An Effective Authentication Method for Document Type Color Images with Data Repairing Capabilities

Ashwini V. Kurzekar
Priyadarshini Institute of Engineering and technology, Nagpur

A. R. Mahajan, Ph.D
Priyadarshini Institute of Engineering and technology, Nagpur

ABSTRACT

This is new authentication scheme based on the secret sharing method with a data repair capability for document type color images via the use of portable network graphics (PNG) image. And generate the authentication signals to each block of image, which together with the binarized block content, this authentication signals are transformed into a several shares using the secret sharing Scheme. The characters are carefully chosen from image so that many shares as possible are generated and embedded into an alpha channel plane. The alpha channel is combined with the original cover image to form a PNG image. While shares embedding process, the computed shares values are mapped into a range of alpha channel value near their maximum value of 255 to yield a transparent stego image. In the process of image authentication, the block in an image is marked as a tampered if the authentication signal computed from the current block content of a binary image does not match that extracted from the share embedded in the alpha channel plane. Data repair is applied to each tampered block after collecting two shares from unmarked block.

Keywords

Image Authentication, Data Hiding, Secret Sharing, Portable Network Graphics, Data Repair, stego image

1. INTRODUCTION

Image transmission is a major activity in today's discussion. As Digital images are widely distributed via the internet and different public channels. With the advance of digital technologies; it is now easy to modify the content of digital images without causing noticeable changes, resulting possibly in tampering of images. And for that design the effective method for image authentication, which aims to check the integrity of received images. There is a need for copyright protection against the unauthorized data reproduction.

Conventional copyright protection technologies such as authentication mechanism that is employed for digital content applications are helpless by a drawback. The illegal reproduction of the copyrighted content can no longer be prevented. Once the image is authenticated and if someone can make some modification in that image, that time we cannot say that the image is authenticated.

1.1 Image Authentication

Authentication of digital documents has the great interest due to their wide application areas such as important certificates, digital books, legal documents and engineering drawings. Important certificates such as fax doc, insurance copy and personal documents are digitized and stored. It is very important that how to ensure the authenticity and integrity of the documents. And on the other side, there is a powerful image editing software is available which copying and editing an image more easily with less noticeable changes. Authentication of images and detection of tampering in an image are thus main goal. Data hiding or watermarking for binary images authentication has been a promising approach to alleviate these concerns. Most prior works on data hiding with watermarking focus on grayscale or color images in which the pixel takes a wide range of values, slightly perturbing the pixel value by a small amount causes no perceptible distortions.

Digital Image is used to preserving important information of a document. But, advance of digital technologies, it is easy to make modifications to the contents of digital images. So, how we ensure the authenticity and integrity of a digital image is thus a challenge. So it is important to design effective methods to solve this kind of image authentication problem, particularly for document type images whose security must be protected. And, if any block of a document image is verified and which have been illicitly altered or changed, then contents of an image which is destroyed can be repaired. Such as image authentication and repair capabilities are useful for the security protection of digital documents in many fields, such a signed documents, certificates, scanned checks, design drafts, circuit diagrams, art, last will and testaments, and so on. Document-type images, which include tables, texts, line arts, etc.

1.2 Data Hiding

Data hiding represents a class of processes used to embed a data, like as copyright information about the document, into various forms such as audio, image or text with a minimum amount of perceivable degradation to the "host" signal; i.e., the embedded data should be invisible and inaudible to a human observer.

Data hiding, is a one of the form of steganography, embeds data or information into digital media for the identification purpose, copyright, annotation. Several constraints which affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g. lossy compression I an image, and the degree to which the data must be immune to modification, interception, or removal by a third party. Two important uses of data hiding in digital media are giving the assurance of content integrity and to provide proof of the copyright.

2. LITERATURE SURVEY

A novel blind data hiding method for binary images authentication aims at preserving the connectivity of pixels in a local neighborhood. Data hiding is pattern based method for

binary image authentication in which three transition criteria are used to determine the flippabilities of pixels in each block; the watermark is embedded into embeddable blocks that deal with the uneven embeddability condition which present in the host image.

The "flippability" of a pixel is determined by imposing three transition criteria in a 3*3 moving window centered at the pixel. The "embeddability" of a block is invariant in the watermark embedding process; hence if want to extract watermark then it can be extracted without referring to the originl image. The "uneven embeddability" of the host image is handled by embedding the watermark in only those "embeddable" blocks in an image [1].

