IMAGE AUTHENTICATION FOR PNG AND JPEG IMAGES WITH DATA REPAIR CAPABILITY

Mr.K.M.Aldar[1], Prof.A.N.Mulla[2]

[1,2] *Department of CSE, ADCET, Ashta, Sangli, Maharashtra, (India)*

ABSTRACT

A blind authentication method is used to ensure the integrity and the authenticity of gray-scale document images. An authentication signal in the form secret image is embedded in alpha plane of target stego image without any noticeable distortion for JPEG images it is embedded in $C_b$and C_r planes. For generation of authentication signal binary version of target image is used. This authentication signal is transformed into several shares using the Shamir scheme for keeping by participants, and when some of the shares,not necessarily all of them, are collected, the secret message can be lossless recovered. The image authentication process marks current block as modified block if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane. For altered block data repairing is applied by reverse Shamir scheme after collecting two shares from unmarked blocks.

***Keywords:** Data Hiding, Data Repair Image Authentication, Secret Sharing and Self-Repairing Ability.*

I INTRODUCTION

Digital image can be used to preserve important information such as important certicates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Image transmission is a major activity in today's communication. Digital images are now widely distributed via the inter-net and various public channels. With the advance of digital technologies; it is now easy to modify digital images without causing noticeable changes, resulting possibly in tampering of transmitted images. It is desirable to design effective method for image authentication, aiming to check the fidelity and integrity of received images. There is an urgent need for copyright protection against the unauthorized data reproduction. In image authentication of documents whose security must be ensured it is important to ensure the integrity and the authenticity of digital images. It is also desirable to have ability to verify if the part of image is changed and to repair the damaged parts if possible.

Most prior works on data hiding and watermarking focus on gray scale images in which the pixel takes a wide range of values, slightly perturbing the pixel value by a small amount causes noperceptible distortions. This authentication problem is difficult for binary images because of their simple binary nature. Embedding of authentication signals into binary images will cause destruction of image contents, and so arouses possible suspect from invaders. Therefore, a good solution should take into consideration not only the security issue of reducing the possibility of being tampered with imperceptions but also the effectiveness of reducing image

distortion resulting from authentication signal embedding. Binary-like document images content two major gray values one close to binary zero and one close to binary one. In this paper, an authentication method that deals with half-tone grayscale document images is considered that is capable of adding secrete data for authentication without any perceptible distortion as well as ability to repair tampered image parts.

II RELEVANCE/MOTIVATION

The problem encountered in the image authentication and the self-repairing capability for the original image data under possible at-tack are summarized as below

(1) The original data of the cover image are embedded into the image itself for use in later data repairing, the cover image is destroyed in the first place and the original data are no longer available for data repairing, resulting in a contradiction.

(2) The data to be embedded in the carrier are often large sized resulting in distortion of original image.

(3) Conventionally, the concepts of secret sharing and data hiding for image authentication are two irrelevant issues in the domain of information security.

To overcome above mentioned problems a system is used which utilizes the extra alpha channel and $C_b$and $C_r$planesin a image to embed the original binary like gray scale image content data and authentication signals and also secret shares to help repair tampered data.

III LITERATURE REVIEW

Recently Che-Wei, Lee have proposed image authentication and fidelity for binary like grayscale images by embedding authentication signal and repairing data into alpha component of PNG images[14].Wu and Liu manipulated the so-called flippable pixels to create specific relationships to embed data for authentication and annotation of binary images[4]. H. Yang and Kot proposed a two-layer binary image authentication method in which one layer isused for checking the image fidelity and the other for checking image integrity [5]. Yang and Kot [6] proposed a pattern-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 embeddable blocks to deal with the uneven embeddability condition in the host image. In H. Yang and A. C. Kot, a set of pseudo-random pixels in a binary or half tone image are chosen and cleared, and authentication codes are accordingly computed and inserted into selected random pixels [7]. In Tzeng and Tsais method, randomly generated authentication codes are embedded into image blocks for use in image authentication, and a so-called code holder is used to reduce image distortion resulting from data embedding [8]. Lee et al. proposed a Hamming-code-based data embedding method that flips one pixel in each binary image block for embedding a watermark, yielding small distortions and low false negative rates [9]. Lee et al. improved the method later by using an edge line similarity measure to select flippable pixels for the purpose of reducing the distortion [10].

