INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 4, Issue 5, September – October (2013), pp. 23-30
© IAEME: www.iaeme.com/ijcet.asp
Journal Impact Factor (2013): 6.1302 (Calculated by GISI)
www.jifactor.com

IJCET

©IAEME

A HARMONIC SECRET SHARING AND PERMUTATION BASED DOCUMENT IMAGE AUTHENTICATION

[1]Muna Ghazi, [2]Dr. Hanaa M. A. Salman

Computer Science Department, University of Technology, Iraq
Computer Science Department, University of Technology

ABSTRACT

In this paper, we are presenting blind authentication method which is based on harmonic secret sharing technique and permutation with data repair capability and error localization for document image and verification of its owner, with the use of the PNG image. We are generating a block based authentication from document image, and transform it into several shares using the Shamir secret sharing scheme, and embedding these shares into an alpha channel plane. The alpha channel plane is permuted with secret key and combined with the original image to form a PNG image. In the process of document image authentication, if the authentication signal computed from the current block content does not match the one extracted from the shares embedded in the alpha channel plane, a document image block localize as tamper block ,then a repairing process is implement else a document image block is authentic. In the repairing process a reverse Shamir technique is implementing for each tampered block after collecting any two or more shares from unmarked blocks. Also, owner verification process is implementing based on the secret key used for the permutation.

Keywords: Document Image authentication, secret sharing, Data repair, Data hiding, and PNG (Portable Network Graphics) image, Permutation, Owner verification.

1. INTRODUCTION

Important documents such as fax insurance, digital books, engineering drawings, signed document, scanned checks, and personal documents are usually digitalized and stored as an image. These digitalized document images are prone to duplicated or tamper, duo to the advance of digital and network technology, therefore, issues such as copyright protection, content authentication, tamper detection localizes and self-repair capabilities must be taken into consideration more seriously.

Steganography is defined as a technique for transmitting secret information without being noticed over non-covered channels, as depicted into Figure (1). Steganography may be used to embed a message into the document image to protect the owner's copyright of the document image or to authenticate the document images or to covered communication over insecure channels. However there is a weakness common to all steganoraphic techniques, which is, if one stego media is lost or corrupted, the secret data cannot be revealed exactly, and completely.

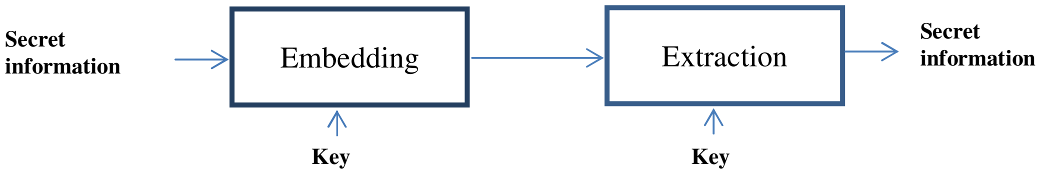

Figure 1: Block diagram of steganography

Secret Sharing Schema (SSS), which defined as "a method which distributes shares of a secret to a set of participants in such a way that only specified groups of participants can reconstruct the secret by pooling their shares." is a promising approach to alleviate these concerns, through the use of shares. The SSS is developed not only to carry authentication signals and image content data but also to help repair tampered data through the use of hares.

Several SSS techniques have been proposed to overcome this weakness from these technique is the well none (k, n) threshold schemes. A secret is transformed into n shares and distributed to n participants and only k of them can pool their shares, where $k \leq n$, to recover the secret d. Algorithm (1) review the detail of secret sharing, while algorithm (2), is secret recovery [1],[2],[3].

Algorithm 1: (k, n) Threshold Secret Sharing

Input: Take secret d in the form of an integer, number n of participants and threshold $k \leq n$.

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

Process:

Step1: Choose a random prime number p larger than d.

Step2: Select $k - 1$integer values, $c_1, c_2, \dots c_{k-1}$range of 0 through $p - 1$.

Step3: Select $n$distinct real values $x_1, cx_2, \dots x_n$

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

$F(x_i) = \left(d + c_1x_i^1 + c_2x_i^2 + \cdots . + c_{k-1}x_i^{k-1}\right)$, ……. (1)

Step5: Deliver the two tuple $\left(x_i, F(x_i)\right)$, as a share to the ith participant where $i = 1, 2, 3, \dots., n$

Step6: End.