Yang and Kot proposed a two-layer binary image authentication method in which one layer is used for checking the image fidelity and the other layer is for checking image integrity. In authentication method which is based on two layers, a connectivity- preserving transition of pixel criterion is used for determining the flippability of a pixel for embedding the cryptographic signature and for the block identifier purpose. A two-layer blind binary image authentication scheme, in which the first layer is design for overall authentication and the second layer, is design for identifying the tampering locations. The "flippability" of a pixel is determined by the "connectivity-preserving" transition criterion.

The authentication is achieved in the first layer by hiding the cryptographic signature (CS) of the image. The detection of tampering is achieved in the next layer embedding the block identifier (BI) [2].

A new binary image authentication method with small distortion and low false negative rates system is proposed. It is based on Hamming-code- data embedding method that flips one pixel in each binary image block which is used for embedding a watermark into an image, so causing the small distortions and low false negative rates [3].

Y. Lee, H. Kim and Y. Park proposes a data hiding scheme for binary images, which includes the document type images, scanned figures text and signatures. In data hiding method, embedding efficiency and the placement of embedding changes are perform simultaneously. Take M×N image block, the upper bound of the amount of bits that can be embedded of the scheme is nlog2((M×N)/n + 1) by changing at most n pixels. This scheme can embed more data, as wel it maintain a better quality, and have wider applications. This data hiding scheme embed more amount of data and it will not affected the quality of the image [4].

Min Wu and Bede Liu propose a new method to embed data in binary images, the images contains scanned text, figures, and signatures. The data hiding method in which "flippable" pixels criterion is used to enforce specific blockbased relationship in order to embed a significant amount of data without causing noticeable changes. Shuffling of pixels is applied before embedding to equalize the uneven embedding capacity from region to region. The hidden data in image can be extracted without using the original image, and data can be extracted after high quality printing and scanning with the help of a few registration marks. The data embedding method can be used to detect unauthorized use of a digitized signature, and annotate or authenticate binary documents [7]

Min Wu and Bede Liu proposed in paper data hiding in image and video in that they addresses a number of fundamental issues of data hiding in image and video and propose general solutions to them. Also they propose a new multilevel embedding framework to allow the amount of extractable data to be adaptive according to the actual noise condition. As well as the issues of hiding multiple bits through a comparison of various modulation and multiplexing techniques. Finally, the non-stationary nature of visual signals leads to highly uneven distribution of embedding capacity and causes difficulty in data hiding. Min Wu and Bede Liu proposed an adaptive solution switching between using constant embedding rate with shuffling and using variable embedding rate with embedded control bits. They verify the effectiveness of their proposed solutions through analysis and simulation. And apply these solutions to specific design problems for embedding data in grayscale and color images and video [8].

3. PROPOSED RESEARCH METHODOLOGY

The conventional copyright protection technologies such as authentication mechanism that is employed for digital content applications are helpless by a common drawback. The illegal reproduction of the copyrighted material can no longer be prevented. Once the image is authenticated and if someone can make some modification in that image, that time we cannot say that the image is authenticated.

To provide a well-developed intellectual property rights protection scheme, an innovative approach has been proposed. The proposed method preserves image authentication whatever modification has been made in that image.

Authentication method based on the secret sharing technique with detection of tampering and data repair capability for color document type images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a color document image which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. PNG image is created from a binary document image with an alpha channel plane. The alpha channel is act like a carrier. The original image may be thought as a grayscale channel plane of the PNG image. Since the alpha channel plane is used for carrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication. So, first we add the alpha channel to the original color image. Now the image containing the four channels i.e. ARGB. In that 'A' stands for alpha. Alpha channel is used for carrying the authentication signals.

The concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security. However, in the proposed method, combine them together to develop a new image authentication technique. The secret sharing scheme is used in the developed technique not only to carry authentication signals and image content data but also to help repair tampered data through the use of shares.

