New Approach To Authentication And Data Repairing For Document Image

Miss. Aparna Dhone, Prof. P. S. Mohod
G. H. Raisoni College for Engineering & Technology For Womens,Nagpur,India

Abstract

This paper proposed a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images .Shamir proposed threshold secret sharing scheme in which a secret message is transformed into shares for keeping by participants, and when some of the shares, not necessarily all of them, are collected, the secret message can be losslessly recovered.. This secret sharing scheme is useful for reducing the risk of incidental partial data loss. For tampered block data repairing is applied by reverse Shamir scheme. This paper also presents the security issues and discuss on keeping high quality visual effect.

1. Introduction

Authentication of digital documents has aroused great interest due to their wide application areas such as legal documents, certificates, digital books and engineering drawings. In addition, more important documents such as fax insurance and personal documents are digitized and stored. With the advance of digital technologies, it is now easy to modify digital images without causing noticeable changes, resulting possibly in illicit tampering of transmitted images. It is desirable to design effective methods to solve this kind of *image authentication* problem, particularly for images of documents whose security must be protected. Authentication and detection of tampering and forgery are thus of primary concerns. Data hiding or watermarking for binary images authentication has been a promising approach to alleviate these concerns. 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 no perceptible 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. In this paper, we propose an authentication method for binary images with good balance between the mutually conflicting goals of distortion reduction and security enhancement.

Secret sharing has broad applications in the real world and can be used for situations in which access to important resources has to be protected. There is an old story which is believed to have motivated the secret sharing principle**:** a group of pirates discovered a map that would lead all group to an island full of treasure. Then there is question arises who was going to be entrusted to keep the map? A safe solution is: the map should be divided into number of pieces such that all pieces are needed to recover the map and missing any piece would make the map totally unreadable. Thus, every pirate was given one such piece. Another important application of secret sharing is e-voting where the vote of every individual participant will be absolutely and correctly counted in the overall voting result but there is no way for other people (including candidates and authorities) to know and understand whom the individual voted for. In today's information and networking world, secret sharing is also a important issue in network security and can be used in key management and multi-party secure computation. The secret sharing scheme is developed not only to carry

authentication signals and image content data but also to help repair tampered data through the use of shares.

2. Related work

2.1 Weighted multi-secret sharing

The concept of secret sharing proposed by Shamir in 1979. Secret sharing schemes can be classified into various categories, in terms of numbers of secrets to be shared, two classes can be identified: single secret and multiple secrets. In terms of share's capabilities, two classes can be identified as well: same-weight shares and weighted shares. Weighted shares concept tell us that different shares have different capabilities in recovering the secret(s)–a more weighted share needs fewer other shares and a less weighted share required more other shares to recover the secret(s). Based on this technique two typical classes can be identified: polynomial based schemes and Chinese Remainder Theorem (CRT) based schemes.

In this, we identify a simple relation between the lengths of shares and their weights and based on this relation, a new CRT based (*w*, *N*)-threshold secret sharing scheme is proposed. Creating partial shares using following equation:

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + \ldots\ldots\ldots + c_{k-1} x_i^{k-1}) \bmod p \quad (1)$$

Where, i=1, 2, 3…n

For recovering the secret message use the following equation:

$$d = (-1)^{k-1} \left[F(x_1) \frac{(x_2 x_3 \ldots\ldots x_k)}{((x_1-x_2)(x_1-x_3)\ldots\ldots(x_1-x_k))} \right] + \left[F(x_2) \frac{(x_2 x_3 \ldots\ldots x_k)}{((x_2-x_1)(x_2-x_3)\ldots\ldots(x_2-x_k))} \right] + \ldots\ldots \left[F(x_k) \frac{(x_2 x_3 \ldots\ldots x_k)}{((x_k-x_1)(x_k-x_2)\ldots\ldots(x_k-x_{k-1}))} \right] \bmod p \quad (2)$$

Comparisons of CRT based scheme with MIGNOTTE'S scheme:

Both scheme are based on CRT and use the same operation to recover the secret. They use the same operation to generate all same weight shares. For the shares of different weights pi, the new scheme generates pi × n bit primes (or co-primes) directly. However, Mignotte's scheme generates a Mignotte sequence of *n* bits each first and then gets pi × n bit (maybe pi × n − *pi* + 1 bit) primes (or co-primes) by multiplying pi primes (or co-primes) in the Mignotte sequence. After generating primes (or co-primes), both schemes use the same modular operation to get shares. The difference in generating primes (or co-primes) affects only performance but not security features. As a result, the new scheme and Mignotte's scheme have identical security features [11].Advantage of this new scheme is simple and its implementation is straightforward. Disadvantage of this scheme affects only the performance ratio but not security features.