Algorithm 2: (k, n)Secret Recovery of Shares

Input: Select k shares from the n, participants and the prime number p with both t and p are being those used in Algorithm 1

Output: Secret d hidden in the shares and coefficients c_i used in (1) of Algorithm 1, where $i = 1, 2, 3, .., k - 1$

Step1: Use the k shares $\left(x_1, F(x_1), x_2, F(x_2), \dots, x_k, F(x_k)\right)$, to set up

$F(x_i) = \left(d + c_1x_i^1 + c_2x_i^2 + \dots + c_{k-1}x_i^{k-1}\right)_{\mathrm{mod}_p} \cdots$ (2) Where $j = 1, 2, 3, \dots, k$

Step2: Solve the k equations above by Lagrange's interpolation to obtain d as follows:

$$d = (-1)^{k-1}\left(\sum_{i=1}^{k} F(x_i) \prod_{i\neq j,1\leq j\leq k} \frac{x_j}{x_i - x_j}\right)_{\mathrm{mod}_p} ,\ldots (3)$$

Step3: End.

Generally the research in this direction focused on different topics such as [2],[3],[4],[5],[6],and[7]: Distortion in Stego-image, Tampering Localization Capability, Repair Capability, Reported Authentication precision, Distribution of authenticated image parts, Manipulation of data embedding, as shown in Table 1. All but Lee& Tsai [2], and kavitha&shanavas [3] method will create distortion in the stego-image during the authentication process. More importantly, only Lee& Tsai [2], and kavitha&shanavas [3] 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 like, Yang and Kot [5], Tzeng, Tsai [7], Lee& Tsai [2], and kavitha&shanavas [3].Method, Lee& Tsai [2], and kavitha&shanavas [3] provide a finer authentication precision with the block size of 2×3. Specifically, the method in [5] needs larger macro-blocks to yield pixel flip abilities for embedding authentication data. In the case of using smaller blocks, Tzeng and Tsai’s method [7] has a high possibility to generate noise pixels as mentioned in [6], and so they conducted experimental results with the larger block size of 64×64.

Table 1: Comparison of different document image authentication methods

	Distortion in Stego-image	Tampering Localizatio n	Repair Capability	Reported Authenticatio n precision	Distribution of authenticated	Manipulation of data embedding
Wu & Liu [4]	Yes	No	No	Macro-block	Non-blank part	Pixel flippability
Yang & Kot [5]	Yes	Yes	No	33×33 block	Non-blank part	Pixel flippability
Yang& Kot [6]	Yes	No	No	Macro-block	Non-blank part	Pixel flippability
Tzeng& Tsai	Yes	Yes	No	64×64 block	Entireimage	Pixel replacement
Lee& Tsai[2]	No	Yes	Yes	2×3 block	Entire image	Alpha channel Pixel
kavitha& shanavas[3]	No	Yes	Yes	2×2 block	Only at strong points	Adaptive mod 4 Embedding.

Lee&Tsai [2], and kavitha&shanavas [3], uses random number generator to randomize the location for embedding the mapped partial shares.

This paper presents a Proposal for harmonic secret sharing and permutation based authentication technique to document image, with the aim of using secret sharing that can achieve requirements listed below:

1. Authenticate a document image.
2. Verify the owner of a document image.
3. Detect the error in a document image, and
4. Correct the error in a document image.
5. Localizes the alteration in a document image.

The proposed technique uses permutation based ID as a secret key to randomize the location for embedding the mapped partial shares; also the proposed technique added another layer of security to the stego-image.

The rest of the paper is organized as follows; Section 2. The proposed method ispresented in Section 3.concludes the work and lists future directions of the work.

2. PROPOSED SCHEMA

A detailed description of the proposed scheme is depicted in this section. In our scheme, a binary version of the image S of the size RXC with one bit per pixel is generated from a grayscale digital document image S of the size RXC with 8 bit per pixel. The proposed scheme includes two main procedures: the first is embedding and authentication phase as depicted in Figure (2), and the other is reconstructing and verifying phase as depicted in Figure (3), Figure (4), with algorithm (3) of secret key generation [8], following on the details described in proposed authentication technique to document image.

Algorithm 3: Secrete Key Generation

```
Input: ID, key K.
Output: secret key
Process:
Step1: Input the ID, integer number as a secret key
Step2: Convert ID to digital form
Step3: Remove the replicated
Step4:Find their classes using secret key
Step5: End.
```

2.1 Embedding and Authentication Phase

We create a PNG image from a binary like grayscale document image S with an alpha channel plane. The actual image S may be assumed as a grayscalechannel plane of the PNG image, and then S is converted to binary form with moment preserving threshold, yielding a binary version of S, which we denoted as S_b, and taken as an input to generate n secret shares of the data. The share values are mapped subsequently into a small range of alpha channel values near the maximum transparency value to create an imperceptibility effect. Lastly, the mapped secret shares are randomly entrenched into the alpha channel for the function of promoting the security, protection and data repair capability.