The self-repairing of tampered data in an attack image, after the original data of the cover image are embedded into the image itself for use in later data repairing, but if the cover image is destroyed and the original data which is embedded in that image are no longer available for data repairing, resulting in a contradiction. So in the proposed system to embed the original image data somewhere else without altering the cover image itself. So we proposed the solution for that is using the extra alpha channel in PNG image to embed the original image data. Alpha channel is used for creating transparency in the PNG image. In proposed system is to map the resulting Alpha channel value into small range near their value of 255 yielding an imperceptible transparency effect on the alpha

channel plane. So, in the proposed system, a PNG image is created from binary type color document image, the image containing the alpha channel plane. First change this color image into the grayscale image. Then we get grayscale image, and we consider this grayscale image is original image may thought as a gray scale channel plane of the PNG image.

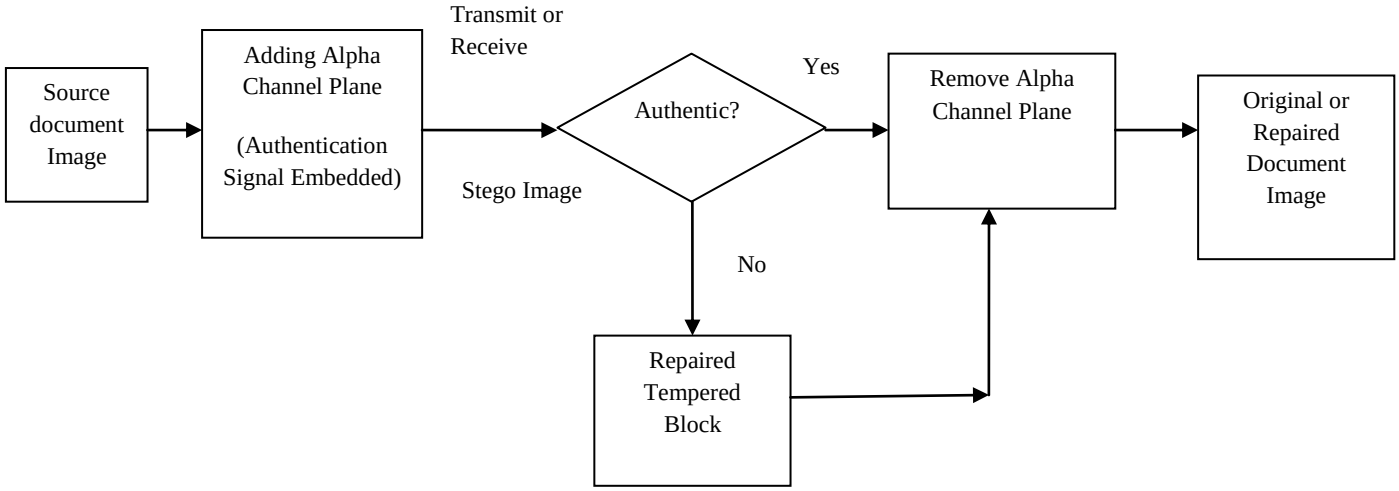


Fig 1: Framework of proposed document image authentication method

Alpha channel is used for carrying data, which is used for authentication method and for repairing process. Authentication method causes the destruction in original image to overcome this problem we proposed secret sharing authentication method for document type color image as well as provide the data repairing capacity.

4. SECRET SHARING AND SECRET RECOVERY

4.1 Secret Sharing

Secret sharing algorithm is introduced by the Shamir [9]. In secret sharing algorithm, secret data d with n participant and threshold k which is passed as an input, Where k<= n. And getting n shares as output for the n participant. So for that we required the prime number p which is greater than d and k-1 coefficient i.e. c_1, c_2... c_{k-1} and n real values i.e. x_1, x_2...x_n. So shares are generated using the following formula,

Algorithm1: Secret Generation

Step1: Choose prime number p randomly, which is greater than d

Step2: Choose integer value c_1, c_2, c_3,…, c_{k-1}; which is in the range of 0 to p-1

Step3: Choose n different real values i.e. x_1, x_2, x_3,…,x_n

Step4: Calculate partial shares using formula

$$F(x_i) = (d+c_1x_i+c_2x_i^2+\ldots+c_{k-1}x_i^{k-1}) \bmod p \quad (a)$$

Step5: $[x_i, F(x_i)]$ which is taken as a shares for i=1,2,3,…,n.

