Image Tampering Detection and Repairing

Jyoti Rao
Pad.Dr. D.Y.P.I.E.T. Pimpri
Pune

Sarika Jankar
Pad.Dr. D.Y.P.I.E.T. Pimpri
Pune

Ashwini Jarali
Pad.Dr. D.Y.P.I.E.T. Pimpri
Pune

ABSTRACT
It is very crucial to design efficient methods to provide authentication to document images mainly for images whose security must be protected. In digital media the authentication, tampering detection and repairing of the tampered data is main concern. Nowadays many digital documents are transferred on the internet regularly e.g. circuit diagrams, scanned cheques, signed documents, drawings, design drafts etc. Here the method of image authentication, tampering detection and repairing is explained. The grayscale image document image authentication with self repair method is provided. The authentication signal is calculated from binary image of the original document image. Secret sharing scheme is used to calculate this authentication signal. The extra alpha channel is embedded in the original grayscale document image. The calculated authentication signal is then embedded in this alpha channel. This is one of the way of visual cryptography in which image is visible but authentication signal will not be recognized. Then this authentic image is encrypted for better security. this whole procedure is done at sender side. In second module i.e. receiver side the image is decrypted. Then the embedded authentication signal is extracted from the received authentic image. The new authentication signal is calculated from the binary image of the received authentic image. This new authentication signal is compared with the extracted signal and the integrity check is provided. If data modification is detected, then the method is proved to repair the tampered pixels using the reverse secret sharing method. The tampering of data is detected successfully in this method without any original image backup. This type of secret sharing scheme is helpful for reducing the risk of incidental partial data loss. This method is also applicable to the color image. Algorithm for color image is also same as grayscale images. In this paper the result is provided only for the grayscale images and supposed to expand for color images as well.

Keywords
Data repair, Encryption, Alpha Channel, Secrete sharing scheme, greyscale image.

1. INTRODUCTION
Due to the open availability of digital image processing tools open access of the digital data is easily possible. So changes to original data and reuse of visual material are also becoming easy. And so nowadays is very easy to create illegal copies and to change the images in such a way that the identification of big economic or human lives losses is very difficult. These problems can be understood with an example. As nowadays the university papers are exchanged online the integrity of the papers is main issue. If some of the questions are modified at the time of transmission, that is a loss which cant be tolerated. It is very necessary to ensure the integrity and authenticity of a digital data of images. It is very important to propose effective methods to solve this type of image authentication problem. Secret image sharing scheme has been offered to solve this problem. Secret image sharing method generates several share which are then shared in the protected document image, and the protected image at receiver side is reconstructed by enough different shared shares. If part of an image is verified to be modified illegally, the changed content can be repaired. The main advantage of this method is here we don't require original image to check the integrity of received data. The integrity is checked with received image only.

This type of image content authentication and self-repair capabilities are of use for security protection of digital documents or images. In this paper, a system for authentication of document images with extra self-repair capability for fixing tampered image data is explained. Using this extra authentication signal the tampering of the data is detected. This authentication signal is calculated form binary image with 2 main values. After this, the cover image is transformed into a stego-image by combining it with alpha channel for transmission on network. This image is then encrypted for security purpose. At receiver side the stego image is decrypted and then verified for its authenticity and integrity. Data modifications of the stego-image can be detected and repaired at the pixel level. In case if the alpha channel is completely removed from the stego-image, the integral resulting image is considered as unauthenticated, meaning that the integrity verification of the image fails. This method is based on the (k, n) secret sharing scheme. In this system a secret message is converted into n shares i.e authentication signal for embedding it in the original image; and when k of the n shares, are collected, the secret message can be recovered without any loss. This type of secret sharing scheme is helpful for reducing the risk of significant partial data loss.

In the proposed method the binary image authentication with repair capability is designed for both grayscale as well as color images. Using secret sharing scheme the shares are generated which are distributed randomly in the image block. For this authentication signal is generated and used to calculate the shares. Alpha channel is used for transparency and for mapping this extra authentication signal[2,4].

2. PROPOSED METHOD
The proposed system is based on the (2,6) secrete sharing scheme in which random sequence of decision are made for embedding the shares. The alpha channel can be used to embed the extra authentication signal information in the image. The alpha channel embedded in the PNG image is used to create required transparency of the image. In the proposed system the resulting alpha channel values are in a range of 142 to 254. The authentication signal is generated using the block size of 2 by 3 or can be changed to any size as per the size of the image (small or large size). Then these authentication signals are mapped as shares in the image. This is an image authentication method, not a secrete sharing method. These embedded shares are then used for checking the integrity of the image at receiver side.. If tampered, the system should recover it. The main advantage of this system is tampering detected successfully. Only problem is with the selected range e.g. if some pixel is in the range of 0 to 140 i.e. consider 130 and the range of 130 is changed in between of 0

and 140, this type of changes can't be verified. The same problem is faced with the color images.