2.2 Pattern-Based data hiding method binary image authentication

The In this paper Huijuan Yang and Alex C. Kot, April 2007, the "uneven embeddability" of the image by embedding the watermark are proposed. Similarly the problem of locating the "embeddable" pixels has been addressed and an authentication scheme is designed to incorporate the cryptographic signature to ensure the authenticity and integrity of the image. The main objectives of this paper are as follows:

1) Assess the "flippability" of a pixel using the connectivity preserving criterion to achieve good visual quality of the watermarked image.

2) Handle the "uneven embeddability" of the image by adaptively embedding the watermark only in those "embeddable" blocks.

3) Study the invariant features in flipping pixels in binary images to achieve blind watermark extraction.

4) Explore different ways of partitioning the image to achieve larger capacity.

5) Investigate on how to locate the "embeddable" pixels in the watermarked image so as to incorporate cryptographic signature to achieve higher security [11].

In this paper, a novel blind data hiding scheme for binary images authentication based on connectivity-preserving of pixels is presented. A window of size 3 X 3 is employed to assess the "flippability" of a pixel in a block [4]. No side information is required for the watermark retrieval due to the feature of the data embedding process. The "uneven embeddability" of the input binary image is handled by embedding the watermark based on the three transition criteria. A smaller block size is chosen for increasing the data hiding capacity. The fixed 3 X 3 block, non-interlaced and interlaced block schemes are discuss and compare the capacity the capacities using different types of blocks. Different types and sizes of block can be chosen for different applications. Also address the problem of how to locate the "embeddable" pixels in a block for different block schemes, which facilitates authenticity and integrity of the image are ensured. Advantage of the proposed scheme can be applied to a wide variety of binary images authentication. Disadvantage is, the interlaced block scheme is the most time-consuming due to the largest number of blocks.

2.3 Binary image authentication with tampering localization by embedding cryptographic signature and block identifier

Author In this paper Huijuan Yang and Alex C. Kot, december 2006, proposes a novel two-layer blind binary image authentication scheme, in which the first layer is targeted at the overall authentication and the second layer is targeted at identifying the tampering locations. The "flippability" of a pixel is determined by the "connectivity-preserving" transition criterion. The image is partitioned into multiple macro-blocks that are subsequently classified into eight categories. The block identifier is defined adaptively for each class and embedded in those "qualified" and "self-detecting" macro-blocks in order to identify the tampered locations.

The overall authentication is achieved in the first layer by hiding the cryptographic signature (CS) of the image. The localization of the tampering is achieved in the second layer by embedding the block identifier (BI) in the "qualified" or "self-detecting" macro-blocks (MBs). Specifically, we group multiple overlapping 3X 3 blocks to form an MB and classify the MBs to "qualified" macro-blocks (QMBs) and "unqualified" macro-blocks (UMBs) based on the number of "flippable" pixels Nf [3].

The QMBs are chained, and the BI that is used to identify the tampering occurred both to the QMB and its neighbouring UMB is embedded. Advantage of this proposed method is effective in detecting any changes, and in the meantime, the locations being tampered can be identified. Disadvantage is the MB size should be chosen such that a good compromise can be made between the capacity required for embedding CS and the localization accuracy. Missmatch detection and the false alarm are most likely occurred if MBs that do not have enough "flippable" pixels to embed a complete BI.

3. Proposed Method

The Following methods need to study and included in this project work:

Data hiding and watermarking techniques:
The hiding and watermarking techniques for a digital media applications, including ownership protection, signature verification, copy control, annotation, and authentication.

Data Secret-sharing Scheme:
Secret sharing is important in information and network security and has broad applications in the real world area. A secret sharing scheme starts with a secret and then creates certain shares which are distributed to a group of participants. The secret may be uniquely recovered from certain predetermined groups of users which constitute the access structure. An important category of access structure is the (w, N)-threshold access structure in which, an authorized group contains any w or more participants and any group of at most $w-1$ participants is an unauthorized group. These schemes deal with either single or multiple secrets and their shares have either the same weight or different weights.

Data Embedding:
The data embedding method can be used to detect unauthorized use of a digitized signature, and annotate or authenticate binary documents.

Concept:

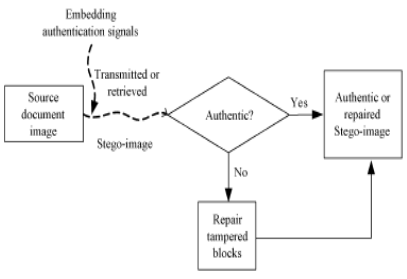


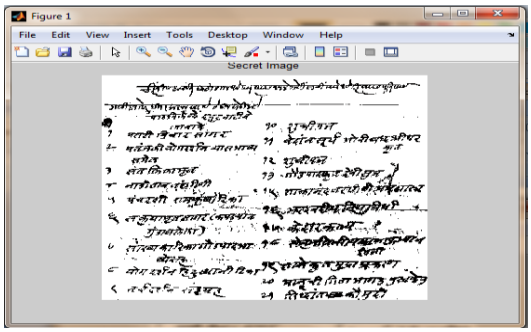
Figure 1, Framework of proposed document image authentication method [1].