IV IMAGE AUTHENTICATION AND DATA REPAIRING

Authentication of any digital type documents has the great interest due to their wide application areas. Important documents such as fax document, insurance copy and personal documents in the digitized form and stored. The powerful image editing software tools are available with which copying and editing an image has become quite easy. Hence it is important to ensure the authenticity and integrity of the documents.

The used method assumes that the input cover image is a binary-like gray scale image with two major gray values. The cover image is transformed into a stego image with an supplementary alpha channel for transmission on networks or archiving in databases. The stego image, when received or retrieved, may be verified by the technique for its authenticity. Integrity modifications of the stego image can be detected by the method at the block level and repaired at the pixel level. In case that the alpha channel is totally re-moved from the stego-image, the intact resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The used method is based on the so-called (k, n)-threshold secret sharing scheme proposed by Shamir in which a secret message is transformed into n shares for keeping by n participants; and when k of the n shares, not necessarily all of them, are collected, the secret message can be recovered without any loss. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss. Main steps in the used method

(1) Take as input binary-type gray scale document image.
(2) Add an alpha channel plane with all values initially set to 255.
(3) Binarize the gray scale channel plane of the original image.
(4) Data for authentication and repairing are then computed from binary image and taken as input to the Shamir secret sharing scheme to generate secret shares.
(5) The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect.
(6) Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair capabilities.

Two block diagrams describing the used method are shown in Figs. 1 and 2.

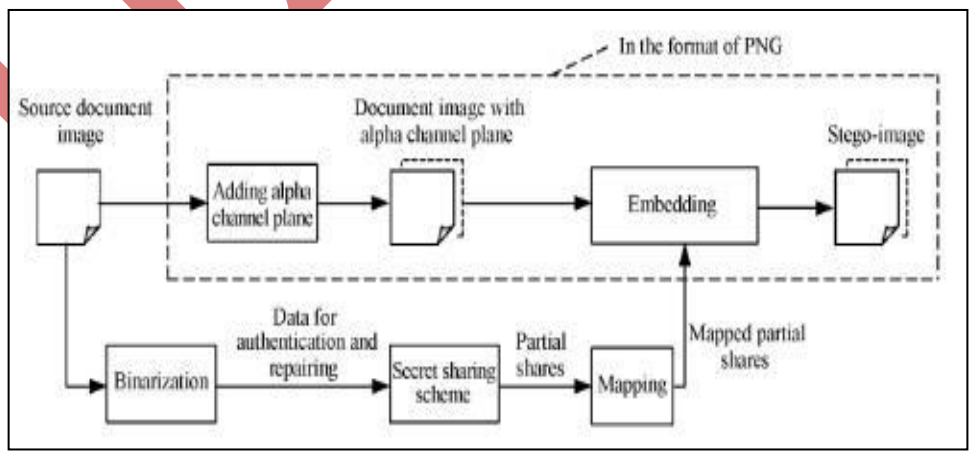

Figure 1.Generation of Stego Image.

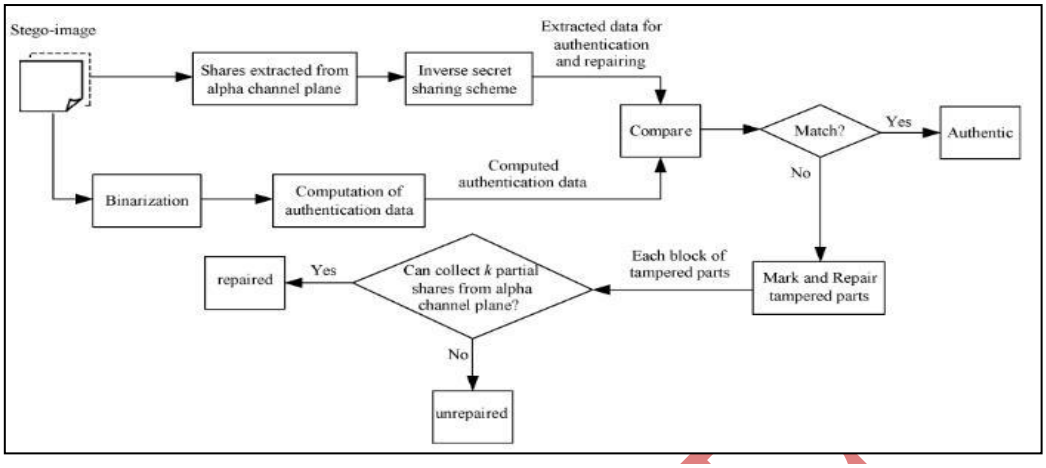

Figure 2: Authentication and data recovery from possibly attacked stego image.

