ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

A Secure Authentication Method for Grayscale Document Images

[I]M.Mahalakshmi, [II]C.Callins Christiyana
[I,II]Dept. of Computer and Communication Engg., Sethu Institute of Tech., Virudhunagar, India

Abstract
In the process of sharing document image, the intruder may attacks the data easily. A secret image is embedded in another image called stego image and shared secretly. For secret sharing of information Shamir scheme is used and at the receiver side reverse Shamir scheme is used. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content. This content is transformed into several shares using the Shamir secret sharing scheme. In the process of image authentication the tampered image block is marked and it is matched with the current block. If it does not match, self repair capability is applied to the tampered block and it is repaired automatically by a reverse Shamir scheme. Such image content authentication and self repair capabilities are useful for the security protection of the digital documents in many fields, such as important certificates, circuit diagrams, design drafts, signed documents, art drawings, scanned checks, last will and testaments.

Keywords
Portable Network Graphics, Image Authentication, Secret Sharing

I. Introduction

Information hiding is the principle of steganography. It is used to protect any part of information or confidential messages from extensive modification created by the intruders. This information hiding is the powerful technique embeds in digital image to reduce the complexity and prevent the information from any modification. This digital image is a numeric representation of a two-dimensional image. Digital image authentication is an issuefor the providers and producers of digital images such as health care organizations,law enforcement agencies and insurance companies. There are several met used in past.Wu and Liu[2] manipulated the so-called flappable pixels to create specific relationships to embeddata forauthentication and annotation of binary images. In this method numbers of digital images are used for business purpose. Cryptographic authentication is approach is used for authentication. The disadvantage is it affects visual quality.Yang and Kot[3] proposed a two-layer binary image authentication method, in which one layer is used for checking the image fidelity and the other for checking image integrity. In the method, a connectivity-preserving transition criterion for determining the flippability of a pixel is used for embedding the cryptographic signature and the block identifier. The major drawback is it occupies large memory.Later Yang and Kot [4] proposed a pattern-based data hiding method for binary image authentication in which three transition criteria are used to determine the flipabilitiesof pixels in each block, and the watermark is adaptively embedded in to embeddable blocks to deal with the uneven embeddability condition in the host image. In this method the disadvantage is high complexity. In the method proposed in [5], a set of pseudorandom pixels in a binary ore halftone images are chosen and cleared, and authentication codes are accordingly computed and inserted into selected random pixels. In Tzeng and Tsai's method[6], randomly generated authentication codes are embedded into image blocks for used in image authentication, and so-called code holder is used to reduce image distortion resulting from data embedding. Lee at al.[7]Proposed a Hamming-code based method flips one pixel in each binary image block for embedding a watermark, yielding small distortion and low false negative rates. Lee et al.[8] similarly measure to select flappable pixels for the improved the method later by using an edge line purpose of reducing the distortion. But this method is not secure.

In proposed method secret image sharing with steganography and authentication is established. Steganography is data hiding techniques that providers security protection for digital image data. The proposed method is used to handle full color images and quality of the recovery results is nearly lossless.
The Structure of this paper is described as follows: In section II deals with the proposed method, including authentication signal generation, share data embedding and tampered data repairing and merits of proposed systems are described. Experimental results and a comparison of performance of the proposed method with other are shown in Section III, followed by conclusion in Section IV.

II. Proposed System

An image content authentication with a datarepair capability for grayscale document image viathe use of the Portable Network Graphics (PNG)image is proposed.An authentication signal is generated for each block of a grayscale document image and combined with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The generated shares are embedded into an alpha channel plane. 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 In the process of image authentication, an image block is marked as altered if the authentication signal computed from the current block content does not match thatextracted from the shares embedded in the alpha channel plane.
Data repairing is then applied to each altered block by a reverse Shamir scheme. Protecting the security of the data hidden in the alpha channel is also measured. This project proposes an authentication method that deals with the binary-like grayscale document images instead of pure binary ones and simultaneously solves the problem of image tampering

A. System Model

1. Pre-processing

In pre-processing method median filter is used to remove noise from the input test images.The median filter is a nonlinear digital filtering technique Median filtering is very widely used in digital image processing.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