The input cover image is assumed to be grayscale image .After the proposed method is applied; the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format .The stego-image is verified by the proposed method 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 [1].

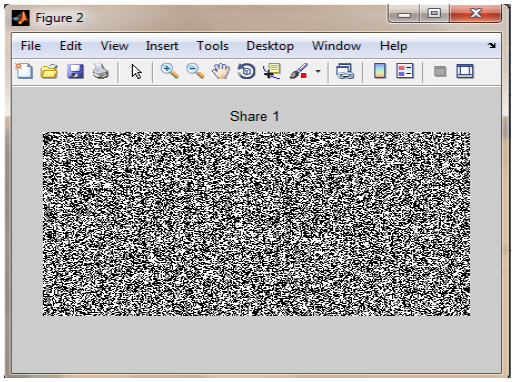
4. Experiments and results

Following first module has been implemented:

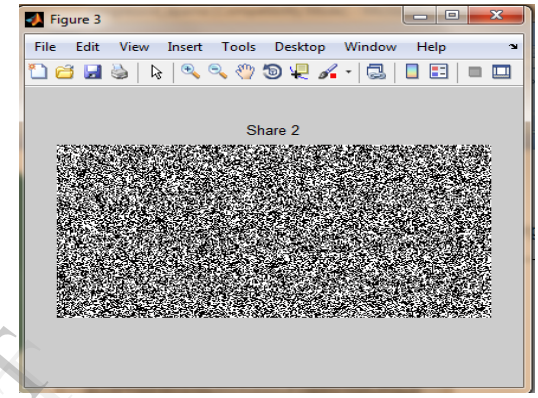
Here we creates the shares and distributed to the n participants. By collecting k number of shares we recover the secret message which is same as original document contents. These are some screen snapshots showing the result.



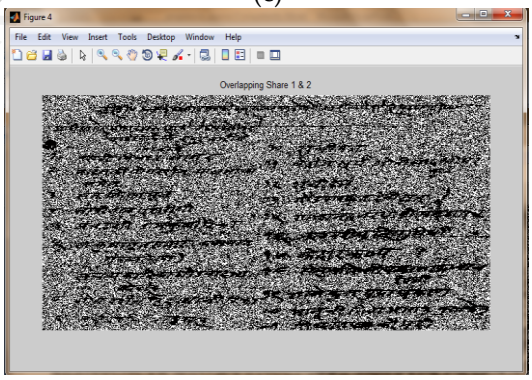
(a)



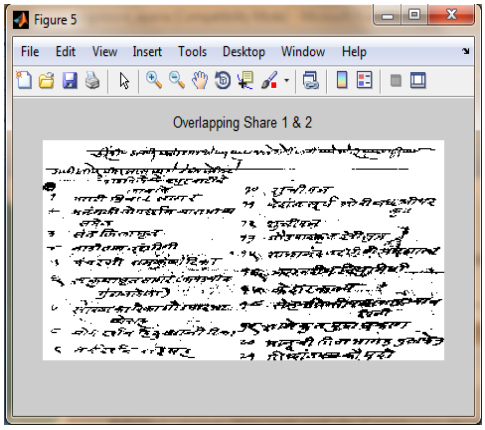
(b)



(c)



(d)



(e)

Figure 2, (a) original image, (b) creating share1 (c) creating share 2, (d) overlapping image, (e) same image come after XOR operation.

5. Conclusion

A new blind image authentication method with a data repair capability for binary grayscale document images based on secret sharing has been proposed. With the Shamir method shares are distributed in well designed manner to create stego image .For the self-repairing of the content of a tampered block, the reverse Shamir scheme has been applied to compute the original content of the block. .

6. References

[1] Che-Wei Lee,IEEE Transaction on Image processing January 2012, and Wen-Hsiang Tsai,Senior Member, IEEE "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability ".

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

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

[4] H. Yang and A. C. Kot, "Pattern-based data hiding for binary images authentication by connectivity-preserving,"*IEEE Trans. Multimedia*,vol.9,no. 3, pp. 475–486, Apr. 2007.

[5] 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.

[6] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of Binary images for multimedia communication with distortion reduction and security enhancement," *IEEE Commun. Lett.*, vol. 7, no. 9, pp.443– 445,Sep. 2003.

[7] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates, "*IEICE Trans. Commun.*, vol. E90-B, no. 11, pp. 3259–3262, Nov. 2007.

[8] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binary image authentication with small image distortion," *Inf. Sci.*, vol. 179,no. 22,pp. 3866–3884, Nov.2009.

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

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

[11] Xukai Zou, Fabio Maino, Elisa Bertino, Yan Sui, Kai Wang and Feng Li, "A New approach to Weighted Multi-Secret Sharing", 978-1-4577-0638-7,2011 IEEE.