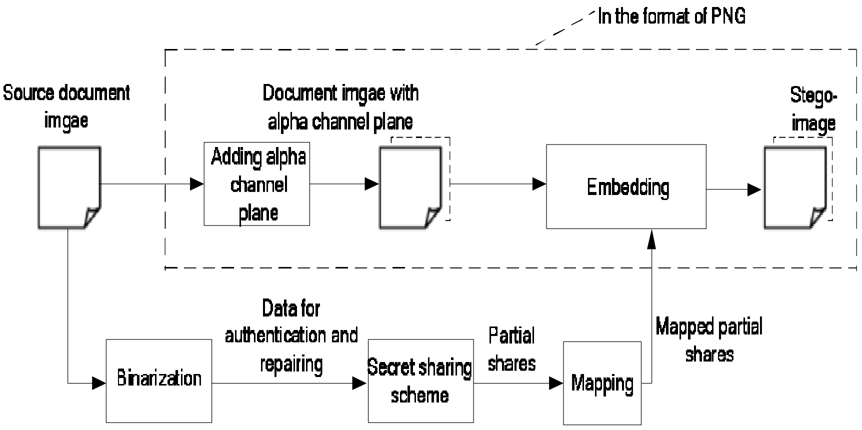

Figure 1: Illustration of creating a PNG image from a grayscale document image and an alpha channel

The alpha channel plane is used for carrying data for authentication and repairing so no demolition will occur to the input image in the process of verification.

The algorithm for generation a stego-image in the PNG format of the anticipated method is described below:

Algorithm 4: Generating a stego-image in PNG format from a given grayscale image.

Input:A document image in grayscale S with two major gray values, and a secret key K.

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

Process:

Step A: Cover Generating: Convert S into a PNG image with an alpha channel plane Sα by creating a new image layer with 100% opacity and no colour as Sα and combining it with S using an image processing software package.

Step B: authentication signals Generating:

1. Binarization: Apply moment-preserving threshold [9] to S to obtain two representative gray values g1 and g2, compute the threshold T

T = (g1 + g2)/2; and use T to convert S into binary form, yielding the binary version Sb with "0" representing g1, and "1" representing g2.

2. Loop: Take a 2×3 block Bb of Sb with pixels p1, p2 …p6.

3. Creating authentication signals: Create a 2-bit authentication signal Z= a1a2 witha1 = $\sum_{i=1}^{3} \mathbf{p_i}$ $(\mathbf{mod\ 2})$ and a2 =$\sum_{i=4}^{6} \mathbf{p_i}(\mathbf{mod\ 2})$, then concatenate the 8 bits of a1, a2, and p1 through p6 to form an 8-bit string, divide the string into two 4-bit segments, and convert the segments into 2 decimal numbers m1 and m2, respectively.

4. Partial Share Generation: Set p, ci, and xi in Eqn. (1) of Algorithm 1 to be the following values:p = 17; d = m1, c1 = m2; x1 = 1, x2 = 2… x6 = 6; and execute Algorithm 1 as a (2, 6) - threshold secret sharing scheme to generate six partial shares q1 through q6 using the following equations:qi = F(xi) = (d + c1xi)mod p (3)Where i = 1, 2… 6.

5. Mapping: Adding 238 to each of q1 through q6, resulting in the new values of q1 ′ , through q6 ′ , respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane Sα.

6. Embedding two fractional shares in the current block: receive the block Bα in Sα corresponding to Bb in Sb, select the first two pixels in Bα in the raster-scan order, and substitute their values by q1 ′ and q2 ′, respectively.

7. End of loop: If there exists any unprocessed block in Sb, then go to (2), else, go to (Step C)

Step C. Permutation: permute Sα using a secret k, then take the final S in the PNG format as the preferred stego-image S ′.

2.2 Stego-Image Authentication

A complete algorithm describing the proposed stego-image authentication process,including both verification and self-repairing of the original image content, is described below.

Algorithm 4: Authentication of a given stego-image in the PNG format

Input: A stego-image S ′, the representative gray values g1 and g2, and the secret keyK used in Algorithm 3.

Output: An image Sr with tampered blocks marked, and their data repaired if possible.

