Authentication of Document Images with Self Repair Capability

Sarita Kulhari
Department of Electronics & Telecommunication
Navi Mumbai, Maharashtra, India

Nilashree Wankhede
Department of Electronics & Telecommunication
Navi Mumbai, Maharashtra, India

ABSTRACT

An authentication method for grayscale document images, based on the secret sharing technique with a data repair capability via the use of Portable Network graphics (PNG) image is proposed. An authentication signal is generated for each block of a grayscale document image and then using Shamir secret sharing scheme grayscale document image authentication signal and binarized block content is combined and transformed into several shares. These several binarized block content shares are combined into an alpha channel plane. The original grayscale image combines with alpha channel plane to form a PNG image. If the authentication signal measured from the current block content does not match that extracted from the shares embedded in the alpha channel plane then image block is marked as tempered. Further, two shares from unmarked blocks are collected using reverse Shamir scheme and then data repairing is applied. Some security measures for protecting the security of the data hidden in the alpha channel are also proposed.

Keywords

Data repair, grayscale document image, image authentication, PNG, secret sharing.

1. INTRODUCTION

Digital images and documents are widely used to preserve important information. With the advancement of digital technologies, it is easy to make modification in the content of digital images. But biggest challenge in the security of digital image is to provide authentication to digital documents. So it is urgent to design an effective method to solve authentication problem [1]. If part of document image has been tempered, the destroyed content can be repaired.

In many fields, self repairing capability and image content authentication are useful for protection of digital documents images. Many fields such as important agreement, signed documents, marks cards, legal documents, scanned cheques and certificates etc require highly efficient authentication and image repair capability. These kinds of images are known as binary, although they have gray valued in nature. The advantage with this type of images is to reduce the size of image by using the concept of Binarization. But the Binarization process often destroys the smoothness of boundaries of text characterizes and creates reduced zigzag pattern of contours.

In general, authentication of binary documents image is difficult because of its simple binary nature that leads to discernible changes after authentication process. The recognition of tampered part of binary images is very complex in nature and it is challenging task. The problem with binary image is visual quality of resulting image and issue of preventing image tampering.

In the paper, we proposed authentication method with self repair capability of grayscale images instead of pure binary and overcome the problem of image tampering detection and keeping visual quality. The proposed method is based on (k, n) threshold secret sharing scheme proposed by Shamir [2] in which a secret message is divided into n participants and when k participants are present they can recovered secret message. Conventionally, secret sharing and data hiding for image authentication are two issues in information security. In the proposed method, we combined them together and developed a new authentication method. A secret sharing scheme is used to carry authentication signals and also help to repair tampered data through the use of shares.

The problem with self-repairing of tampered data at attacked part is after the original data of cover images are embedded into the image itself. Cover image is removed from the first place for use of later data repairing and the original data are no longer available for data repairing. So data repaired result is not accurate.

A solution for this problem, embed the original data image over other place without change the cover image. In proposed method, this problem is solved by using extra alpha channel in PNG image to embed the original image data. Another problem is data embedded in carrier are often large sized. In our case, alpha channel as the carrier, this is not a problem because cover image that deal with binary like and thus may just embed into the carrier a binary version of cover image that contain much less data.

2. LITERATURE REVIEW

One such method was proposed by Chih-Hsuan Tzeng and Wen-Hsiang Tsai [3] where they authenticated images with embedding special codes. Embedding randomly generated codes into the blocks of a given cover image they produced a stego-image. Authentication was achieved by them when verifying the code in the blocks of a given stego image.

H. Yang and A. C. Kot [4] proposed a method for authentication cryptographic signature and block identifier provide a two-layer authentication in which the first layer provides the overall authentication by hiding the cryptographic signature(CS) of the image and the localization of the tampering is obtained from the second layer by embedding the block identifier(BI) in the "qualified" or "self-detecting" macro-blocks(MBs).

M Wu and B. Liu [5] proposed an authentication method where flippable pixels were manipulated. In this method image is portioned into blocks and significant amount of data will be embedded into each block and then maintain a block based relationship without introducing noticeable artifacts.

