Volume : 1 | Issue : 7 | Dec 2012 • ISSN No 2277 - 8160

Research Paper | Computer Science

A Novel Method for Secret Sharing Gray-Scale Document Images with data Repair Capability

K. Mohan

Asst. Professor, Member of IACSIT, Department of Computer Science & Engineering, Thirumalai Engineering College, Kanchipuram

ABSTRACT

A new blind authentication method based on the secret sharing techniques with a data repair capability for gray-scale document images via the use of the Portable Network Graphics (PNG) image with stego image is proposed. An authentication signal is generated for each block of a gray-scale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many share as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original gray-scale image to form a PNG image. During the embedding process, the gray-scale document image getting from stego image that's the image stegonagraphy used to hide the original image behind the gray-scale document image then it is converted into gray-scale image after getting the gray-scale image to add with alpha channel. In the process of image authentication, an image block is marked as tampered if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane. Data repairing is then applied to each tampered blocks by a reverse Shamir scheme after collecting two shares from unmarked blocks. Measures for protecting the security of the data hidden in the alpha channel are also proposed.

KEYWORDS : Stego-image, Data hiding, data repair, gray-scale document image, Portable Network Graphics (PNG)

I. INTRODUCTION

Digital image is a form for preserving important information. However, with the fast advance of digital technologies, it is easy to make visually imperceptible modifications to the contents of digital images. How to ensure the integrity and the authenticity of a digital image is thus a challenge. It is desirable to design effective methods to solve this kind of image authentication problem [1]–[3], particularly for images of documents whose security must be protected. It is also hoped that,

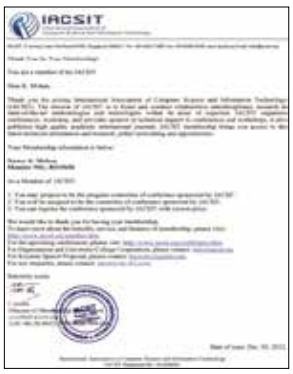

Fig. 1. Binary-like gray-scale document image with two major gray values.

if part of a document image is verified to have been illicitly altered, the destroyed content can be repaired. Such image content

authentication and self-repair capabilities are useful for the security protection of digital documents in many fields, such as important certificates, signed documents, scanned checks, circuit diagrams, art drawings, design drafts, last will and testaments, and so on. Document images, which include texts, tables, line arts, etc., as main contents, are often digitized into gray-scale images with two major gray values, one being of the background (including mainly blank spaces) and the other of the foreground (including mainly texts). It is noted that such images, although gray valued in nature, look like binary. For example, the two major gray values in the document image shown in Fig. 1 are 174 and 236, respectively. It seems that such binary-like gray-scale document images may be thresholded into binary ones for later processing, but such a thresholding operation often destroys the smoothness of the boundaries of text characters, resulting in visually unpleasant stroke appearances with zigzag contours. Therefore, in practical applications, text documents are often digitized and kept as gray-scale images for later visual inspection.

In this paper, Hide the original document gray image with image using image stegnopgraphy, then this gray-scale document image added with alpha channal and a method for the authentication of document images with an additional self-repair capability for fixing tampered image data is proposed. The input cover image is assumed to be a binary-like gray-scale image with two major gray values like the one shown in Fig. 1. After the proposed method

is applied, the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format with an additional alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be 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. In case the alpha channel is totally removed from the stego-image, the entire resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The proposed method is based on the so-called -threshold secret sharing scheme proposed by Shamir [11] in which a secret message is transformed into shares for keeping by participants, and when of the shares, not necessarily all of them, are collected, the secret message can be losslessly recovered. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

II. REVIEW OF THE SHAMIR METHOD FOR SECRET SHARING

In the (k, n) threshold secret sharing method proposed by Shamir [11], secret d in the form of an integer is transformed into shares, which then are distributed to participants for them to keep; and as long as of the shares are collected, the original secret can be accordingly recovered, where k<=n. The detail of the method is reviewed in the following.