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. In contrast, conentional image authentication methods often sacrifice part image contents, such as least significant bits (LSBs) or flippable pixels, to accommodate data used for authentication. In addition, once a stego-image generated from a conventional method such as an LSB-based one is unintentionally compressed by lossy compression method, the stego-image might cause false positive alarms in the authentication system. In contrast, the used method yields a stego-image in the PNG format, which, normal cases, will not be further compressed, reducing the possibility of erroneous authentication caused by imposing undesired compression operations on the stego-image.

4.1 Algorithm for (k, n)-threshold secret sharing

Shamir [11] have proposed secrete sharing method for n participants. The algorithm is given below

Input: secret d in the form of an integer, number n of shares, and threshold k <= n.

Output: n shares in the form of integers for the n participants to keep.

This module uses Shamir secret sharing scheme which allows the original secret message d to be divided in to n shares to be kept by n participants and as long as k of the n shares are available the original secret message d can be recovered where k<= n .This method is called (k, n)-threshold secret sharing because minimum k shares out of n shares are required in order to recover original message d.

(1) Choose randomly a prime number p that is larger than d.

(2) Select k-1 integer values $c_1, c_2, c_3, \ldots\ldots, c_{k-1}$ within the range of 0 through p-1.

(3) Select n distinct real values $x_1, x_2, x_3, \ldots\ldots, x_n$.

(4) Use the following k-1 degree polynomial to compute n function values $F(x_i)$, called partial shares for i=1,2,3,...,n. i.e.,

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + \ldots\ldots\ldots + c_{k1} x_i^{k1})_{\text{mod}p} \qquad (1)$$

4.2 Algorithm for Secret recovery

Input: k shares collected from the participants and the prime number p with both k and p being those used in module 1.

Output: secret hidden in the shares and coefficients used in (1) in Algorithm 1, where i=1,2,3,..,k-1.

(1) Use the k shares $(x_1, F(x_1))$; $(x_2, F(x_2))$,……, $(x_k, F(x_k))$ to set up

$$F(x_j) = (d + c_1 x_j + c_2 x^2_j + \ldots\ldots + c_{k1} x^{k\,1}_j)_{modp} \quad (2)$$

where j=1,2,...,k.

(2) Solve the equation (2) by Lagrange interpolation to obtain d.

In equation (1) there are k coefficients we need at least k shares from the n participants to form equations of the form of (1) to solve these coefficients in order to recover secret . This explains the term threshold for and the name (k,n)threshold for the Shamir method.

4.3 Algorithm for Generation of a Stego-Image

A brief overview of algorithm [14] describing generation of a stego image is presented below.

Input: a grayscale document image I with two major gray values and a secret key K.

Output: stego-image in the PNG format with relevant data embedded, including the authentication signals and the data used for repairing.

A. Algorithm for Generation of a Stego-Image

Stage I:Generation of authentication signals.

In this stage input image binarization is performed by applying moment-preserving thresholding.Then the cover image I is transformed into the PNG format with an alpha channel plane I by creating a new image layer with 100 % opacity and no color as I.Then from each 2 x 3 block of image I generate 2 bit signals for authentication and repairing.

Stage II: Creation and embedding of shares.

Data for authentication and repairing computed is taken as input to the Shamir secret sharing scheme to generate secret shares. The share values are subsequently mapped into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Finally, the mapped secret shares are randomly embedded into the alpha channel for the purpose of promoting the security protection and data repair capabilities.

4.4 Algorithm for Stego-Image Authentication

A brief overview of algorithm describing the stego-image authentication process [14], including both the verification and the self-repairing of the original image content, is presented below.

Algorithm: Authentication of a given stegoimage.

Input: stego-image I_1 and the secret key K used in Algorithm for generation of stego image.

