International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 8, August - 2013

Authentication and Self Recovery Of Color Images

Aswany Shaji[1], Silpa Joseph[2]

[1]M.Tech Student (CSE), Mahatma Gandhi University
Viswajyothi College of Engineering and Technology, Muvattupuzha, Kerala, India

[2] Assistant. Professor (CSE), Mahatma Gandhi University
Viswajyothi College of Engineering and Technology, Muvattupuzha, Kerala, India

Abstract *– An authentication and self recovery method for color images based on a secret sharing technique is proposed. Half toning technique is applied to each gray scale planes of color image. A half toned image is a binary image which consists a set of dots rather than continuous tones. Each half toned binary plane is divided into equal sized blocks. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The secret shares generated for the first plane is embedded into the alpha channel plane itself. Two other images. One is black and one is white, are selected for embedding the secret shares of remaining two planes. In the process of image authentication, Each plane of color image is verified separately, 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 block by a reverse Shamir scheme after collecting two shares from any two untampered blocks.*

Keywords*: *Authentication, self recovery, color image, secret sharing scheme, half toning

I. INTRODUCTION

Images are form of preserving secret information. With the advance of digital technologies, it is easy to make visually unnoteceble modifications to the contents of digital images. How to ensure the integrity and the authenticity of images are now become a challenge. It is desirable to design effective methods to solve this kind of image authentication problem, particularly for document images whose security must be protected.

In this paper, we propose an authentication method that deals with color images, particularly color document images simultaneously solves the problems of image tampering detection and visual quality keeping. The remainder of this paper is organized as follows: In Section 2, the proposed method is explained briefly.. In Section 3, the modules of the proposed method, including authentication signal generation, share data embedding, authentication of stego image and tampered data repairing, are described. In Section 4, Experimental results are given, followed by conclusions and future enhancement in Section 5.

2. PROPOSED SYSTEM

The input cover image is assumed to be a color image so it contains three gray scale channel planes. Each grayscale image planes are processed separately. Firstly, half toning technique is applied to each planes. A half toned image is a binary image made up of a series of black and white dots rather than a continuous tones. Then each half toned binary images are divided into equal sized blocks. An authentication signal is generated for each block by the method proposed by Che-Wei Lee and Wen-Hsaing [1]. The authentication data for each block is transformed into several shares using Shamir secret sharing scheme. The secret shares generated for the first plane is embedded in alpha channel plane of the secret image itself using a secret key. Two other images. One is black and one is white, are selected for embedding the secret shares of remaining two planes. Secret data is embedded in alpha channel planes of selected images using the above mentioned same secret key. 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 that carry secret shares of one channel. In addition to this we have one black image and white image, whose alpha channel plane contains secret data for other two channels. These two images need to be sent with the stego image for authentication and recovery purpose. The stego-image, when received or retrieved, may be verified by the proposed method for its authenticity. Integrity modifications of each red green and blue channels of stego-image can be detected at the block level and repaired at the pixel level. Binary content of each

channel plane is repaired by applying inverse Shamir secret sharing scheme. Then, the gray scale colors of modified parts are restored by using inverse half toning technique. 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 (k,n) -threshold secret sharing scheme proposed by Shamir [2] 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.

3. MODULES

3.1. Authentication Signal Generation

Binarize each gray scale channel plane of RGB image by applying half toning. Then, divide each half toned image into 2×3 blocks. We generate authentication data for every 2×3 blocks. Take in an unprocessed raster scan order a 2×3 block of half toned image with pixels p1,p2,…p6. Then Generate a 2-bit authentication signal s = a1a2 with a1 = p1 x-or p2 x-or p3 and a2= p4 x-or p5 x-or p6. Next. Create data for secret sharing by Concatenating the 8 bits of a1,a2 and p1 through p6 to form an 8-bit string, divide the string into 4-bit segments. And transform the segments into 2 decimal numbers m1 and m2. These decimal numbers m1 and m2 are the secret data for a particular 2×3 block. In this way, we calculate authentication and scret data for every 2×3 block of three halftoned binary planes.