Algorithm 1: (k, n)**-threshold secret sharing.**

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

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

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

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

Step 3. Select n distinct real values $x_1, x_2, \ldots, x_n$.

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

$$F(x_i) = \left(d + c_1 x_i + c_2 x_i^2 + \cdots + c_{k-1} x_i^{k-1}\right)_{\bmod p}. \quad (1)$$

Step 5. Deliver the two-tuple $(x_i, F(x_i))$ as a *share* to the ith participant where $i = 1, 2, \ldots, n$.

Algorithm 2: Secret recovery.

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

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

Steps.

Step 1. Use the k shares $(x_1, F(x_1)), (x_2, F(x_2)), \ldots, (x_k, F(x_k))$ to set up

$$F(x_j) = \left(d + c_1 x_j + c_2 x_j^2 + \cdots + c_{k-1} x_j^{k-1}\right)_{\bmod p} \quad (2)$$

where $j = 1, 2, \ldots, k$.

Step 2. Solve the k equations above by Lagrange's interpolation to obtain d as follows [12]:

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

Step 3. Compute c_1 through c_{k-1} by expanding the following equality and comparing the result with (2) in Step 1 while regarding variable x in the equality below to be x_j in (2):

$$F(x) = \left[F(x_1)\frac{(x-x_2)(x-x_3)\ldots(x-x_k)}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)} + F(x_2)\frac{(x-x_1)(x-x_3)\ldots(x-x_k)}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)} + \cdots + F(x_k)\frac{(x-x_1)(x-x_2)\ldots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}\right]_{\bmod p}.$$

Step 3 in the above algorithm is additionally included for the purpose of computing the values of parameters Ci in the proposed method. In other applications, if only the secret value d need be recovered, this step may be eliminated.

III. IMAGE STEGNOGREAPHY WITH DATA REPAIRING

In the proposed method, The original document image behind the image by using image –stegnography techniques, then the gray-scale document image combined with alpha channel. This process called as embedded after finally to get PNG (Portable Network Graphics). The alpha channel is transparency of pixel when embedded with gray-scale image, the pixel occupied in alpha channel so easily identify if any changes occur in the origianl gray-scale image otherwise decrypt the image using image-stegnography from this to get origianl source of gray-scale document image.

Since the alpha channel plane is used for arrying data for authentication and repairing, no destruction will occur to the input image in the process of authentication. In contrast, conventional image authentication methods often sacrifice part of image contents, such as least significant bits (LSBs) or flippable pixels, to accommodate data used for authentication

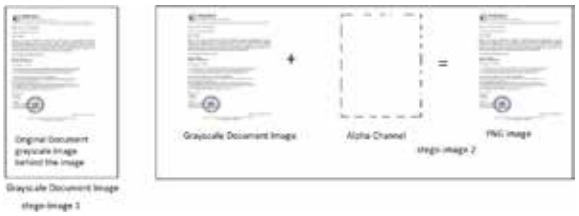

Fig.2 Illustration of Creation of a PNG image from gray-scale document image with alpha channel

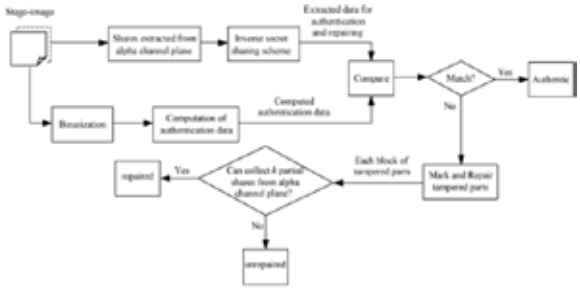

Fig.3 Authentication process including verification and self-repairing of a stego-image in PNG format.

V. CONCLUSION

A new blind image authentication method with a data repair capability for binary-like gray-scale document images based on secret sharing has been proposed. Both 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 in the PNG format. 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 black authentication, two stegno-images used in this paper. That's while adding the alpha channel before to get stego-image1 then after adding alpha channel to get stego-image2.

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. 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. | [3] 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. | [4] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979. |