4.2 Secret Recovery

The Secret recovery algorithm is also introduces by Shamir. Secret recovery algorithm which is used for recover the secret at the time of authentication and data repairing. So input to the secret recover algorithm is k shares which is collected from the secret sharing algorithm with prime number p and threshold k. And output as secret data d which is present in the shares and coefficient. So for extracting d from shares with the use of following formula,

Algorithm2: Secret Recovery

Step1: Take input as k shares i.e. $[x_1, F(x_1)]$, $[x_2, F(x_2)]$, $[x_3, F(x_3)]$…, $[x_k, F(x_k)]$

Step2: Calculate the value of d using the formula

$$d = (-1)^{k-1}[F(x_1) * x_2x_3\ldots x_k / (x_1-x_2)(x_1-x_3)\ldots(x_1-x_k) + F(x_2) * x_1x_3\ldots x_k / (x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)+\ldots + F(x_k) * x_1x_2\ldots x_{k-1} / (x_k-x_1)(x_k-x_2)\ldots \ldots (x_k-x_{k-1})] \bmod p \quad (b)$$

Step3: Find the coefficient c_1 to c_{k-1} from equation (a) of algorithm 1

5. IMAGE AUTHENTICATION AND IMAGE REPAIRING

5.1 Image Authentication

In this proposed scheme, The Stego image I' is generated which is present in PNG format from the simple document type color image I with an alpha channel plane. The alpha channel is used for carrying the data, which is used at the time of authentication and data repairing. PNG image is generated with passing the alpha channel to binary color document type image. Then embed the shares, which are generated by the secret sharing algorithm into document type PNG image. After embedding the shares into an image this is called as Stego image I'.

In this algorithm we give input as the stego image I' with threshold value k and the output is tampered image I_t, with

tampered block marked. The following block diagram shows the authentication process. After giving input as a stego image, extract the shares from alpha channel plane then applying the reverse secret sharing algorithm for extracting data for authentication. At the same time binarized the given image and compute the authentication data from current block of image. Then compare extracted authentication data from alpha channel and computational authentication data, if match is occurred then image is authentic and match not occurred then marked as a tampered image and then repairing this block of an image.