Output: image with tampered blocks marked and their data re-paired if possible.

Gray scale plane of given stego image is binarized and then authentication signals are computed from this binarized version and are compared with extracted data for authentication and repairing from alpha channel plane of given stegoimage. If match is found mark the block as authentic else mark block as a tampered and apply the secret recovery algorithm for data recovery

. **Table 1**

Experimental result	Number of blocks	Number of tampered blocks	Number of detected blocks	Number of repaired blocks	False acceptance ratio	False rejection ratio
Experiment shown in fig 4	28666	23104	23104	23104	0 %	0 %
Experiment shown in fig 5	28666	1525	1525	1525	0 %	0 %
Experiment shown in fig 6	28666	7088	7088	7088	0 %	0 %

V DISCUSSIONS

5.1 Key Features of the Method

(1) With two untampered partial shares tampered block can be re-paired at the pixel level.

(2) The method can survive malicious attacks of common con-tent modifications, such as superimposition, painting, etc., as will be demonstrated by experimental results subsequently de-scribed.

(3) Many other methods use LSBs as the carriers of hidden data while this method uses alpha plane as the carriers of hidden data.

(4) Other methods cause destruction to the image content to a certain extent as hidden data is embedded in original image gray scale channel. This method uses the alpha channel plane and hence no distortion to the original image.

5.2 Measures for Security Enhancement

(1) The secret key, which is used to randomize the pixel positions for embedding the mapped partial shares provides a measure to protect the shares.

(2) To enhance further the security of the data embedded in the stego-image, the constant values of x_1 to x_6 used in algorithm for generation of a stego-image are randomized.

VI EXPERIMENTAL RESULTS AND COMPARISON WITH OTHER METHODS

Table 1 and 2 includes the statistics of the performance of the used method shown by the above experimental results in terms of the five parameters, i.e., tampering, detection, repair, false- acceptance, and false-rejection ratios, which are defined in the following:

(1) tampering ratio= (the number of tampered blocks)/(the total number of blocks);

(2) detection ratio= (the number of detected blocks)/(the number of tampered blocks);

(3) repair ratio= (the number of repaired blocks)/(the number of detected blocks);

Table 2

Experimental result	Number of blocks	Number of tampered blocks	Number of detected blocks	Number of repaired blocks	False acceptance ratio	False rejection ratio
Experiment shown in fig 7	28666	1735	1735	1735	0 %	0 %
Experiment shown in fig 8	28666	20460	20460	20460	0 %	0 %

Table 3

	Distortion in Stego image	Tampering Localization capability	Repair capability	Authentication Precision	Distribution Of Authenticated Image parts	Manipulation Of data embedding
Wu and Liu[4]	Yes	No	No	Macroblock	Non-Blank Part	Pixel Flippability
Young & Kot[5]	Yes	Yes	No	33 X 33 Block	Non-Blank Part	Pixel flippability
Young & Kot[6]	Yes	No	No	Macroblock	Non-Blank Part	Pixel flippability
Tzeng &sai[7]	Yes	Yes	No	64 X64 block	Entire image	Pixel Replacement
Che-Wei Lee & Wen-Hsiang Tsai[1]	No	Yes	Yes	2X3 block	Entire image	Alphachannel PixelReplacement