The approach to secret image sharing is based on the (k, n)-threshold secret sharing method. For a group of n secret sharing participants n shares are generated from a secret integer value y for the threshold k. In next part the algorithm for image authentication and repairing are explained with results. Mainly explained in two modules sender side and receiver side.

2.1 Image Authentication at Sender Side

Input: Color/greyscal image. If color image then convert to greyscle. An image in grayscale G with two main gray values.

Output: A stego-image G in the PNG format with embedded authentication signals.

1) The input image is converted to binary image for authentication signal calculation. Threshold value is calculated using the main grayscale values. Then this threshold is used to generate the binary image.
2) Sequentially the alpha channel is embedded in the input image G. This extra alpha channel is used to embed the authentication signal which is used for authentication and repairing purpose. Then this image is converted to PNG format.

3) A 2 by 3 block of binary image is scanned in raster scan with pixels value p1,p2,…..p6. Using these pixel values two strings are generated. One is used as coefficient factor & second string used as secret.
4)For secret sharing scheme above values are set as follows
(a) d (secret)= $p_1p_2p_3$, c_1 (Coefficient)= $p_4p_5p_6$
(b) values of x_1 to x_6 are generated using Random generator for random values of X in the range of 0 less than xi less than 17 [1];

Following equation is executed for authentication signal generation. This is a (2, 6)-threshold secret sharing scheme [8], which is used to generate six partial shares q_1 through q_6

$$q_i=F(x_i)=(d+c_1x_i+c_2x_i^2+\ldots+c_{k-1}\,x_i^{k-1}) \quad \ldots\ldots\ldots\ldots(1)$$
where i = 1, 2..... 6.

5) New values of authentication signal are calculated by adding 142 to each of q_1 through q_6, resulting in the new values of qd_1 , through qd_6 , respectively. This fall in the range of 142 through 254 in the alpha channel plane G_α.
$qd_i = q_i + 142$;

6) Now these calculated qd_1 , through qd_6 are embedded in the six random position outside current block. The chosen 2 by 3 block position should be different from the embedded pixel positions. Because at receiver side these embedded pixels are used to repair the original pixel values. If we put authentication signal of original pixel on same position, we will miss the data used for the repairing. One key K is used to put these signals randomly in the alpha channel.

7) Same procedure is repeated for the whole blocks in the image. We can change the block size as well.

8) Now final G in the PNG format will be transferred to the receiver. Consequent embedding of q_1 to q_6 in such a narrow distance into the alpha channel plane means very alike values will appear everywhere in the image block, resulting in approximately consistent transparency effect.

2.2 Tampering detection and repairing at Sender Side

Input: A Stego-image G

Output: Original image if not tampered else repaired image.

Part 1: Take out the two embedded main representative gray values.

1) Take out the embedded authentication signal.
2) Convert the stego image to binary image. Foe binary conversion computes the threshold using the two representative grey values.
3) Start the loop until no block of 2 by 3 remains processed. Scan each 2 by 3 block in raster order with pixel values p_1 through p_6, & the new values qd_1, through qd_6 are calculated.
4) Now compare the extracted authentication signal with the new calculated authentication signal. If both the signal are same for the particular pixel then image is authentic else if image is tampered perform the following steps:

i) Subtract 142 from each of the untampered qd_i and qd_j partial shares. With two signal q and x Lagrange's interpolation equation can be solved [8] to obtain the 2 values d and c_1 (the secret and the coefficient value, respectively).

ii) Now convert this d and c_1 into two 4-bit binary values, and then find the pixel values $p_{1\ to}\ p_6$.

iii) Check the tampered pixels. Using these pixel values convert to either grey value g1 or g2 depending on its range. Put g1 if pixel value is 1 & g_2 if pixel value is 1 in received G image. If authentication signal is untampered then only repairing is possible. . If all the signals are tampered, repairing is not possible.

5) Exit the loop.

3. RESULTS AND DISCUSSION

Integrity and authentication of image can fail due to the fixed values of the x1 to x6 and K [2]. If x1 to x6 values are used between 1 to 6, then (1,q1) and (2,q2) can be easily forged. So it is possible to create a forged authentication signal.
In proposed method random values within the range of 3 to 17 are used. For all the m × n / 6 blocks the possibility of correctly guessing all these values in a stego- image can be roughly around
1/ [(17 × 16 ×15 × 14 × 13 × 12)] m × n /6.

Fig 1: Result Analysis

Here the example of the circuit diagram is taken to illustrate the system with a detailed result analysis. The sender side algorithm is applied on images which creates a stego image which is visually nearly same to the cover image. To check the system, attacks are performed on the stego image. Then depending on the tampered area analysis is done. As the size of tampering increases the repairing result decreases, because the embedded authentication signal is not enough for the repairing.

