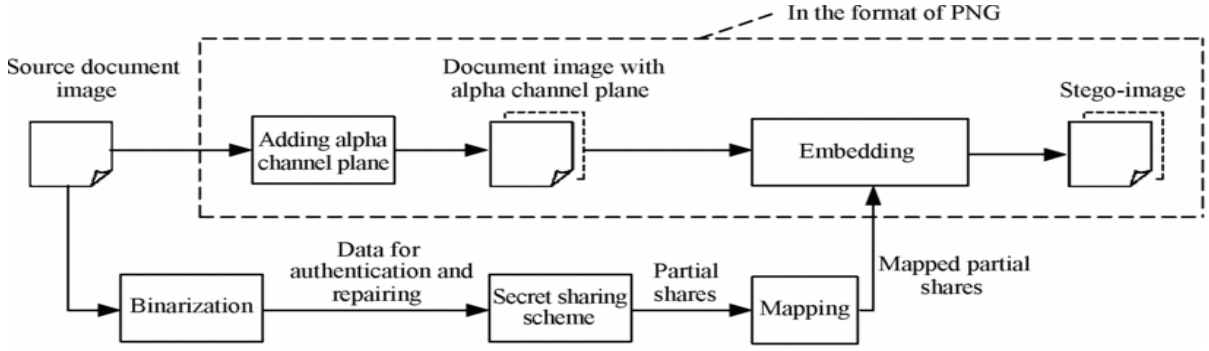


Fig. 3 Illustration of creating a PNG image from a grayscale document image and an alpha channel.

Input: a grayscale document image with two major gray values and a secret key .
Output: stego-image in the PNG format with relevant data embedded, including the authentication signals and the data used for repairing.

IV. CONCLUSION

We have proposed a secure authetication scheme for gray scale document images by the use of secret sharing method and alpha channel plane security is provide by using shamir's secret sharing method.Both the genrated authetication signal and the content of block have transformed into partial shares by shamirs method which are genrated into alpha channel plane to create a PNG image .Stego image is form in PNG format and from embedding the partial shares by mapping the share values. A block in stego image authentication has been tampered if computed authentication signals does not match for self repairing of tamped block the shamirs reverce scheme is used.

REFERENCES

[1] 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.
[2] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 822–831, Jun. 2005.
[3] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11,pp. 612–613, Nov. 1979.
[4] 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 Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec. 2006.
[6] 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.
[7] W. H. Tsai, "Moment-preserving thresholding: A new approach," *Comput. Vis. Graph. Image Process.*, vol. 29, no. 3, pp. 377–393, Mar. 1985.

