IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VII (Mar-Apr. 2014), PP 75-79
www.iosrjournals.org

Authentication of grayscale document images using shamir secret sharing scheme.

[1]Mrs.G.Niranjana,M.Tech (Asst.prof), [2]Ms.K.Siva Shalini,M.Tech
[1]*SRM University, Chennai.*
[2]*SRM University, Chennai.*

***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 in to shares for keeping by participants, and when some of the shares, not necessarily all of them, are collected, the secret message can be lossless recovered.. This secret sharing scheme is useful for reducing the risk of incidental partial data loss. In additional image transformed in to a stego-image in the PNG format with an additional alpha channel for transmission on networks. For tampered block data repairing is applied by reverse Shamir scheme. It also presents the security issues and discuss on keeping high quality visual effect.*

***Keywords:** Data hiding, data repair, grayscale document image, image authentication, Portable Network Graphics (PNG) image, secret sharing.*

I. Introduction

Authentication of digital documents has aroused great interest due to their wide application areassuch 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 a new Blind authentication method for binary images with good balance between the mutually conflicting goals of distortion reduction and security enhancement. 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 multiparty 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. We propose a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the PNG image. We use Shamir scheme which reduce the data volume of the generated shares effectively so that more shares can be embedded in to the alpha channel plane. we distribute the multiple shares randomly into the alpha channel to allow the share data to have large chances to survive attacks and to thus promote the data repair capability. 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. The concepts of "secret sharing" and "data hiding for image authentication" are two irrelevant issues in the domain of information security.

II. Related Work

A-New Blind Authentication

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification. The authentication 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.

B-Data Secret Sharing Scheme

Secret sharing is important in information and network security 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.

C-Review Of The Shamir Method For Secret Sharing

Shamir's Secret Sharing is an algorithm in for of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Counting on all participants to combine together the secret might

Be impractical, and therefore sometimes the threshold scheme is used where any K of the parts are sufficient to reconstruct the original secret. In this scheme, any t out of n shares may be used to recover the secret. The system relies on the idea that you can fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic curve, and so on. That is it takes t points to define a polynomial of degree t-1. The method is to create a polynomial of degree t-1 with the secret as the first coefficient and the remaining coefficients picked at random. Next find n points on the curve and give one to each of the players. When at least t out of the n players reveal their points, there is sufficient information to fit a (t-1)th degree polynomial to them, the first coefficient being the secret. The essential idea of Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes K points to define a polynomial of degree K-1. Suppose we want to use a threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size o< k<=n< p where P is a prime number. Choose at random K- 1 coefficients a_1 , ---, a_{k-1} in F, and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \text{---} + a_{k-1}\, x^{k-1}$. Let us construct any n points out of it, for instance set i = 1 ---- n to retrieve (i , f(i)). Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of K of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

III. Png Image Authentication And Datahiding

In image authentication and data repairing, we create a PNG image from a binary type grayscale document image E with an alpha channel plane. Then the actual image E is converted into binary form by moment preserving threshold which is denoted as E_b. This is taken as an input to Shamir's secret sharing scheme to generate n secret shares. The mapped secret shares are embedded into alpha channel plane to produce an imperceptibility effect. Then, the mapped secret shares are embedded randomly into alpha channel plane. The PNG image crated is then encrypted by chaotic logistic map [4]. Embedded shares providing security and repairing capability, encryption gives extra security by scrambling the PNG image. It is shown in fig 1

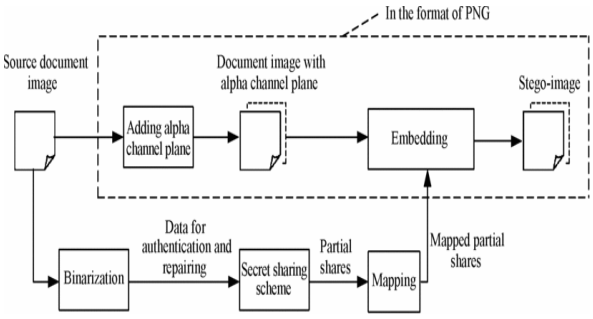

Fig. 1 Creating a PNG image from a grayscale document image and an alpha channel

IV. Stego –Image

It is the process of hiding messages inside a computerized image file, as for example hiding the name and copyright notice of the owner of an image as protection against violation of the copyright. Here we are Generating the stego Image, when received or acquired, can be verified by the proposed method for its authenticity. Integrity alterations of the stego-image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is fully removed from the stego-image, the complete resulting image is regarded as unauthentic, meaning that the fidelity check of image fails. After performing the Binarization [1] at the receiver side, the Image is to be filtered the Alpha channel. After stego image generation if there is no authentic process Repair the Tampered Image Blocks then remove the alpha channel. If the Authentication is success directly receive the PNG Image at the receiver side.

A-Algorithm For Stego-Image

A detailed algorithm for describing the generation of a stego-image in the PNG format is

Part 1: Drawing out the embedded two representative
gray values.

Step 1: (Stego-image to Binary form conversion)

Compute T = (g1 + g2)/2 and use it as a threshold t

o convert S into Binary Form, yielding the binary version S of S with ”0” representing g1 and ”1” representing g2.

Part 2: Stego-image authentication.

Step 2: (Start looping) Take in a raster-scan order

an unprocessed block B from S with pixel values p1 through p6, and. find the 6 pixel values qd1, through qd6 of the corresponding block B in the alpha channel plane S of S

Step 3: (Extraction of the secreted authentication

Signal) to extract the six bits hidden as authentication signal ad from B follow the steps:

(1) Subtract 142 from each of the untampered qd

and ad partial shares of B With the shares to obtain the 2 values d and c1 (the secret and the
Coefficient value, respectively).