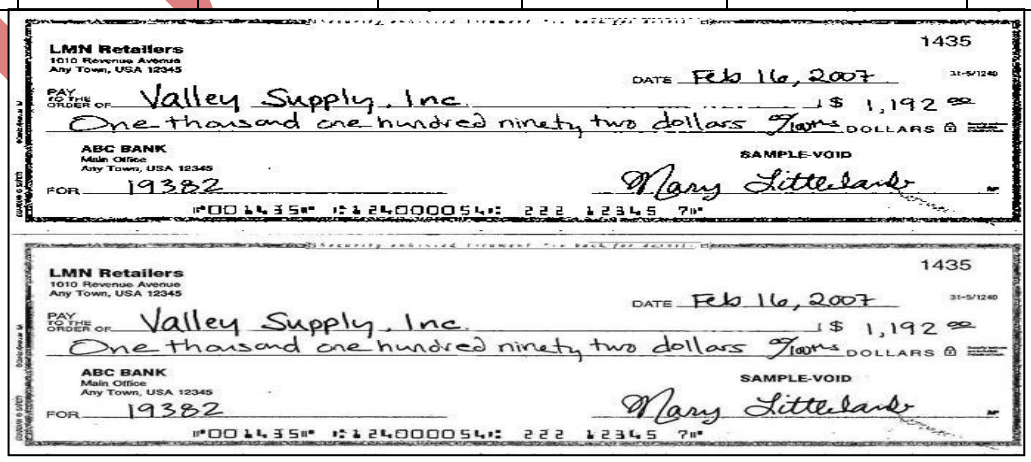

Figure 3: Experimental result of a document image of a signed paper. Original cover image (first image) and stego-image with embedded data(second image).

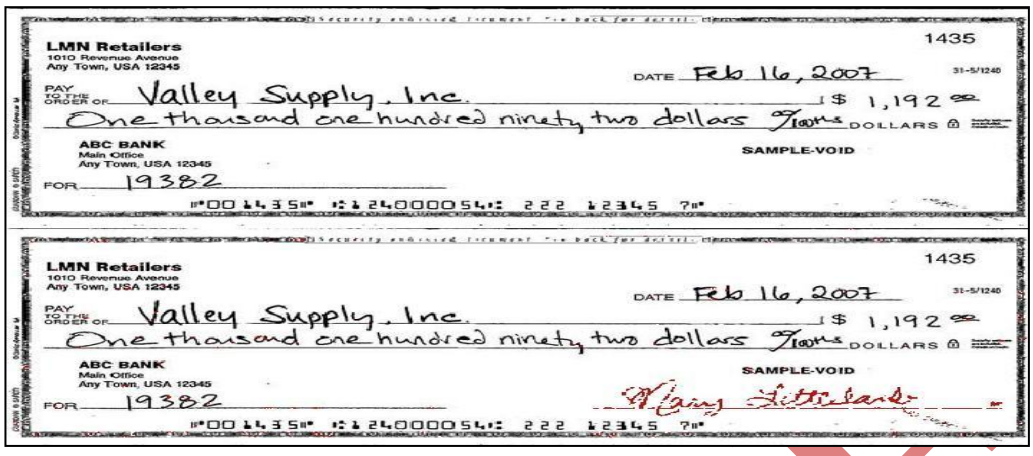

Figure 4:Authentication result of a document image of a signed paper at-tacked by superimposing a white rectangular shape on the signature. At-tacked stegoimage (first image) and repaired stego-image with recovered pixels marked as red(second image)

(4) false-acceptance ratio= (the number of tampered blocks marked as untampered)/(the total number of tampered blocks);

(5) false-rejection ratio= (the number of untampered blocks marked as tampered)/(the total number of untampered blocks).

The detection ratios are all 100% due to the ease of detection of the alpha channel values of 255 at image parts attacked by superimposing. The alpha channel value corresponding to an intact block will not be 255 and can be easily checked to be so, yielding a false rejection rate of 0%. The alpha channel value corresponding to a tampered block is 255, which is easy to check as well, yielding a false acceptance rate of 0 %.