Using Adobe Fireworks i.e. image editing tool the superimposing attack is performed which is explained in the figure 1 & analysis is explained in table 1. In fig1.a the stego image is shown in which the signal is embedded for authentication purpose and its result is displayed in 1.a.1 without any tampering. Fig. 1.a.1 is final result at receiver side. In diagram 1.b the data is simply rubbed using an eraser which then detected and repaired at receiver side successfully. But it also tries to repair the untampered data. In 1.d the more size of the image is tampered it also successfully detected and

repaired at the receiver side in fig 1.e. But as shown in fig1.g and fig 1.h.1 repairing result is degrading.

Detection of tampering is done successfully. Consider one example if the range of pixel is from 10 to 200. So mid is 105. If somebody change s the pixel value from 130 to 150 or 50 to 10 it is not recognized as tampered due to the thresh holding of the image. The binary values are used to calculate the authentication signal and this authentication signal is used for repairing.

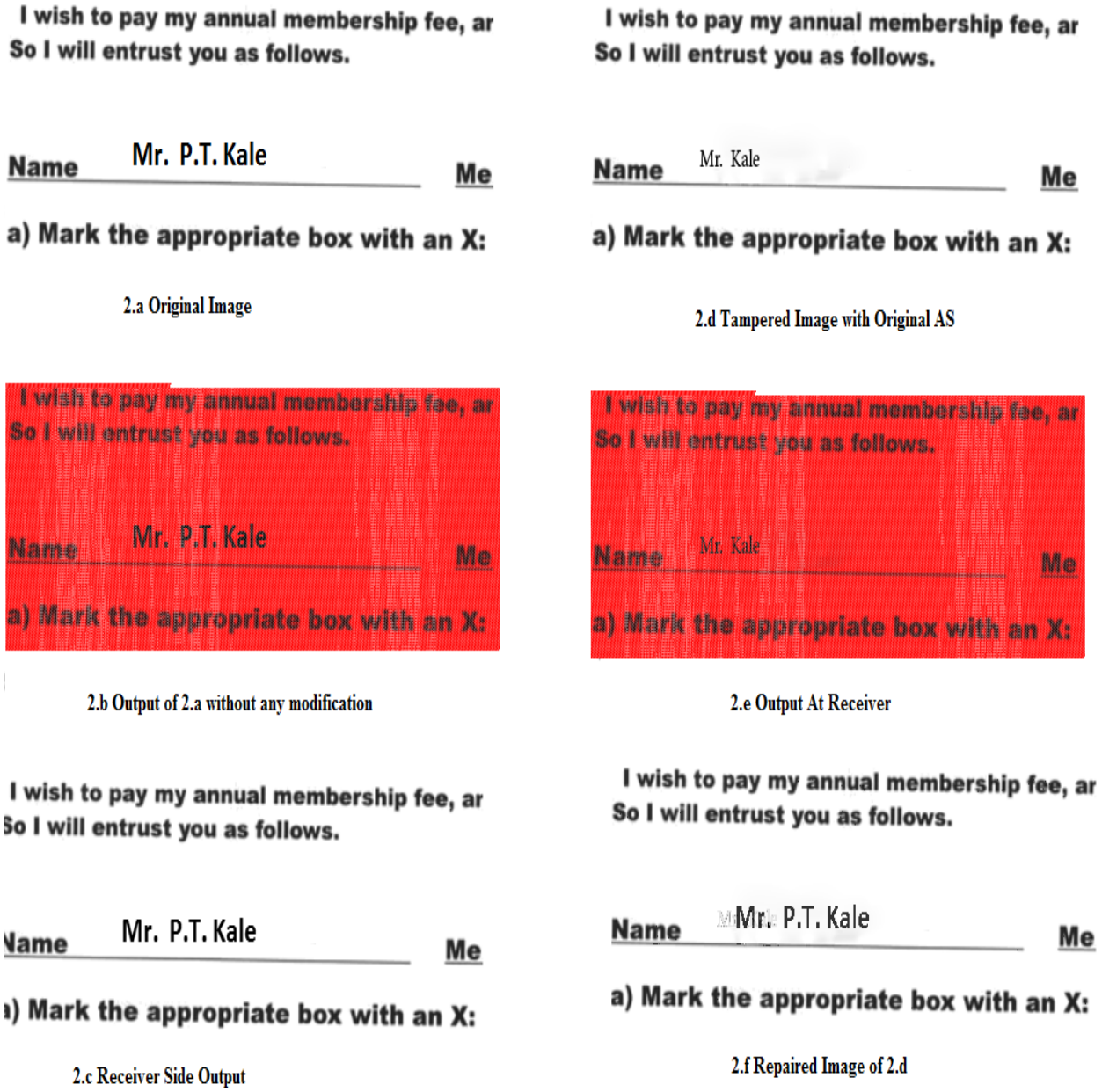

Fig 2: Result of the image which is tampered with the help of original authentication signal. Result of 2.d to 2.f shows the detection and repairing of tampered data.