3.2. Partial Share Generation

In order to create shares of secret data for a particular 2×3 block, perform Shamir secret sharing algorithm [2] as a (2,6) threshold secret sharing scheme with m1 and m2 as inputs. The detailed algorithm is given in the method proposed by Che-Wei Lee and Wen-Hsaing [1].

3.3. Mapping of partial shares

The next step is to embed the generated secret shares of each block of each gray scale plane into the alpha channel planes of images. Secret shares for the first plane is embed in the alpha channel plane of secret image itself. In order to embed the secret shares of remaining two planes, we select one black image and one white image. Then embed the secret shares into alpha channel plane of those images. The algorithm for embedding the secret shares of gray scale image is given in Che-Wei Lee and Wen-Hsaing [1] method. We applied this algorithm to embed the secret shares of remaining two planes in alpha channel planes of additionally selected black image and white image. These black image and white image is sent with the secret image for image authentication.

3.4. Image Authentication

Each gray scale channel plane is processed separately for authentication. We binarize each gray scale channel of received stego image using half toning technique. Image authentication is performed at the block level, ie every 2×3 binarized blocks are verified separately. Take in raster scan order an unprocessed binary block with pixel values p1 through p6 and corresponding block in the alpha channel plane. Extract first two shares from alpha channel plane and apply the reverse of shamir secret sharing scheme [2] to extract the 2-bit authentication signal s = a1a2. Also, compute the authentication data form the binary blocks of received stego image as explained above. Then, compare the extracted authentication signal and computed authentication signal. If these two signals are not matched, the given block is marked as tampered. In this way, authenticate every 2×3 blocks of three channels.

3.5. Recovery of tampered blocks.

If a particular block is marked as tampered , it implies two shares embedded in the current block of alpha channel plane are modified or lost. There are 6 partial shares for a block. For tampered blocks, extract the remaining four partial shares using the secret key. If we can collect any two partial shares from two untampered block, the binary content of a block can be reconstructed by applying the inverse Shamir secret sharing scheme. Again, the gray scale content of modified parts can be reconstructed by applying inverse halftoning technique.

4. EXPERIMENTAL RESULTS

The results that we show come from our experiments using a color image poster shown in Fig:1. We have also conducted image-modification attacks to the stego-images using two common image editing operations, namely, superimposing and painting. The repaired image is shown in Fig 4.

Fig1: Orginal Image

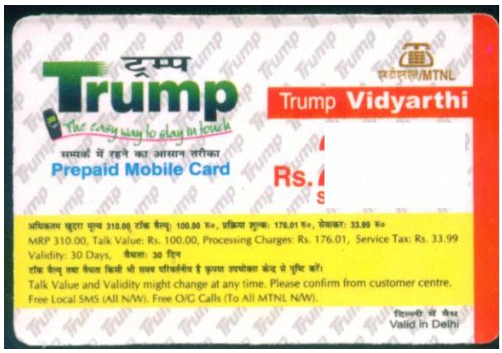

Fig2: Tampered Image (Painting)

Fig3: Tampered Image (superimposing)

Fig 4: Repaired image

5. CONCLUSION

A new blind image authentication method with a data repair capability for color images based on secret sharing has been proposed. An authentication signal is generated for every block of each gray scale channels of RGB image. The generated authentication signasl and the content of each block have been transformed into partial shares by the Shamir method. Authentication data generated for one plane is embedded in alpha channel plane of secret image itself. Two images, one black image and one white image is created for embedding authentication data for other two planes. 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. Experimental results have been shown to prove the effectiveness of the proposed method. Future studies may be directed to avoid the use of two additional images to carry the secret data.

REFERENCES

[1] Che-Wei Lee, Wen-Hsaing, "A secret sharing based method for authentication of grayscale document image via the use of PNG image with a data repair capability," IEEE Transactions on image processing, vol. 22, no. 11, pp. 612–613, Jan. 2012.

[2] A. Shamir, "How to share a secret," Commun. ACM, vol. 21, no. 1, pp. 612–613, Jan. 1979.

[3] 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.

[4] Niladri B. Puhan, Anthony T. S. Ho, "Binary Document Image Watermarking for Secure Authentication Using Perceptual Modeling" 2005 IEEE International Symposium on Signal Processing and Information

[5] 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.