Lee et al. [6] proposed a hamming code based data embedding method that flips one pixel in each binary image block for embedding a watermark. They provide reconstructed image with small distortion.

Che Wei Leeand Wen Hsiang Tsai [7] proposed a secret sharing method for authentication of grayscale document images. This method provides data repair capability via the use of PNG image.

Maxemchuk et al. [8] used a method for bulk electronic publications to embed information in textual images where the line spacing was changed along with character spacing. The amount of data that can be hidden is limited in these approaches and cannot be easily extended to other binary images.

Another approach data embedding in text for a copier system was proposed by A. K. Bhattacharjya et al. [9] by treating binary image as a grayscale one and manipulating the luminance of dark pixels slightly so that the change is hardly noticeable to human eyes yet detectable by scanners. This approach, targeted at intelligent copier systems, is not applicable to bi-level images hence is beyond the scope of this method. For grayscale or colour images to binary images have the bi-level constraint also limits the extension of many approaches proposed.

Hae Yong Kim, Amir Afif [10] proposed a secure authentication watermarking for halftone and binary images which compiles with this requirement. The method is quite simple. It consists on choosing a set of pseudo-random pixels in the image, clearing them, computing the message authentication code (MAC) of the random-pixels-cleared image, and inserting the resulting code into the selected random pixels. The technique is proposed for authentication of only digital binary images. Printed images cannot be authenticated using the proposed technique.

3. PROPOSED WORK

The proposed scheme is (2, 6) secret sharing scheme based on (k, n) threshold secret sharing scheme proposed by Shamir. The authentication signal is generated using 2 by 3 block size of image. Then these authentication signals are mapped as shares in the image. Reverse Shamir secret sharing method is used for repairing of tampered part of image.

Algorithm 1: (k, n) threshold secret sharing

Input- considers secret‘d’ in form of integers, ‘n’ numbers of participants and threshold should be k ≤ n.

Output- output is ‘n’ shares in the form of integer for ‘n’ participants.

1) in this step choose randomly prime number ‘p’ which is larger than‘d’.

2) Choose k-1 integer values $c_1, c_2 \dots\dots\dots, c_{k-1}$ between 0 to p-1.

3) Choose n distinct real values $x_1, x_2 \dots\dots\dots.., x_n$

4) By using the following (k-1) degree polynomial equation, compute n values$F(x_i)$, known as partial shares, for *i=1, 2, n.*

$$F(x_i) = (d + c_1x_1 + c_2x_2^2 + \cdots + c_{k-1}x_i^{k-1}) mod\ p \qquad (1)$$

5) Then transfer the two tuple $(x_{i,}\ F(x_i))$ as a share to i^{th} participants *i=1, 2......., n.*

There is k number of coefficients denoted by d and c_1 throughc_{k-1}. Finally collect k shares from n participants to form k equations to recover secret d.

Algorithm 2: secret recovery of shares

Input- from the n number of participants selects k shares and the prime p where as p and k both are prime.

Output- in the shares, the secret d hidden and coefficient c_i used in $F(x_i)$ where *i= 1,2.....k-1*

1) In this step use k shares

$(x_1, F(x_1)), (x_2, F(x_2)), \dots, (x_n, F(x_k))$To set up

$$F(x_j) = (d + c_1x_j + c_2x_j^2 + \cdots + c_{k-1}x_j^{k-1}) mod\ p \qquad (2)$$

Where *j=1,2.....,k.*

2) By using Lagrange’s interpolation equation [2] to solve the above equations

$$\begin{aligned} d &= (-1)^{k-1}\Bigg[F(x_1)\frac{(x_2x_3 \dots\dots..x_k)}{((x_1-x_2)(x_1-x_3)\dots(x_1-x_k))} \\ &+ F(x_2)\frac{(x_1x_3 \dots\dots..x_k)}{((x_2-x_1)(x_2-x_3)\dots(x_2-x_k))} + \cdots \\ &+ F(x_k)\frac{(x_1x_2x_3 \dots\dots..x_{k-1})}{((x_k-x_1)(x_k-x_2)\dots(x_k-x_{k-1}))}\Bigg] modp \qquad (3) \end{aligned}$$