If someone tries to change the original image (without authentication signal) and then tries to embed the original authentication signal in the modified image, it also detected at receiver side. As the alpha channel range is in-between 142 to 254, if the value of alpha channel is 255 means it is tampered. Using alpha channel it becomes very easy and cheap for image authentication and repairing (Fig. 2). To check whether image original or tampered we don't need original image at receiver side. Though repairing is not done successfully at least the content visualization is done using this method which is also very beneficial for content verification.

If full authentication signal i.e. alpha channel is removed from the image means the received image is fully tampered. Reject the image and to sender to send the new image.

This is another type of attack in which original authentication signal of the stego image is extracted from the stego image. Then the modification is done on the stego image and the extracted authentication signal is embedded in the modified image. As and when the image is received at receiver side the authentication signal is extracted from the stego image and new authentication signal is calculated from the image

(without alpha channel). This new calculated authentication signal is checked with the extracted authentication signal. If both the signal matches image is ok but if these signals differ, the data embedded in the authentication signal is used for repairing purpose. The same embedded data is used for tampering detection and repairing. Here tampering/modification is not done on the original stego image, the embedded authentication signal is taken out of the stego image. The modification is done on the original image. Then the extracted authentication signal is again embedded in the modified image in the concern that the change will not be detected by the receiver.

Table 1 Result of Superimposing Attacks

Size of Image (329 by 153)	No. of tampered pixels	No. of pixels repaired
Image 1.b	100	100
Image 1.d	38	30
Image 1.f	847	811
Image 1.h	1362	1249

This system is very useful in each and every filed where the authentication of the images is main concern. To check the authenticity of the image without any original backup is difficult. This system does not require lot of calculations and any complicated system to check the authenticity. Tampering localization is done successfully but repairing is bit complicated.

4. CONCLUSION

In this paper the document image authentication is explained, which provides image authentication with repairing capacity. In this system secret sharing scheme used for authentication calculation not for secret sharing method. These shares are embedded in the image itself for authentication and data is hidden in authentication signal for repairing purpose. To provide a better security than the previous one random values of x_1 to x_6 and K factor are used. To regain the original value of the tampered block the reverse secret sharing scheme is applied on the embedded authentication signal. Untampered authentication are used for repairing, else repairing is not possible. (2,6) secret sharing scheme is used for this purpose.
This algorithm is also useful for the color images. For color images binary thresholding should be strong so the exact color values of the tampered pixels can be regained from the authentication signal.

5. REFERENCES

[1] Shyamalendu Kandar, Bibhas Chandra Dhara , "K-n Secrete Sharing Visual Cryptography Scheme on Color Image using Random Sequence",IJCA (0975-8887)Volume 25-No.11 July 2011.

[2] Che-Wei Lee, And Wen-Hsiang Tsai, "Secret-Sharing-Based Method For Authentication Of Grayscale Document Images Via the Use Of The PNG Image With A Data Repair Capability "At IEEE Transactions on Image Processing, Vol. 21, No. 1, January 2012.

[3] Che Wei Lee, Wen Hsiang Tsai "A Grayscale Image Authentication Method with a Pixel-level Self-Recovering Capability against Image Tampering" MVA2011 IAPR Conference on Machine Vision Applications, June 13-15, 2011, Nara, JAPAN.

[4] 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, No. 12,Pp. 741-744, Dec. 2006.

[5] Chang-Chou Lin, Wen- Hsiang Tsai, "Secret Image Sharing With Steganography And Authentication" Department Of Computer And Information Science, National Chiao Tung University, Hsinchu 300,Taiwan,;Accepted 20 July 2003.

[6] Ching-Nung Yang , Tse- Shih Chen, Kun Hsuan Yu, Chung-Chun Wang "Improvements Of Image Sharing With Steganography And Authentication" Department Of Computer Science And Information Engineering, National Dong Hwa University, Sec. 2, Da Hsueh Rd., Hualien, Taiwan Received 22 October 2005;

[7] W. H. Tsai, "Moment-Preserving Thresholding: A New Approach," Comput. Vis. Graph. Image Process. Vol. 29, No. 3, Pp. 377-393, Mar.1985.

[8] Shamir, "How To Share A Secret," Commun. ACM,Vol.22, No.11,Pp.612-13,Nov. 1979.

[9] H. Yang And A. C. Kot, "Pattern-Based Data Hiding For Binary Images Authentication by Connectivity-Preserving," IEEE Trans. On Multimedia, Vol. 9, No. 3, Pp. 475-486, April 2007