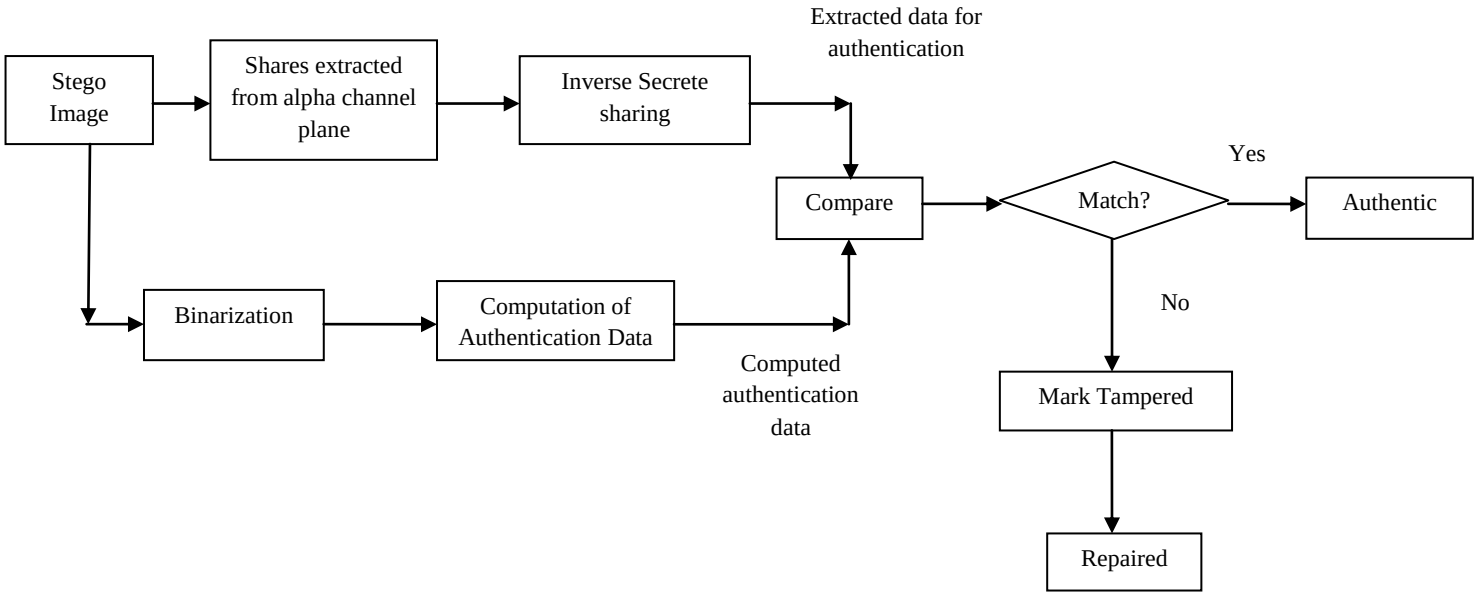


Fig 2: Authentication process for document type color image in PNG format

Algorithm3: Stego image generation in PNG format

Step1: Authentication signal generation

a. Convert the color image into grayscale image using following formula
(Red×0.1) + (Green×0.3) + (Blue×0.6)

b. Binaries the grayscale image
For image binarization apply the moment preservating threshold method [10]. So for that first draw the histogram for grayscale image and from that calculating the value of g1 and g2, apply the formula T= (g1+g2)/2, and using this Formula binarized the image i.e. I_b with value 0 for g1 and 1 for g2.

c. Apply raster grid method on whole image with 2×3 block

d. Generation of authentication signal
Authentication signal of 2 bit length i.e. S=a1a2 as $a1=p_1 \wedge p_2 \wedge p_3$ and $a2=p_4 \wedge p_5 \wedge p_6$

Step2: Creation of the data for secret sharing algorithm

a. First take the 8bit string contains the authentication signals a1, a2 and pixels p_1,p_2,p_3,p_4,p_5,p_6

b. Divide the 8 bit strings into two 4 bit strings i.e.

$m1=a1a2p_1p_2$ and $m2=p_3p_4p_5p_6$

c. Calculating m1 and m2 and consider m1 as a data d and m2 as a coefficient c (m1=d and m2=c)
$m1= 1\times p_2+2\times p_1+4\times a1+8\times a2$

$m2= 1\times p_6+2\times p_5+4\times p_4+8\times p_3$

(The number 1, 2, 4 and 8 are the binary position of the bits)

Step3: Generation the partial shares

Give input p, coefficient c_i, real values x_i and data d to algorithm 1. Using the following formula generates the six partial Shares q_1 to q_6

$q_i = F(x_i)=(d+c_1x_i)_{modp}$ where i=1,2,...,6

Step4: Calculate min transparency value using following formula

Minimum transparency value= 255-p as p=17, so the value 238 i.e. add this 238 to each shares i.e. q_1 to q_6 and resulting

the new values q_1'to q_6' mapping transparency into the range of 238 to 254 of alpha channel.

Step5: Embed two shares into current block of image into first two position

Step6: Embed remaining shares in any pixel position into image.

Step7: performing all above steps on each block of image if any block is remaining then perform step1c to step6 otherwise consider final image as a stego image I'.

The figure 3 shows the details of above algorithm i.e. two shares embedded at the current block and remaining four shares are placed at random into image.

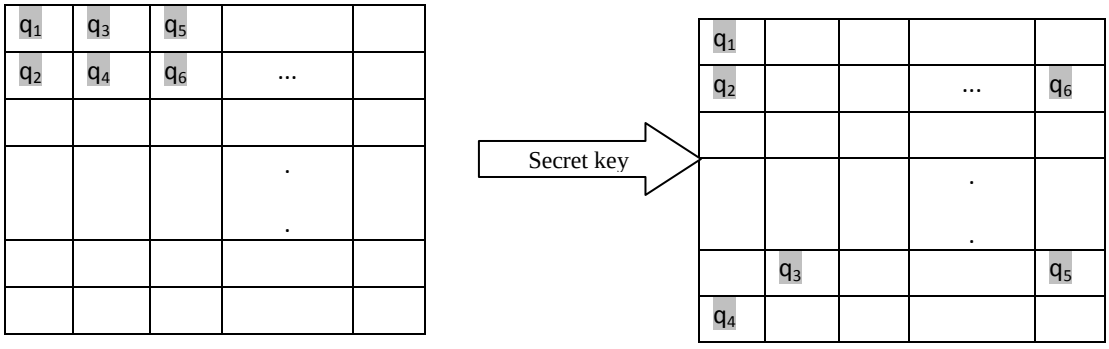


Fig 3: Embedding six shares in block of image. Two at first two positions in current block and remaining four shares are placed randomly in an image