3) Then the following equality and comparing the result with (1) in step, find out c_1 throughc_{k-1}, while regarding variable x in the equality below to be x_j in (2)

$$\begin{aligned} F(x) &= \Bigg[F(x_1)\frac{(x-x_2)(x-x_3)\dots(x-x_k)}{((x_1-x_2)(x_1-x_3)\dots(x_1-x_k))} \\ &+ F(x_2)\frac{(x-x_1)(x-x_3)\dots(x-x_k)}{((x_2-x_1)(x_2-x_3)\dots(x_2-x_k))} + \cdots \\ &+ F(x_k)\frac{(x-x_1)(x-x_2)\dots(x-x_{k-1})}{((x_k-x_1)(x_k-x_2)\dots(x_k-x_{k-1}))}\Bigg] modp \end{aligned}$$

4. IMAGE AUTHENTICATION AND DATA REPAIRING

In the proposed method, by using a binary like grayscale document image with alpha channel plane a PNG image is created. Fig.1 shows creation of PNG image. Then PNG image is binarized using threshold value. Data for authentication and repairing are then computed from binarized image and taken as input to the Shamir secret sharing scheme to generate n secret shares.

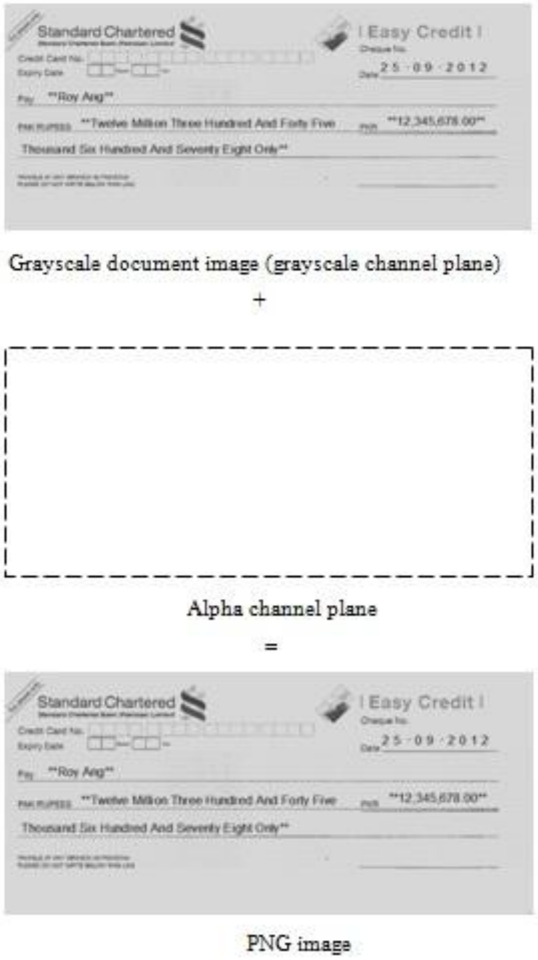


Fig 1: illustration of creation of a PNG image from a greyscale document image and an additional alpha channel plane

Finally for data authentication and data repairing capability, mapped secret shares are embedded into the alpha channel plane. Fig 2 shows Creation of stego image.

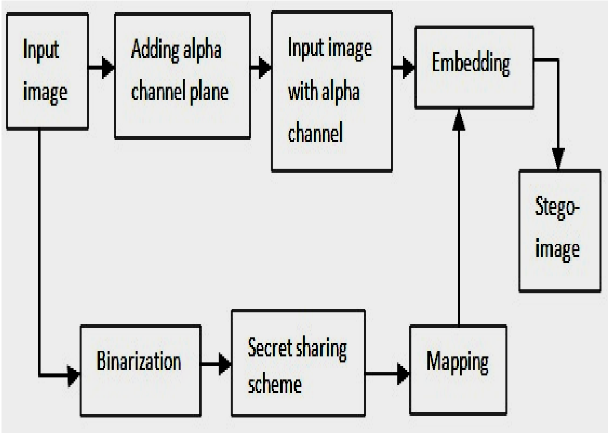


Fig 2: Creating stego image with embedded authentication signal

Algorithm 3: generation of stego image

1) The input image is converted into binary image using threshold value and threshold value is calculated using the main gray scale values.

