International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

An Authentication and Recovery method for Color Images

Subhash Rathod[Å*] and A. K. Gupta[Å]

[Å] Computer Engineering Department, University of Pune, JSCOE, Pune, India

Accepted 15 July 2014, Available online 01 Aug 2014, **Vol.4, No.4 (Aug 2014)**

Abstract

With fast advance of digital technology image processing is the fastest growing area of research and development. Sharing the data and authenticate the same is the big challenges now a days. To overcome the problem of pretending the documents as well as image as on his /her name, we invent the new method of an authentication and recovery of color tampered image using secure Shamir secret sharing method. The proposed method is an authentication and recovery technique for color images based on a Shamir secret sharing technique. An alpha channel signal which is used for authentication is generated for each block of a color document image, which, together with the binaries block content, is transformed into several shares using the Shamir secret sharing scheme. Care should be taken while selecting the parameter so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original image to form a PNG image. During 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 block by a reverse Shamir scheme after collecting two shares from unmarked blocks. By considering the lager database for images as well scan documents images with good experimental results prove the effectiveness of the proposed method for real applications.

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

1. Introduction

Digital image is used for storing and preserving the importance as well as confidential information in the information era. With growing need of digital technology and image as well as data transfer fast over the internet. Images are form of preserving secret information. With the advance of digital technologies, it is easy to make visually unnoticeable 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 proposed an Authentication and Recovery Technique for Color Images Based on a Shamir Secret Sharing Technique, 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 I Introduction, Section II Literature Survey, Section III the proposed method is explained briefly, Section IV Methodology, Section V pros and cons of method & conclusion.

2. Literature Survey

Shamir Secret Sharing Scheme

Shamir proposed (k, n) threshold mechanism also called secret sharing scheme based on polynomial interpolation. (Shamir, 1979). Dealer constructs n shares denoted by (S1, S2… Sn), from a secret S. The dealer selects a large prime number p and a (k−1) degree polynomial is constructed as in (1) to compute shares using the secret:

$$F(x) = (S + a1x + a2x2 +\cdot\cdot\cdot+ak-1xk-1) \bmod p \qquad (1)$$

Coefficients of the polynomial (a1, a2, · · · ak−1) are randomly selected from integers within the range [0, p]. The dealer then computes shares as in (2):

$$y1 = (1, F(1)),\ y2 = (2, F(2)),\ \cdot\cdot\cdot,\ yn = (1, F(n)) \qquad (2)$$

Each share is a pair of two integers satisfying xi / = 0. If any k of the n pairs gathers, involved participants can reconstruct polynomial F(x) using Lagrange's interpolation technique.

Therefore, all the coefficients of the polynomial are recovered. The constant term of the polynomial is the secret S. Any number of participant's less than k cannot recover the secret at all. Therefore, Shamir's secret sharing scheme is a perfect secret sharing scheme.

The proposed method use Shamir's method to share the secret image such as medical images, wanted images, copyright images etc.

*Corresponding author: **Subhash Rathod**

3. 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 plane. A half toned image is a binary image 1 made up of a series of black and white dots rather than 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. (Che-Wei Lee and Wen-Hsaing, 2012). 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 (Shamir, 1979) 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 recovered without loss. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.

4. Methodology

A. Authentication Signal Generation

Binaries 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 secret data for every 2×3 block of three halftone binary planes.

B. Partial Share Generation

In order to create shares of secret data for a particular 2×3 block, perform Shamir secret sharing algorithm (Shamir, 1979) as a (2,6) threshold secret sharing scheme with m1 and m2 as inputs. The detailed algorithm is given in the method proposed. (Che-Wei Lee and Wen-Hsaing, 2012)

C. 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 (Che-Wei Lee and Wen-Hsaing, 2012) 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.

D. Image Authentication

Each gray scale channel plane is processed separately for authentication. We binaries each gray scale channel of received stego image using half toning technique. Image authentication is performed at the block level, i.e. every 2×3 binaries 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 (Shamir, 1979) 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.

E. 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 un-tampered blocks, 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 half toning technique.

F. Identification of Reference Color Plane

In this phase, we use digital image as input to the system. Then we split the given digital image into its three bit planes. Since, each pixel of the image is of 24-bit, we divide it into 3 different bytes of RGB planes. Then we select a reference plane whose least significant bit of every pixel in the digital image would be used to generate the watermark that is needed during embedding phase. That is we store the least significant bit values for every pixel for a reference plane and use it for producing watermark. As every image might have different least significant bit values it would help us producing the watermark in dynamic way. We will not be considering the reference plane for pixel difference expansion the other two planes will be considered for pixel difference expansion. The pixels of digital image in the proposed scheme are given in 24-bits. The green channel of the digital image contains the important details than other color channels. Hence, the green color plane is chosen as reference color plane to generate the watermark.