Step3: Extract the authentication signal which is hidden in a stego image I' i.e. S' =a1a2. So for extracting the authentication signal the following steps are performed

a. Extract q_1' and q_2' from the stego image I'

b. Substract 238 from q_1' and q_2' for getting q_1 and q_2

c. Gives input as a share q_1 and q_2 to secret recovery algorithm and extract secret data d and coefficient c as an output

d. Using these secret data d and coefficient c compute the authentication signals S'=a1a2

Step4: Extract authentication signals from current block of an image i.e. a1' and a2' with pixel value p_1 through p_6 i.e. S=a1'a2' a1'=p_1^p_2^p_3 and a2'=p_3^p_4^p_5

Step5: Match the hidden authentication signal with computed authentication signal i.e. a1=a1' and a2=a2' and if match is not found i.e. a1≠a1' and a2≠a2' then marked as image is tampered i.e. I_t'.

Step5: apply all steps on whole image and if any block is remaining then go to step2.

5.2 Image Repairing

After applying authentication algorithm to a stego image, if any tampered blocks present in a stego image I' then self repairing is applied for repairing the content of an image. So input to the algorithm is stego tampered image I_t' and get output as repaired image I_r.

Algorithm4: Authentication of stego image

Step1: Binarized the stego image I_b'

Using the moment threshold preservating technique binarized the stego image I_b'. Threshold value T= (g1+g2)/2 as g1 represent 0 and g2 represent 1.

Step2: Apply Raster grid method

Take block size of image 2×3 and applying the raster grid method to whole image.

Algorithm5: Self repairing of image

Step1: Extract the shares

Extract the remaining shares which is placed at random position in an image. So extracting the remaining shares the following steps are performed

a. Using the threshold value k collect the pixels from the stego image i.e. q_3', q_4', q_5', and q_6'.

b. After collecting shares from stego image subtract 238 from q_3' through q_6' and we get q_3, q_4, q_5, and q_6'.

Step2: Repairing the tampered block in an image

a. After marked as a tampered block in stego image I' the following steps are performed

b. Extracting the six partial shares from image

c. Choose any two shares from six shares but ensure that these two shares are not marked as a tampered.

d. Using Algorithm2 compute the value of secret d and coefficient c of these two shares has the length of 8 bit strings s'. From this 8 bit string we take the last six bit from string s' i.e. b_1', b_2',b_3',b_4',b_5',b_6'. And check their binary values for repairing the tampered pixel value i.e. p_1' through p_6' of block of image I_b' using the following

If b_i'=0 then set p_i'=g1

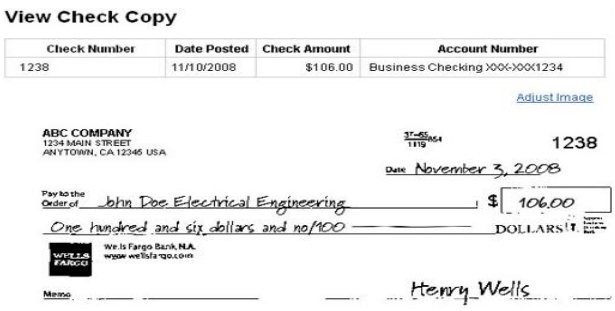
Else p_i'=g2 where i = 1, 2, ..., 6.

Step3: Finally get the repaired image I_r.

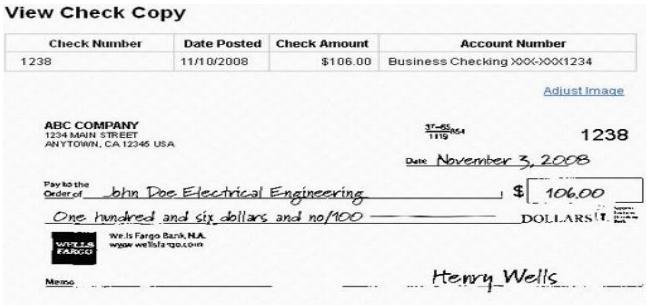
6. EXPERIMENTAL RESULTS

Experimental result of the signed image is shown in the following figure. Test1- The figure 4(a) shows the input image with the alpha channel. Alpha channel is the extra channel which is adds into the cover image for hiding the authentication signal. Figure 4(b) shows the stego image after applying the algorithm 3 to the image i.e. embed the shares into an image and forming the stego image which is visually identical to the original cover image. If any one change the content of the image using some image editing tool such as Photoshop or GIMP software and yielding the tampered image. The figure 4(c) shows tampered block as amount is changed from 10600 to 106.