2) Sequentially the alpha channel is added in the input image and this alpha channel is used to embed the authentication signal for authentication and data repair purpose.

3) In raster scan 2*3 block of binary image is scanned with pixels value $p_{1,}p_2$..........,p_6 and this pixels values are used to create authentication signal$s = a_1a_2$ with $a_1 = p_1 \oplus p_2 \oplus p_3$and $a_2 = p_3 \oplus p_5 \oplus p_6$, Where ⊕ denotes exclusive–or operation.

4) An 8 bit string $a_{1,}a_2$ and p_1 through p_6 is divided into two 4-bit segments and then convert each segments into decimal numbers m_1 and m_2 respectively. Consider d (secret) = m_1 , c_1 (coefficient) = m_2 and $x_1 = 1, x_2 = 2, \dots \dots \dots, x_6 = 6$. Algorithm 1 is performed as (2, 6) – threshold secret sharing scheme to generate six partial shares q_1 through q_6 using equation-

$$q_i = F(x_i) = (d + c_1x_i)modp \qquad (3)$$

Where *i= 1,2,......,6*

5) Mapping partial shares by adding 238 to each of q_1 through q_6 to generate new value $q_1^{'}$ through$q_6^{'}$, respectively. This is fall in the nearly total transparency range of 238 through 254 in the alpha channel plane. $q_i^{'} = qi+238;$

6) Embedded $q_1^{'}$ and $q_2^{'}$(two partial shares) at the first two pixels of current block and remaining partial shares at random pixels outside the block. Whenever selecting these four pixels select any pixels of block but not the first 2 pixels. The key ‘k’ is used to put these four pixels randomly in the alpha channel plane.

7) Same procedure is repeated for the whole blocks in the entire image. Finally image has taken in PNG format.

Authentication, Tamper detection and repairing

1) Convert stego image into binary image by computing threshold value using the two main gray values.

2 Extraction of authentication signal): To obtain shares q_1 through $q_2$subtract 238 from each of $q_1^{'}$ through$q_2^{'}$, respectively. With shares (1,q_1) and (2, q_2) perform algorithm 2 to extract the two value d and c_1. Then transfer this into two binary values to form 8 bit string and take first 2 bit as $a_1$and a_2 of string.

3) Scan each 2 by 3 block in raster order with pixel values p_1 through p_6 and calculated $q_1^{'}$ through$q_6^{'}$. $a_1^{'} = p_1 \oplus p_2 \oplus p_3$ and $a_2^{'} = p_3 \oplus p_5 \oplus p_6$ then compare the extracted authentication signal with calculated authentication signal. If $a_1 = a_1^{'}$ and $a_2 = a_2^{'}$ both the signals are same image is called authentic image otherwise tampered image. if image is tampered perform following step.

i) Extracted remaining partial shares $q_3^{'}$ through$q_6^{'}$ using key k. Then obtain q_3 through q_6 by subtract 238 from $q_3^{'}$ through$q_6^{'}$ respectively.

ii) From 6 partial shares 2 shares is considered as q_r and q_k which are not marked as tampered. With (r, q_r) and (k, q_k) perform algorithm 2 to extract d and c_1. Convert this d and c_1 into 4 bit binary value and formed 8 bit string.

iii) Take the last 6 bit of string $b_{1,}b_2, \dots \dots \dots . . b_6$and check their binary values to repair the tampered pixels value $x_1^{'}, x_2^{'} \dots \dots \dots . . , x_6^{'}$ of block. If $b_1 = 0$ set $x_i^{'} = g_1$ and $x_i = g_2$ where i=1,2....,6.