G. Generating Watermark using Messy System

Messy system (S.Poonkuntranl and R.S.Rajesh, 2011) is a dynamic system whose behavior changes according to time. These changes are very sensitive to the initial conditions. Thus, the behavior of messy system appears to be random, though they are deterministic. The dynamic changes of this system are completely defined by their initial conditions without any random elements. Therefore, the watermark is generated through messy system using the reference color plane as initial condition. Thereby, the watermark is generated dynamically. A general messy system is defined by the following equation (S.Poonkuntranl and R.S.Rajesh, 2011), (J. Tian, 2002).

$$Xn+1 = f(Xn) \qquad (3)$$

Where f (*) refers the iterative, nonlinear function. It iteratively produces the values for initial value. It is known as messy sequence.

In the proposed system, a hybrid optical bi stable messy system is used which is defined by

$$f(Xn) = 4\sin 2(Xn - 2.5) \qquad (4)$$

The watermark is generated through messy system by using prominent pixel values of reference color plane of the image as seed pixel. The initial values to the messy system is designed by

$$x\_seq(k,0)=a*floor(s(k)/2l)*2l+b*pos+c* \qquad (5)$$

key plane of the image. ***a***, ***b*** and ***c*** are predefined constants and ***l*** refers embedding depth. The position information (pos) and secret key (key) is also used in the initial condition. The messy sequence is generated by substituting x_seg (k, 0) value for Xn in Eqn.2. For the kth pixel the sequence is referred as x_seq (k, i), i=l, 2, 3 ... l. The reasonable number of iteration (I) is performed for the kth pixel to attain the messy status e.g. If image is of size 512 X 512, then there will be 512*512 possible iterations. The watermark generated is dynamic and is unique for every image chosen for watermarking. In this phase, we encrypt the watermark with the help of some external key. This same key is required to extract the watermark at verification phase.

H. Embedding of A –Channel

In this phase the α-channel generated within the last phase is embedded within the watermarked image (W_img), along with the undisturbed red, green and blue pixels of the every plane of the image. In this phase 32-bit TGA image (R. Dhanalakshmi and K.Thaiyalnayaki, 2010),(Che-Wei Lee and Wen-Hsiang Tsai, 2012) is generated from watermarked image (W_img).In which first 24 bit stores the RGB planes of watermarked image (W_img) and next 8-bit will store the α-channel values. This watermark is again unique and dynamic for the image. The values of the pixel are kept undisturbed in the image because the image should not be affected because of the watermark produced in the last phase. This phase produces the image with dual watermarking (R. Dhanalakshmi and K.Thaiyalnayaki, 2010). Now the dual watermarked image consists of both watermarks i.e. first watermark produced with the help of reference plane's least significant bit values and the second watermark generated within the last phase.

I. Extraction and Verification

In the extraction process, the watermarked image W_Img is processed in the same way as original image processed for embedding. The extraction process is complete blind. Both original image and original watermarks are not used for the extraction process. In this phase we check if the image has been damaged or not with the help the two watermarks that we have embedded as proposed in the paper.

5. Discussions

Merits of the Proposed Method

In addition to being capable of data repairing and being blind in nature (requiring no overhead other than the stego-image), the proposed method have several other merits, which are described in the following:

1) Providing pixel-level repairs of tampered image parts As long as two un-tampered partial shares can be collected, a tampered block can be repaired at the pixel level by the proposed method. This yields a better repair effect for texts in images because text characters or letters are smaller in size with many curved strokes and need finer pixel-level repairs when tampered with.

2) Having higher possibility to survive image content attacks by skillfully combining the Shamir scheme, the

authentication signal generation, and the random embedding of multiple shares, the proposed method can survive malicious attacks of common content modifications, such as superimposition, painting, etc., as will be demonstrated by experimental results subsequently described.

3) Making use of a new type of image channel for data hiding Different from common types of images, a PNG image has the extra alpha channel plane that is normally used to produce transparency to the image. It is differently utilized by the proposed method for the first time as a carrier with a large space for hiding share data. As a comparison, many other methods use LSBs as the carriers of hidden data.

4) Causing no distortion to the input image. Convention image authentication methods that usually embed authentication signals into the cover image itself will unavoidably cause destruction to the image content to a certain extent. Different from such methods, the proposed method utilizes the pixels' values of the alpha channel for the purpose of image authentication and data repairing, leaving the original image untouched and thus causing no distortion to it. The alpha channel plane may be removed after the authentication process to get the original image.