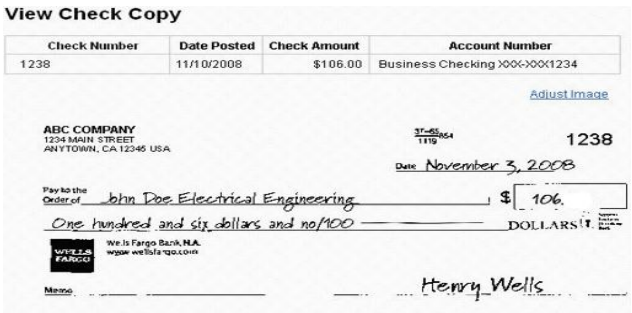
This image editing tool software used to change or modify the content of the image i.e. to destroy the image. Change the content of the alpha channel value with some new values. (Largest alpha channel value of the proposed method is 254). Figure 4(d) shows the authenticated image after applying the algorithm 4. If any tampered block present in the image then using the authentication algorithm the tampered block is detected. As in the following figure 4(c) amount is changed so using authentication process the tampered block is detected and marked with the red rectangles which shows in fig 4(d). The content of the image is repaired and get repaired image with amount 10600 which shows in figure 4(e).



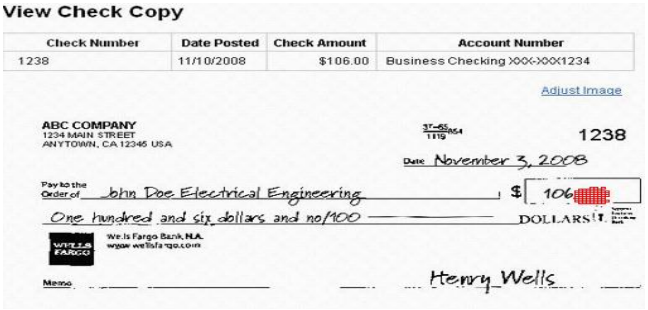
4(a)



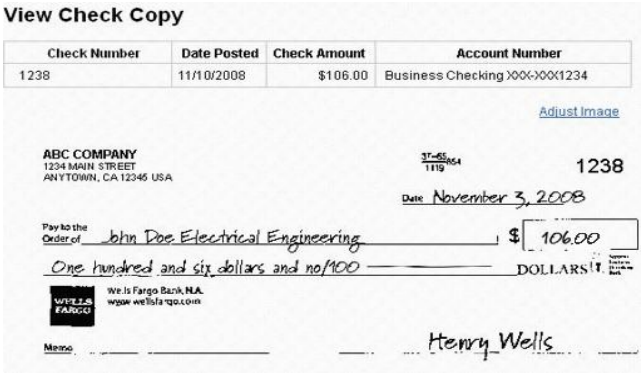
4(b)



4(c)



4(d)



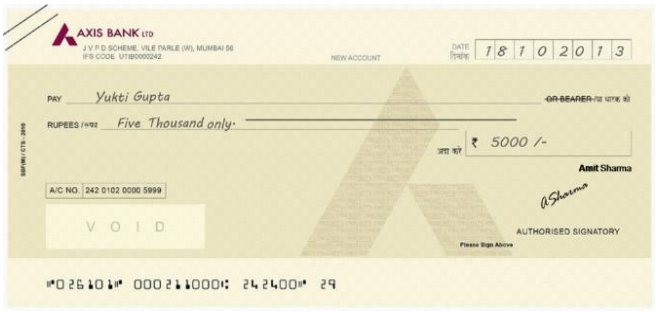
4(e)

Fig4: Test1-Authentication result of the document type color image of check copy after attacked by painting using white color (a) cover image after adding alpha channel (b) Stego image i.e. embedding the shares into an image (c) Tampered image i.e. the content of the image is changed (d) authenticated image shows the tampered block with red rectangular block (e) repaired image

Test2- Figure 5(a) shows the image with alpha channel of DD of axis bank with name Yukti Gupta with amount Rs 5000/- and account number 242 0102 0000 5999 and DD number 026101 000211000 242400 29. 5(b) stego image of axis bank DD. 5(c) shows Tampered image with change of content of image which shows in figure. 5(d) shows the authenticated image with red rectangular block shows the tampered region of image and figure 5(e) shows the repaired image with repaired content of image.