Process:

Part A: Extraction of the embedded two representative grey values.

Part B: Inverse permutation

Part C: Authentication of the stego-image.

Step 1: Binarization: Compute T = (g1 + g2)/2, And use it as a threshold to convert S ′ into Binary Form, yielding the binary version Sb ′ of S ′ with “0 ” representing g1 and “1 ” representing g2.

Step 2: (Start looping) Take in a raster-scan order an unprocessed block Bb ′ fromSb ′ with pixel values p1 through p6, and find the 6 pixel values q1 ′ , through q6 ′ of the corresponding block Bb ′ in the alpha channel plane S α ′ of S ′ .

Step 3: authentication signalExtraction: to extract the hidden 2-bit authentication signal Z = a1a2 from B α ′ we will follow the steps:

(1) Subtract 238 from each of q1 ′ and q2 ′ to obtain the 2 respective partial shares q1 and q2 of Bb ′.

With the shares (1, q1) and (2, q2) as input, perform Algorithm 2 to extract the 2 values d and c1 (the secret and the first coefficient value, respectively) as output.

(2) Transform d and c1 into two 4-bit binary values, concatenate them to form an8-bit string W, and take the first two bits a1 and a2 of W to compose the hiddenauthentication signal Z =a1a2.

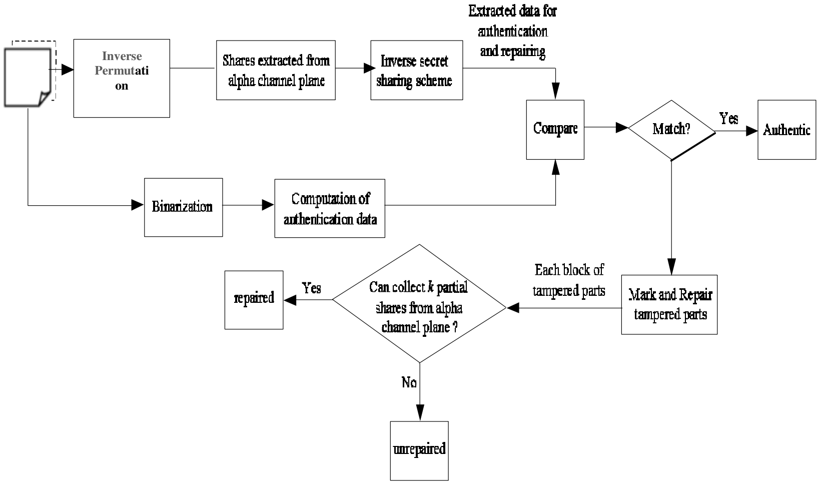
Inverse Permutati on
Shares extracted from alpha channel plane
Inverse secret sharing scheme
Extracted data for authentication and repairing
Compare
Match?
Yes
Authentic
Binarization
Computation of authentication data
Each block of tampered parts
Mark and Repair tampered parts
Can collect k partial shares from alpha channel plane ?
Yes
repaired
No
unrepaired

Figure 2: Authentication process including verification and self-repairing of a stego-image in PNG format

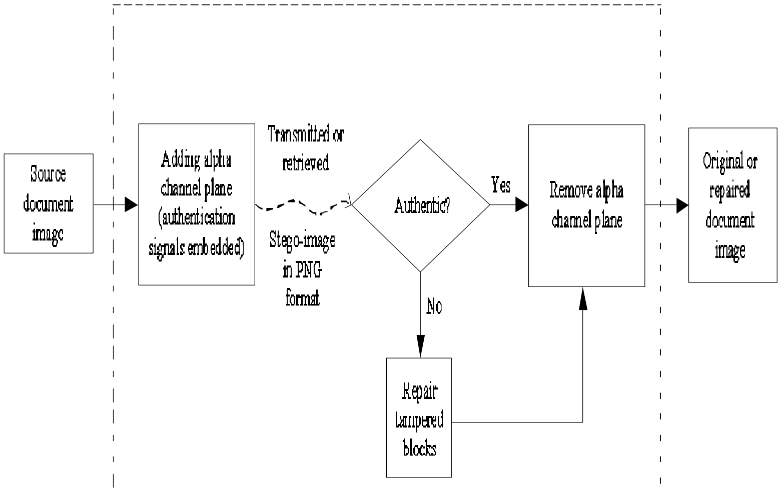
Source document image
Adding alpha channel plane (authentication signals embedded)
Transmitted or retrieved
Stego-image in PNG format
Authentic?
Yes
No
Remove alpha channel plane
Repair tampered blocks
Original or repaired document image