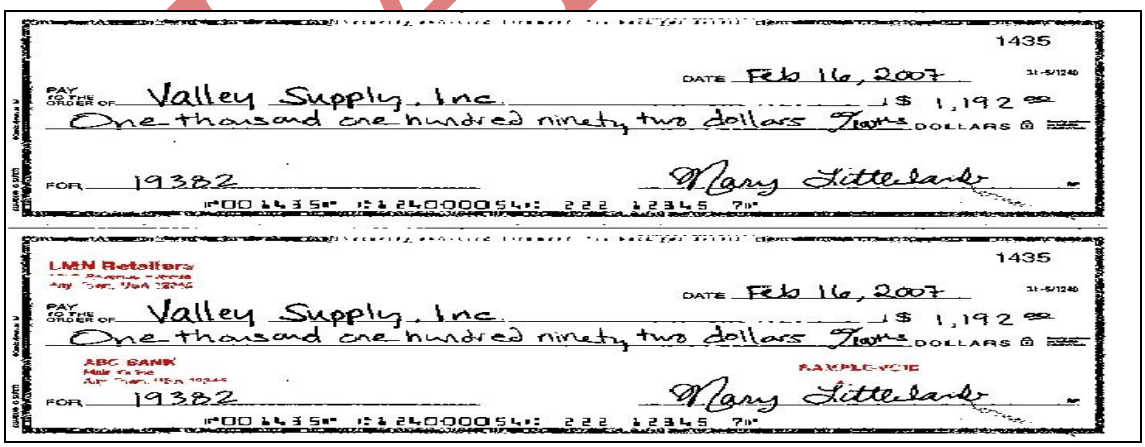

Figure 5: Authentication result of the document image of a signed paper at-tacked by superimposing a white rectangular shape on a piece of text. At-tacked stegoimage(first image) and repaired stego-image with recovered pixels marked as red(second image)

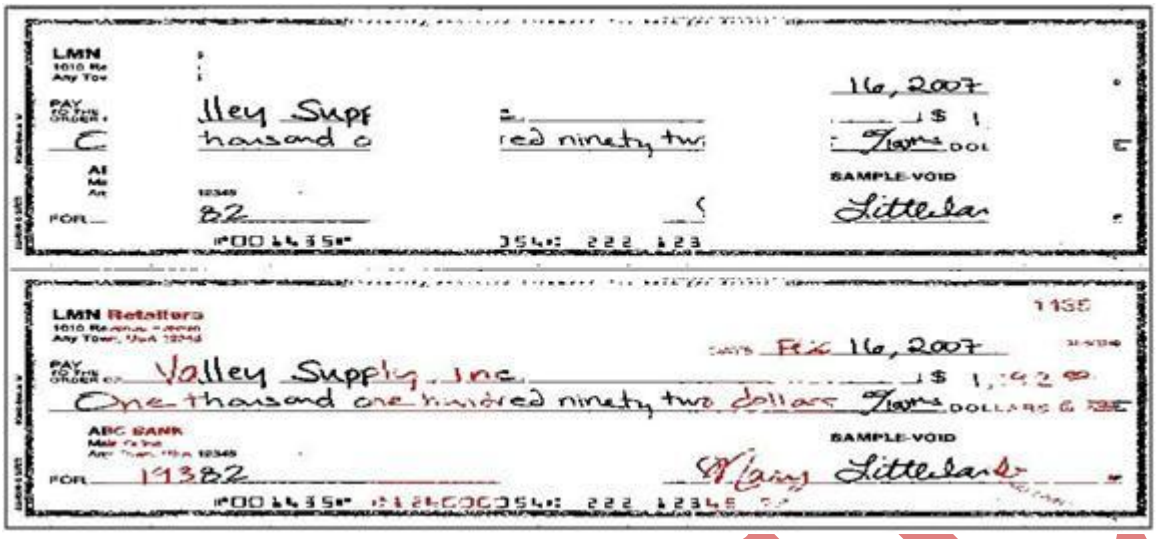

Figure 6: Authentication result of the document image of a signed paper at-tacked by superimposing white raster rectangular shapes on the content. Attacked stegoimage(first image) and repaired stego-image with recovered pixels marked as red(second image).

6.1 Experimental Results Using a Document Image of a Check

Experimental results yielded by the use of a document image of a check are shown in Fig.3, where the cover document image and the stego-image generated by the method are shown. Fig. 4 to Fig. 9 shows the result of authentication and data repairing under different types of attacks. The repaired pixels are shown in red. Also, we show the statistics of this experiment in Table 1 and Table 2.

6.2 Comparison of Performances With Other Methods

In Table 3 a comparison of the capabilities of the method with other existing methods is shown. All but the used method will create distortion in the stego-image during the authentication process. The used method has the capability of repairing the tampered parts of an authenticated image. Furthermore, among the methods with tampering localization capabilities at the block level such as [5], [8], and the pro- posed method, the used method provides a finer authentication precision with the block size of 2 x 3. Specifically, the method in [5] needs larger macro blocks to yield pixel flippabilities for embedding authentication data. In the case of using smaller blocks, Tzeng and Tsais method [8] has a high possibility to generate noise pixels, as mentioned in [6], and thus, they conducted experimental results with the larger block size of 64 x 64.