(2) Now convert this d and c1 into two 4-bit binary values, and then an 8-bit string is formed by concatenating these binary values.

Step 4: (Matching the secreted and computed authentication signals and marking of tampered blocks)

Calculate the q1 to q6 values for 2 by 3 block of S

Match the new calculated q1 to q6 with old embedded (in alpha channel) q1 to q6 and if any variance occurs, mark B the corresponding block B in S , and all the partial shares embedded in B as tampered.

Step 5: (Repairing of the tampered part)

If possible using the binary values of d & c1 find Pixels p1 through p6. Check the tampered pixels then try to repair the values using the extracted binary b & c.

Put g1 if pixel value is 1 & g2 if pixel value is 1 in received S image. If sufficient i.e. 2 untampered authentication signal is available then only repairing is possible. If all the signals are tampered, repairing is not possible.

Step 6: (Exit loop)

If there is any unprocessed block in S, then go to Step 2; otherwise, go on.

V. Methodology For Secret Sharing System

A new authentication method based on the secret sharing technique along with a data repairing capability for gray scale document images via the use of PNG (portable network graphics) is proposed. An authentication signal is generated for every and each block of a gray-scale document image, which, in conjunction with the binarized block content, is remodeled into many shares exploitation the Shamir secret sharing theme. The concerned parameters are cautiously chosen in order that as several shares as potential are generated and embedded into an alpha channel plane. To form a PNG image the alpha channel plane is combined with the original gray scale image. During the embedding process, the computed share values are mapped into a range of alpha channel values near their maximum value of 255 to yield a transparent stego-image with a disguise effect. While the method of image authentication, an image block is spotted as tampered, if the authentication signal computed from the present block content doesn't match with the worth or value extracted from the shares embedded inside the alpha channel plane. For each tampered block, data repairing is applied by using reverse Shamir scheme after collecting two shares from unmarked blocks. Some security measures for protecting the security of the data hidden in the alpha channel are also proposed. It is illustrated in the fig 2.

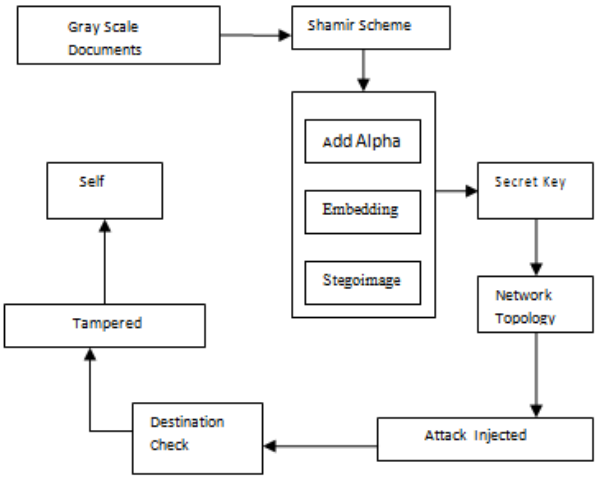

Fig. 2 Architecture for secret sharing system

VI. Vi-Evaluation

A.Data Embedding

The data embedding method can be used to detect Unauthorized use of a digitized signature, and Annotate or authenticate binary documents. 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.

B.Performance With Other Methods

Stego-Image has the capability of repairing the tampered parts of an authenticated image. 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 proposed. Experimental results have been shown to prove the effectiveness of the proposed method.

C. Image Authentication And Protection

It is very necessary to design effective methods to Solve image authentication problem, particularly For images whose security must be protected. The technique for authentication of images with self-repair capability for fixing tampered image data is explained. The input image is assumed to be a binary-type grayscale image with 2 main gray values. Alpha channel is combined in the grayscale image .Using the binary image, authentication signal is calculated which is then embedded in the alpha channel to create an authentic image. After embedding the authentication signal, image is encrypted. If still Content modifications of the stego-image is detected, then data is repaired at the pixel level using reverse secrete sharing scheme.

VII. Conclusion And Future Work

An image authentication method along with a data repair capability for binary-like grayscale images i.e. black and white based on secret sharing is explained. We have proposed a Blind authentication scheme for gray scale document images by the use of secret sharing method and alpha channel plane security is provide by using Shamir's secret sharing method. Both the generated authentication signal and the content of block have transformed into partial shares by Shamir's method which are generated into alpha channel plane to create a PNG image .Stego image is form in PNG format and from embedding the partial shares by mapping the share values. A block in stego image authentication has been tampered if computed authentication signals does not match for self repairing of tamped block the Shamir's reverse scheme is used.

References

[1] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Trans. Image Process., vol. 10,no. 10, pp. 1579–1592, Oct. 2001.

[2] M. U. Celia, 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. 585–595, 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. 822–831, Jun. 2005.

[4] 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.
[5] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifie,"IEEE Signal Process. Lett., vol. 13, no. 12, pp. 741–744, Dec.2006.
[6] 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.
[7] 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.
[8] 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.
[9] D. Gabor, "Theory of communication," J. Inst. Elect. Eng., vol. 93, pp.429–457, 1946.
[10] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Process., vol. 66, pp. 283–302, 1998.
[11] J. R. Hernandez and F. Perez-Gonzalez, "Statistical analysis of watermarking schemes for copyright protection of images," Proc. IEEE, vol.87, pp. 1142–1166, July 1999.
[12] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," in Proc. IEEE Conf. Acoust., Speech, Signal Processing, vol. 5, 1998, pp. 2969–2972.
[13] "Digital watermarking for telltale tamper proofing and authentication," Proc. IEEE, vol. 87, pp. 1167–1180, 1999.
[14] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," J. Electron. Imag., vol. 7, pp. 326332,1998.
[15] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in Proc. SPIE Multimedia Systems Applications, vol. 3528, Boston, MA,Nov. 1998, pp. 423–431