4) Finally obtain the desired self repaired image.

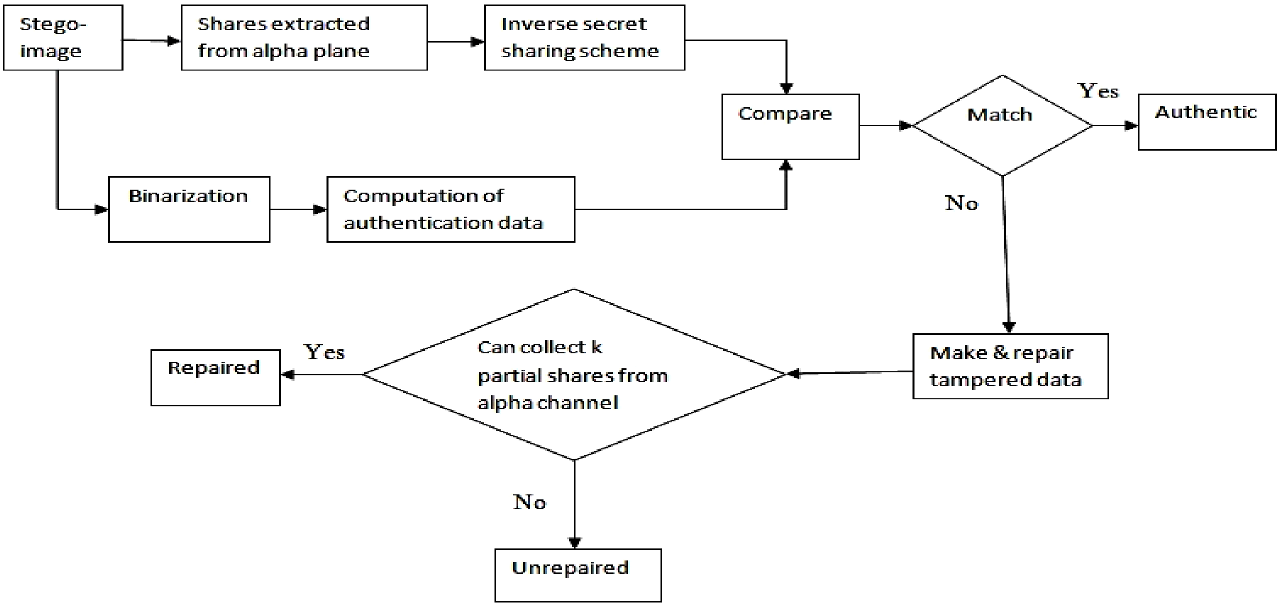
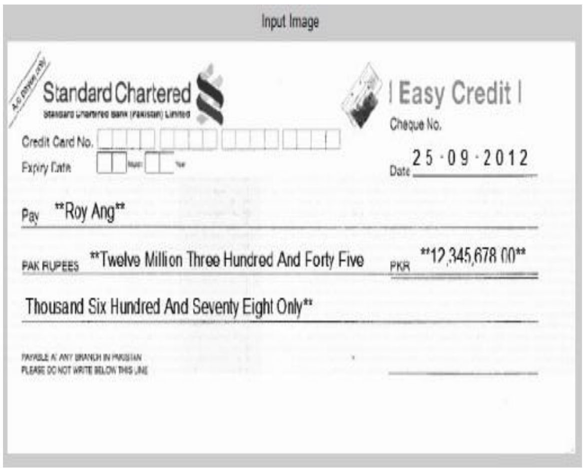

Stego-image
Shares extracted from alpha plane
Inverse secret sharing scheme
Compare
Match
Yes
Authentic
Binarization
Computation of authentication data
No
Make & repair tampered data
Can collect k partial shares from alpha channel
Yes
Repaired
No
Unrepaired

Fig 3: authentication process with self-repairing of stego image

5. EXPERIMENT RESULTS

An experiment result has obtained by using cheque image as shown in fig 4 (a).