5) Enhancing data security by secret sharing Instead of hiding data directly into document image pixels, the proposed method embeds data in the form of shares into the alpha channel of the PNG image. The effect of this may be regarded as double-fold security protection, one fold contributed by the shares as a form of disguise of the original image data and the authentication signals and the other fold contributed by the use of the alpha channel plane.

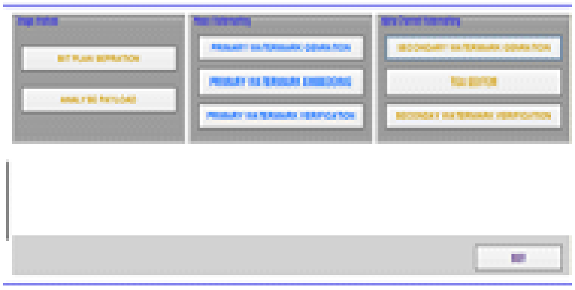
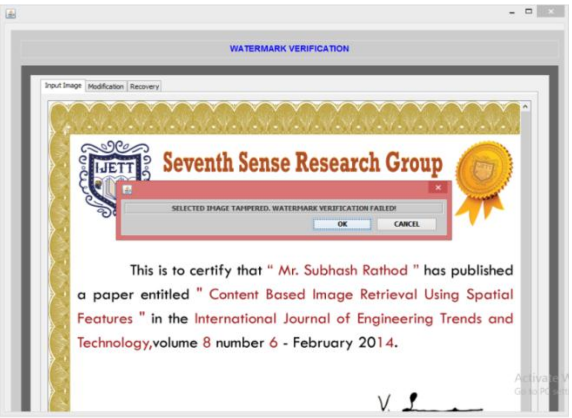

PRIMARY WATERMARK GENERATION
PRIMARY WATERMARK EMBEDDING
PRIMARY WATERMARK VERIFICATION
SECONDARY WATERMARK GENERATION
SECONDARY WATERMARK VERIFICATION

Fig 1 Application Developed

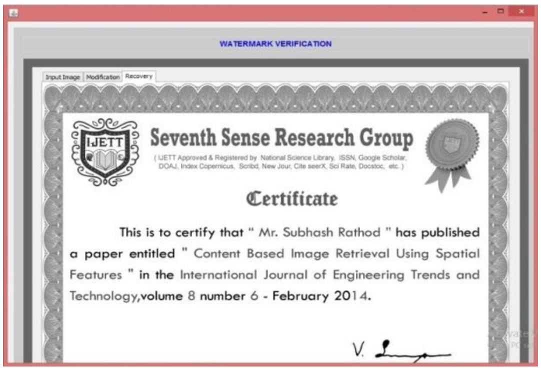


Seventh Sense Research Group

SELECTED IMAGE TAMPERED. WATERMARK VERIFICATION FAILED!

This is to certify that " Mr. Subhash Rathod " has published a paper entitled " Content Based Image Retrieval Using Spatial Features " in the International Journal of Engineering Trends and Technology,volume 8 number 6 - February 2014.

Fig 2 Tampered image



Seventh Sense Research Group

(IJETT Approved & Registered by National Science Library, ISSN, Google Scholar, DOAJ, Index Copernicus, Scribd, New Jour, Cite seerX, Sci Rate, Docstoc, etc.)

Certificate

This is to certify that " Mr. Subhash Rathod " has published a paper entitled " Content Based Image Retrieval Using Spatial Features " in the International Journal of Engineering Trends and Technology,volume 8 number 6 - February 2014.

Fig 4 Recover color images in grayscale formate

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 signals 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 un-tampered 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

Che-Wei Lee, Wen-Hsaing (2012), *A secret sharing based method for authentication of gray scale 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.

A. Shamir (1979), *How to share a secret*, Common. ACM, vol. 21, no. 1, pp. 612–613.

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

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

C. H. Tzeng and W. H. Tsai (2003), *A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement,* IEEE Common. Lett., vol. 7, no. 9, pp. 443– 445, Sep.

S.Poonkuntranl and R.S.Rajesh (2011) *A Messy Watermarking for Medical Image Authentication*. IEEE.

J. Tian (2002). *Reversible watermarking by difference expansion*. IEEE.

A. M. Alattar (2003). *Reversible watermark using the difference expansion of a generalized integer transform*, IEEE.

H. Maitre B. S. Y. R. R. C. G. Coatrieux (2000). Relevance of watermarking in medical imaging, in information technology applications in biomedicine, IEEE.

R. Dhanalakshmi and K.Thaiyalnayaki (2010), Dual Watermarking Scheme with Encryption, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 7, No. 1.

Che-Wei Lee and Wen-Hsiang Tsai (2012). A New Lossless Visible Watermarking Method via The use of The PNG Image.