6.2 Experimental Results Using a Document Image of a Check

Experimental results yielded by the use of a document image of a check are shown in Fig.3, where the cover document image and the stego-image generated by the method are shown. Fig. 4 to Fig. 9 shows the result of authentication and data repairing under different types of attacks.The repaired pixels are shown in red. Also, we show the statistics of this experiment in Table 1 and Table 2.

6.2 Comparison of Performances with Other Methods

In Table 3 a comparison of the capabilities of the method with other existing methods is shown. All but the used method will create distortion in the stego-image during the authentication process. The used method has the

capability of repairing the tampered parts of an authenticated image. Furthermore, among the methods with tampering localization capabilities at the block level such as [5], [8], and the pro- posed method, the used method provides a finer authentication precision with the block size of 2 x 3. Specifically, the method in [5] needs larger macro blocks to yield pixel flippabilities for embedding authentication data. In the case of using smaller blocks, Tzeng and Tsais method [8] has a high possibility to generate noise pixels, as mentioned in [6], and thus, they conducted experimental results with the larger block size of 64 x 64.

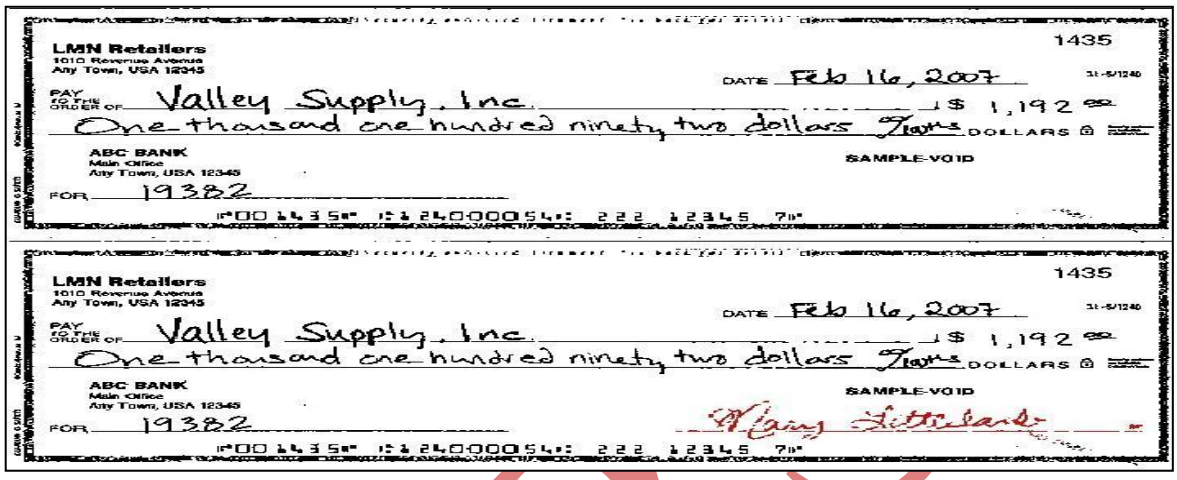

Figure 7:Authentication result of the document image of a signed paper attacked by painting white color on the original signature.Attackedstego image(first image) and repaired stego-image with recovered pixels marked as red(second image).