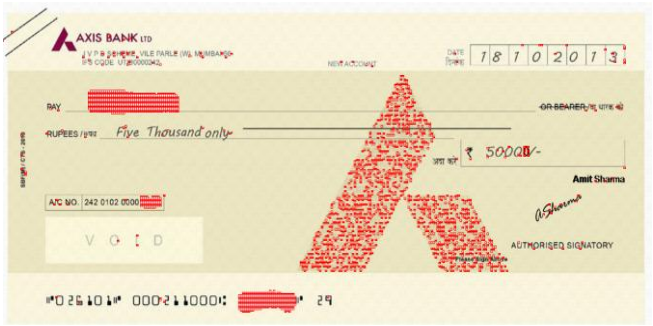
The following table 1 shows the statistics of the experimental result of document type images in terms of the following parameters i.e. the no. Of tampered blocks present in an image, Authentication result, % of authentication, No. Of repaired block and % of repaired block. In test1 the image of size 519*339 having the total blocks 29237 and tampered block 339 after authentication authenticated tampered blocks are 68 and after self repairing the repaired blocks are 68 so total 100% repairing is done. In test2 take the image of size 1024*454 having the total 77407 blocks and 4921 tampered blocks. After authentication authenticated tampered blocks are 2680 after repairing 2670 blocks are repaired so Total 99.70% results of repairing.

5(a)



5(b)

5(c)



5(d)

5(e)

Fig5: Test2- Authentication result of the document image of DD of Axis bank (a) cover image after adding alpha channel (b) Stego image i.e. embedding the shares into an image (c) Tampered image i.e. the content of the image is changed (d) authenticated image shows the tampered block with red rectangular block (e) repaired image.

Table 1. Statistics of Experimental Result of Documents Type Images

Sr. No.	Image Size (width * height)	No. of Blocks	No. of Tampered Blocks	%Tampered Blocks	Authentication Result	Authenticated Tampered Block	% of Authentication	No. of Repaired Block	% of Repaired Block
Test1	519*339	29237	336	1.149	Yes	68	20.239	68	100.00
Test 2	1024*454	77407	4921	6.357	Yes	2680	54.460	2670	99.70

7. CONCLUSION

An effective authentication method for document type color images with self data repair capabilities for document type color image based on the secret sharing method has been proposed. The authentication signals a1 and a2 are generated and these authentication signals and block of image is then transformed into the process for generating the stego image The alpha channel plane is used to hide the authentication signals and create the stego image in a form of the PNG format. The maximum alpha channel value is used in that proposed system is 255. So the share embedding into an image and forms the stego image.

The authentication signals which are hiding into the alpha channel plane are used to find out the tampered block which is present in an image. At the process of the authentication the authentication signals are computed from the image and signals are extracted from the alpha channel of an image. If the computed authentication signal are not match to that of extracted partial shares. Then considering the particular block of image is tampered. And after tampered block is detected the Self repairing capability is provided to repair original content of the block of image. The above table of experimental results, which shows the effectiveness of the authentication method for the document type of color images and the repair capability.

8. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] Meng Guo, Hongbin Zhang, "High capacity data hiding for binary image authentication," International Conference on System Science and Engineering (ICSSE) 2010.

[5] 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.

[6] 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.

[7] Min Wu, Bede Liu,"Data Hiding in Binary Image for Authentication and Annotation," IEEE TRANSACTIONS ON MULTIMEDIA, Vol. 6, No. 4, August2004.

[8] Min Wu and Bede Liu," Data Hiding in Image and Video: Part II—Designs and Applications," IEEE TRANSACTIONS ON IMAGE PROCESSING, vol.12, No. 6, June 2003

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

[10] W. H. Tasai, "Moment preserving thresholding: A new Approach", comput.vis.Graph. Image Proccss, vol. 29, pp. 377-393, Mar1985.

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

[12] H. Y. Kim and A. A?f, "Secure authentication watermarking for halftone and binary images," Int. J. Imag. Syst. Technol., vol. 14, no. 4, pp. 147–152, 2004.

[13] 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.

[14] W. H. Tasai, "Moment preserving thresholding: A new Approach", comput.vis.Graph, Image Proccssing, vol. 29, pp.377-393, Mar1985.

[15] 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.