Input Image

A/c payee only

Standard Chartered
Standard Chartered Bank (Pakistan) Limited

| Easy Credit |
Cheque No.

Credit Card No.
Expiry Date

Date 25 · 09 · 2012

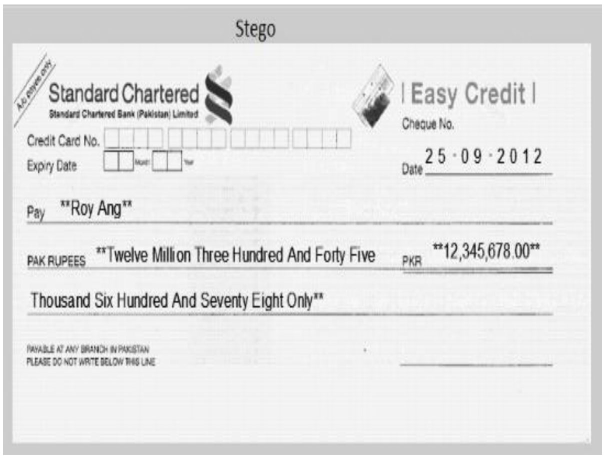
Pay **Roy Ang**

PAK RUPEES **Twelve Million Three Hundred And Forty Five PKR **12,345,678.00**

Thousand Six Hundred And Seventy Eight Only**

PAYABLE AT ANY BRANCH IN PAKISTAN
PLEASE DO NOT WRITE BELOW THIS LINE

(a)



Stego

A/c payee only

Standard Chartered
Standard Chartered Bank (Pakistan) Limited

| Easy Credit |
Cheque No.

Credit Card No.
Expiry Date

Date 25 · 09 · 2012

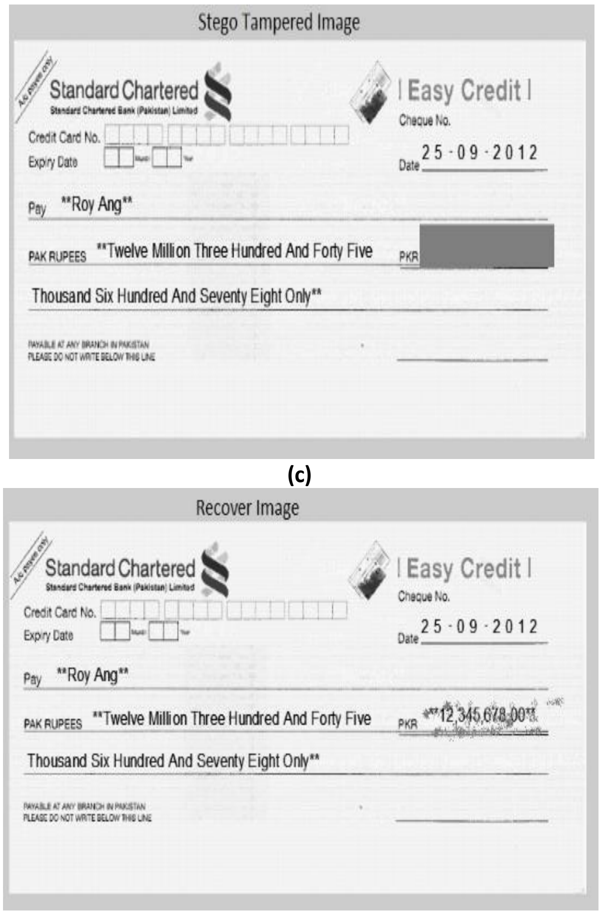
Pay **Roy Ang**

PAK RUPEES **Twelve Million Three Hundred And Forty Five PKR **12,345,678.00**

Thousand Six Hundred And Seventy Eight Only**

PAYABLE AT ANY BRANCH IN PAKISTAN
PLEASE DO NOT WRITE BELOW THIS LINE

(b)