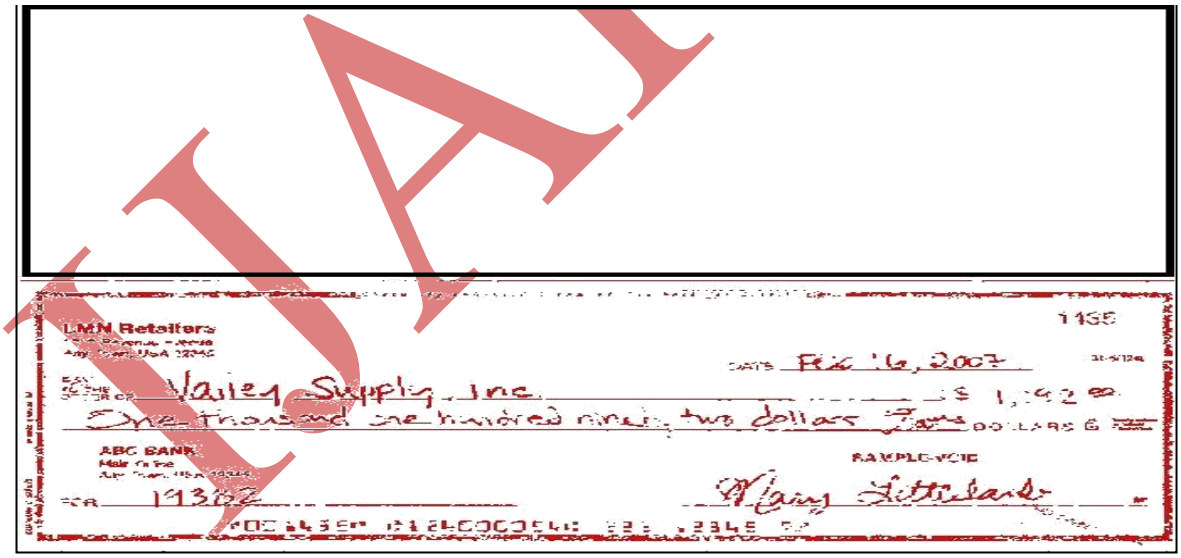

Figure 8:Authentication result of the document image of a signed paper at-tacked by painting white color on the entire content. Attacked stego-image(first image) and repaired stego-image with recovered pixels marked as red(second image).

As to the distribution of authenticated image parts, because there exists no flippable pixel for use by the methods of [4][6] to embed data in all-white regions (such as marginal regions) of a document image, the distribution of authenticated image parts tends to be restricted to be on lines or strokes in the document, whereas

the used method does not have this limitation. Nevertheless, in [4][6], the authenticity of an image part including such all-white regions canbe still ensured by the use of cryptographic signatures embedded in other regions of the image. At last, the methods of [4][6] manipulate pixel flippability, and the method of [8] enforces pixel re-placement for the aim of data embedding. The used method is the only one that makes use of the alpha channel plane instead of the bit plane.

VII CONCLUSION

The generated authentication signal and the content of a block have been transformed into partial shares by the Shamir method, which have been then distributed in a well-designed manner into an alpha channel plane to create a stego-image. 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, a block in the stego image has been regarded as having been tampered with if the computed authentication signal does not match that extracted from corresponding partial shares in the alpha channel plane. For the self-repairing of the content of a tampered block, the reverse Shamir scheme has been used to compute the original content of the block from any two untampered shares. Measures for enhancing the security of the data embedded in the alpha channel plane have been also used. Experimental results have been shown to prove the effectiveness of the used method.

REFERENCES

[1]. S. Lu and H. Y. M. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Trans. Image Process., vol. 10, no. 10, pp. 15791592, Oct. 2001.

[2]. M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, “Hierarchical watermarking for secure image authentication with localization,” IEEE Trans. Image Process., vol. 11, no. 6, pp. 585595, Jun. 2002.

[3]. 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. 822831, Jun. 2005.

[4]. M. Wu and B. Liu, “Data hiding in binary images for authentication and annotation,” IEEE Trans. Multimedia,vol. 6, no. 4, 528538, Aug. 2004.

[5]. H. Yang and A. C. Kot, “Binary image authentication with tampering localization by embedding cryptographic signature and block identier,” IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741744, Dec.2006.

[6]. H. Yang and A. C. Kot, “Pattern-based data hiding for bi-nary images authentication by connectivity-preserving,” IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475486, Apr. 2007.

[7]. H. Y. Kim , “ Secure authentication watermarking for halftone and binary images,” Int. J. Imag. Syst. Technol., vol. 14, no. 4, 147152, 2004.

[8]. 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. 443445, Sep. 2003.

[9]. Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, “A new bi-nary image authentication scheme with small

distortion and low false negative rates," IEICE Trans. Commun.,vol. E90-B, no. 11, pp. 32593262, Nov. 2007.

[10]. 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. 38663884, Nov. 2009.

[11]. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612613, Nov. 1979.

[12]. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," IEEE Signal Process. Lett.vol. 73, no. 3, pp. 405414, Nov./Dec. 2004.

[13]. H. Yang and A. C. Kot, "Moment-preserving thresholding: A new approach," Comput. Vis. Graph. Image Process., vol. 29, no. 3, pp. 377393,Mar. 1985.

[14]. 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 transactions on image processing, vol. 21, no. 1, January 2012