Figure 3: Framework of proposed document image authentication method

Step 4 :(Computationof the authentication: Compute a two-bit authentication signal Z′ = a1 ′ a 2 ′ from the values p1 through p6 of the six pixels of Bb′ by a1′=$\sum_{i=1}^{3} p_i \ (mod\ 2)$ and a2 **′=$\sum_{i=4}^{6} p_i (mod\ 2)$.**

Step 5: (Harmonizing the hidden and computed authentication signals and marking oftampered blocks) Match Z &Z ′ by checking if a1= a1 ′ & a2= a2 ′ , and if any variance occurs, mark Bb ′ , the corresponding block B ′ in S ′ , and all the partial shares embedded in B ′ α as tampered.

Step 6: (Close loop) if there exists any unprocessed block in Sb′, then go to Step 2;otherwise, go on.

Part 3: Self-repairing the original image content**Step 7: (Drawing out of the remaining partial shares)** For each block B ′ α in S α ′ , extract the remaining 4 partial shares q3 through q6 of the corresponding block Bb ′ in Sb ′ from blocks in S α ′ other than B′ α .

(1) collect the 4 pixels in S ′ α , and take out the respective data q3 ′, q4 ′, q5 ′, and q6 ′ embedded in them.

(2) Subtract 238 from each of q3 ′ through q6 ′ to obtain q3through q6, respectively.

Step 8: (Repair the tampered regions) On behalf of each block B ′ in S ′ marked as tampered previously, execute the following steps to repair it if possible.

(1) From the 6 partial shares q1 through q6 of the block Bb ′ in Sb ′ corresponding to B ′ (two computed in Step 3(1) and four in Step 7(2) above), select 2 of them, say qk and ql, which are not marked as tampered, if possible.

(2) With the shares (k, qk) and (l, ql) as input, execute Algorithm 2 to mine the values of d and c1 (the secret and the first coefficient value) as output.

(3) Transform d and c1 into two 4-bit binary values and concatenate them to form an 8-bit string W ′.

(4) Take the last 6 bits b1 ′ , b2 ′ ,… b6 ′ from W ′ and check their binary values to repair the corresponding tampered pixel values y1′ , y2 ′ , …, y6 ′ of block B ′ by the following way: if bi ′ = 0, set yi ′ = g1; otherwise, set yi ′ = g2; where i = 1, 2… 6.

Step 9: Take the final S ′ as the desired self-repaired image Sr.

7. CONCLUSION AND FUTURE WORK

We have proposed an image document authentication method along with self-repair capability, error localization and owner verification for binary-like grayscale document images based on secret sharing and permutation. Both the generated authentication signal and the content of a block are transformed into partial shares by the SSS method, which are then embedded into an alpha channel plane to create a stego-image in the PNG format, after applying a permutation using a secret key. For self-repairing the content of a tampered block, a reverse Shamir scheme is used to compute the original content of the block from any 2 un-tampered shares. The possible Future studies take several directions, including choices of other block sizes and associated parameters to advance data repair effects. Applications of the proposed method for authentication and repairing of attacked colour images, and block based owner validation may also be applied.

ACKNOWLEDGEMENTS

I would like to thank the International Arab Conference on Information Technology, Sudan University of Science and Technology, and CCIS, Zarqa University, Jordan for supporting this publication.

REFERENCES

[1] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[2] 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.

[3] S KavithaMurugesan, Shanavas K A,"Secure Image Authentication of a Grayscale Document using Secret Sharing Method and Chaotic Logistic Map with Data Repair Capability", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013

[4] M. Wu and B. Liu, "Data hiding in binary images for authentication and annotation," IEEE Trans. on 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 identifier," IEEE Signal Processing Letters, 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. on Multimedia, vol. 9, no. 3, pp. 475–486, April 2007.

[7] 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 Communications Letters, vol. 7, no. 9, pp. 443–445.

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

[9] Serge Lang, Linear Algebra, Third edition, Chapter 2, Springer, 1987.

[10] Ahmed Hashim Mohammed, Dr. Hanaa M. A. Salman and Dr. Saad K. Majeed, "A Survey of Cloud Based Secured Web Application", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 4, 2013, pp. 441 - 448, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[11] Dr. Hanaa M. A. Salman, "Information Hiding in Edge Location of Video using Amalgamate FFT and Cubic Spline", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 4, 2013, pp. 240 - 247, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.