Stego Tampered Image

A/c payee only
Standard Chartered
Standard Chartered Bank (Pakistan) Limited
| Easy Credit |
Cheque No.
Credit Card No.
Expiry Date Month Year
Date 25-09-2012
Pay **Roy Ang**
PAK RUPEES **Twelve Million Three Hundred And Forty Five PKR
Thousand Six Hundred And Seventy Eight Only**
PAYABLE AT ANY BRANCH IN PAKISTAN
PLEASE DO NOT WRITE BELOW THIS LINE

(c)

Recover Image

A/c payee only
Standard Chartered
Standard Chartered Bank (Pakistan) Limited
| Easy Credit |
Cheque No.
Credit Card No.
Expiry Date Month Year
Date 25-09-2012
Pay **Roy Ang**
PAK RUPEES **Twelve Million Three Hundred And Forty Five PKR **12,345,678.00**
Thousand Six Hundred And Seventy Eight Only**
PAYABLE AT ANY BRANCH IN PAKISTAN
PLEASE DO NOT WRITE BELOW THIS LINE

(d)

Fig 4: (a) original image. (b) stego- image with embedded authentication signal. (c) Tampered image. (d) Data repaired image.

Fig 4(b) shows stego image in PNG format with embedded authentication signal. Shares are generated and embedded using Shamir secret sharing scheme (2, 6). Where k=2 and n=6. Fig 4(c) shows tampered stego image with image editor. Gray block indicate tampered image parts. For each of detected tampered blocks, if at least 2 untampered shares are collected, its original content is repaired. Repaired image is shown in fig 4(d).

Merits of the proposed method

Proposed method has several advantages, which are

1) This methods provided pixel-level repairs of tampered image parts. So this method provided better repair effect for texts in images. Text or letter requires pixel level repairing because they are smaller in size.

2) This method enhances security of secret image. In this method data are embedded into the alpha channel plane in the form of shares instead of directly hiding in document image pixels.

3) This method use pixel values of alpha channel plane for authentication and repairing purpose. Original image remain untouched thus causing no distortion to it.

4) In this method a new type of image channel is used for data hiding. PNG image has extra alpha channel which is normally used to present transparency of image but in this case it is used for data hiding .so we have large space for data hiding.

6. CONCLUSION

We have proposed an image authentication method with a data repair capability for grayscale document images. By using Shamir secret sharing method, authentication signal are transformed into partial share. These shares are distributed into an alpha channel plane to create stego-image in the PNG format. Reverse Shamir method is used for self-repairing of tampered part which compute original content of block from any 2 untampered shares. For enhancement of security alpha channel plane is used. For future studies, we can select other size of block, prime number and Number of authentication bit etc for advance data repairing effect. Proposed method for authentication and repairing of attacked color images may also be tried.

7. REFERENCES

[1] C. S. Lu and H. Y. M. Liao, oct. 2001 multipurpose watermarking for image authentication and protection, IEEE Trans. Image Process., vol. 10, pp. 1579-1592.

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

[3] H. Tzeng and W. H. Tsai, Nov. 1979A 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.

[4] H. Yang and A. C. Kot, Dec. 2006Binary image authentication with tampering localization by embedding cryptographic signature and block identifier,IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741–744.

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

[6] R. B. Wolfgang and E. J. Delp, "Fragile watermarking using the VW2D watermark", inSecurity and Watermarking of Multimedia content, VOL.3657of SPIE proceedings, January 1999.

[7] Fridrich J (1998b) Methods for tamper detecting in digital images. In: Proceedings of the 6th IEEE international workshop on intelligent signal processing and communication systems (ISPACS ’98), Melbourne, Australia

[8] C.Y. Lin and S.F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content", in Proc. SPIE International Conf. On Security and Watermarking of Multimedia Contents, VOL. 3971, January 2000.

[9] Che-Wei Lee, Student Member, IEEE, 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 transaction on image processing, VOL. 21, NO. 1, JAN 2012.

[10] Venkatesan R, Koon S, Jakubowski M (2000) Robust image hashing. In: Proceedings of the IEEE international conference on image processing, vol 3, pp 664–666