2. Generation of Authentication Signals

Binarization: In binarization movement threshold technique is used. There are two gray values are calculated andapplied to moment-preserving thresholdingI. Compute T=(g1+g2)/2,where T is a threshold to binarize the I.
PNG format: Transform I into PNG format using alpha channel plane.
Beginning of loop: Block of 2x3 to get 6 pixels p1, p2, p3, p4, p5, p6.
Creation of authentication signals: Generate a 2-bit authentication signal

s=a1*a2
a1=p1 xor p2 xor p3
a2=p4 xor p5 xor p6

3. Creation and Embedding of Shares

Creation of data for secret sharing: Concatenate the 8 bits of a1, a2, and p1 through p6 to form an 8-bit string & divide the string into two 4-bit segments, and transform the segments into two decimal numbers and m1,m2 respectively.
Partial share generation: Set p,Ci,Xi values & generate six partial shares q1 through q6.
Mapping of the partial shares: Due to mapping justadd 238 to six partial shares q1 through q6 andget q1' through q6'.The total transparency range is 238 to 254.
Embedding two partial shares in the current block: select the first two pixels in the raster-scan order, and replace their values by q1' and q2' respectively.
End of loop: If there exists any unprocessed blockin Ib , then go to beginning of the loop.
Otherwise, takethe final I in the PNG format as the desired stego-image I'.

4. Extraction of the embedded two representative gray values

Binarization of the stego-image:
Compute T=(g1+g2)/2,and use it as a threshold to binarize I'.Binary version Ib' of I with '0' represents g1 and '1' represents g2.

5. Verification of the Stego Image

Beginning of looping: Take an unprocessed block Bb' from Ib' with pixel values p1 throughp6.
Extraction of the hidden signals: Extract the hidden authentication signal by subtracting 238 from each q1' &q2and extract the two values of d and c1, and transform d and c1 into two 4 bit binary values & concatenate them to form an 8 bit string.
Computation of the authentication signal from the current block content:Compute a 2-bit authentication signal
s'=a1'*a2'.
Matching of the hidden and computed authentication signals and marking of tampered blocks: Match s and s' by checking if a1=a1' and a2=a2'.
End of loop: If there exists any unprocessed block in Ib', then go to beginning of the loop; otherwise, continue.

6. Self Repairing of the Original Image

Extraction of the remaining partial shares: Perform the following steps to extract the remaining four partial shares.Use key to collect the four pixels and take out the respective data q3', q4', q5', and q6' embedded in them.Subtract 238 from each of q3' through q6' to obtain q3 through q6 respectively.

Repairing the tampered regions: Perform the following steps to repair it if possible.

- From the six partial shares q1 through q6 of block Bb' in corresponding to B'.
- Extract the values of c1 and d.
- Transform c and d1 into two 4-bit binary values, and concatenate them to form an 8-bit string s'.
- Take the last 6 bits and check their binary values to repair the corresponding tampered pixel values.

Finallytake the final I' as the desired self-repaired image.

Advantages of Proposed System

- Providing pixel-level repairs of tampered image parts.
- Having higher possibility to survive image content attacks.
- Making use of a new type of image channel for data hiding.
- Causing no distortion to the input image.

III. Experimental Results

Experimental result using a document images are shown below:

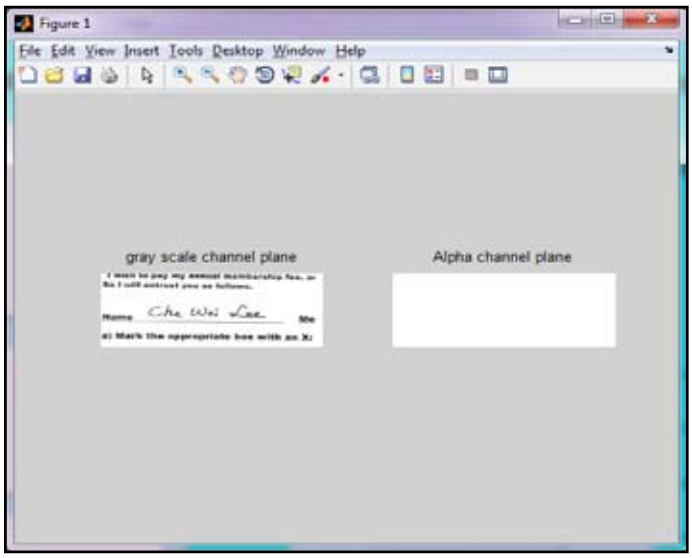

Fig. 1. Grayscale channel plane and alpha plane

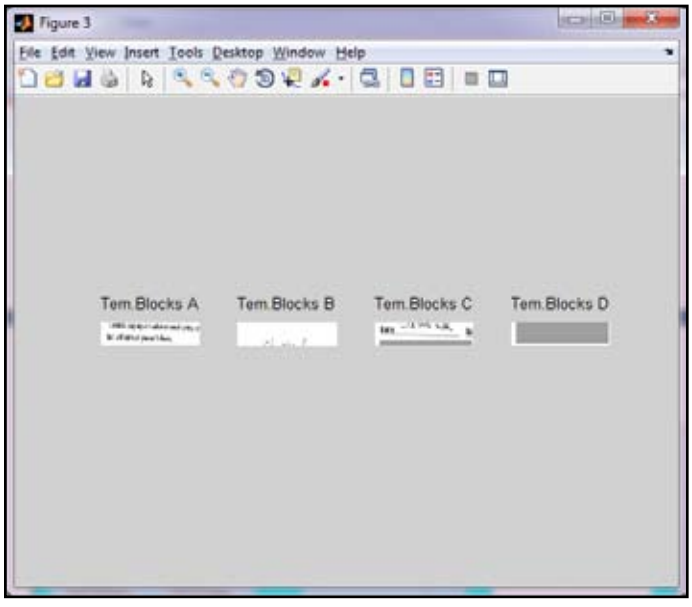

Fig. 2. Various Tampered blocks

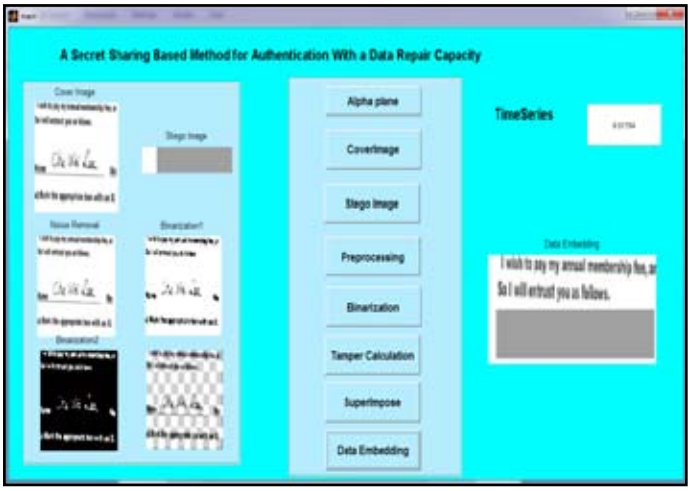

Fig. 3. Authorization result of an image in PNG format
(a) Original cover image. (b)Original image in Stego PNG format. (c) Noise removal. (d& e) Binarizedimage of original image. (f) Super imposing (g) Data embedding result.

Table 1: Comparison of document image authentication methods.

	Distortionin stego-image	Repair cabability	Distribution of authenticated image-parts	Manipulation of data embedding
Wu and Liu [2]	Yes	No	Non-blank part	Pixel fippability
Yang and Kot [3]	Yes	No	Non-blank part	Pixel fippability
Yang and Kot [4]	Yes	No	Non-blank part	Pixel fippability
Tzeng and Tsai[6]	Yes	No	Entire image	Pixel replace-Ment
Proposed method	No	Yes	Entire image	Alpha channel Pixel replace-Ment

Comparison of the capability of the proposed method with those of four existing methods is shown in Table1. All the proposed method will create alteration in the stego-image during the authentication process. More significantly, only the proposed method has the capability of repairing thetampered parts of an authenticated image.

IV. Conclusion

A secret sharing method for binarygrayscale document images has been proposed. In this method an image authentication and if an erroroccurs, data repair capability is available. By usingShamir method, the generated signal is convertedinto shares, and then they are allowed to passthrough the alpha channel plane and form a stegoimage. The image is in the PNG format. The undesired opaque effect visible in the stego-image coming from embedding the partial shares has been eliminated by mapping the share values into a small range of alpha channel values near their maximum transparency value of 255. In the process of image block authentication, an image block is marked as tampered, if the computed authentication signal does not match with the corresponding partial shares in the alpha channel plane,then data repairing is applied to each tampered block by a reverse Shamir scheme. This is used to manipulate theoriginal content of block from untamperedshares obtained.

References

[1] *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 a Data Repair Capability," IEEE Trans. ImageProcess., vol. 21, no. 1, Janury 2012.*

[2] *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.*

[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] *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.*

[7] *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.*

[8] *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.*

[9] *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.*

[10] *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.*

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

[12] *C. S. Lu and H.Y.M.Liao,"Multipupose watermarking for image authentication and protection, "IEEE trans. Image*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

process., v ol.10,no.10,pp.1579-1592,Oct.2011.

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

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

M.Mahalakshmireceivedher B.Edegree in Electronics and Communication engineering in Vickram College of engineering, Sivagangai in 2012.She is currently pursuing her M.E degree in Computer and Communication Engineering in Sethu Institute of Technology, TamilNadu, India.

C.Callins Christiyana received her B.E degree in Computer Science and Engineering in National College of Engineering, Virudhunagar.She has received her M.Tech degree in M.S University, Thirunelveli. She is currently pursuing her Ph.D degree in Anna University, Chennai.