Authentication of Gray Scale Document Images via the Use of PNG Image with Data Repairing

P. Sujitha[1], G. Murali[2]

[1] M. Tech, Department of CSE, JNTUA College of Engineering, Pulivendula, YSR Dist, A.P, India,

[2] Assistant Professor, JNTUACEP, Department of CSE, JNTUA College of Engineering, Pulivendula, YSR Dist, A.P, India,

Abstract: ***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. For real time applications, good experimental results prove the effectiveness of the proposed method.***

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

1. Introduction

DIGITAL image may be a type for conserving necessary info. However, with the quick advance of digital technologies, it's simple to create visually unbearable modifications to the contents of digital images. How to make sure the consistency and therefore the believability of a digital image is therefore a challenge. The most usual technique used for authentication is textual password identification. The vulnerabilities of this technique like eavesdropping, wordbook attack, social engineering and shoulder surfing are well known. Arbitrary and extended passwords will build the system secure. However the most drawback is that the issue of recollecting those passwords. Unfortunately, these passwords will be simply imagined or hacked. The other techniques are graphical passwords and biometrics. But the both techniques have their own disadvantages.

The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are several graphical password schemes that are proposed within the last decade. Document images, which comprise tables, line arts, texts, etc. as main contents, are also often digitized into grayscale images with two major gray values, one being of the background, which comprises mainly blank spaces and the other of the foreground which comprises mainly texts. It is also noted that such images, although they are gray valued in nature, however they appear like binary.

For example, the two main gray values in the document image [1] displayed in Fig. 1 are 174 and 236, respectively. It appears that such a binary-like grayscale document images may be thresholded into binary ones for eventual processing, but such a thresholding operation all along demolishes the smoothness of the boundaries of text characters, resulting in visually disagreeable stroke appearances along with zigzag contours. hence, in practical applications, text documents are all along digitized and maintained as grayscale images for eventual visual inspection.

Usually, the problem [2], [3] is complex for a binary document image due to its simple binary nature that leads to perceptible changes after authentication signals are embedded in the image pixels. Such changes will cause potential anticipations from attackers. An excellent solution to such binary image authentication ought to so take under consideration not only the protection issue of preventing image tampering and also additionally the need of keeping the visual quality of the ensuring image.

In this paper, we aim an authentication technique that deals with binary-like grayscale document images instead of pure binary ones and simultaneously solves the difficulties of image tampering detection and visual quality preserving. In this aimed technique, a PNG image [5] is made from a binary-type grayscale document image with associate degree alpha channel plane.

The initial image is also thought as a grayscale channel plane of the PNG image. The main purpose of this aimed technique is that image data protection and image-based authentication [6] techniques provide effective solutions for controlling however non-public information and picture are created offered solely to elect individuals. Ontological to the planning of systems utilized to manage images that contain confidential information like medical records, money transactions, and electronic vote systems the approaches conferred during this paper helpful to counter ancient encryption techniques, that don't scale well and are less advantageous once applied on to image files.

2. Overview of the Shamir Method for Secret Sharing

The proposed approach to secret image sharing is based on the *(k, n)*-threshold secret sharing method proposed by Shamir (1979). In this section we describe how to use the Shamir method [1] for conventional secret sharing before describing our approach in the next section. By the Shamir technique, to generate *n* number of shares for a group of *n* secret sharing participants from a secret integer value y for the threshold k, we can use the following *(k-1)*-degree polynomial in the following way.

Algorithm 1: (k,n)-**threshold secret sharing**
Input*:* Secret *d* in the form of an integer, number of participants, and the threshold.
Output: Shares in the form of integers for the participants to keep .
Step 1*:* select randomly a prime number that is greater than *d.*
Step 2*:* Select *k-1* integer values within the range of 0 through *p-1*.
Step 3*:* Select *n* distinct real values *x1, x2,…..,xn.*
Step 4*:* Use the following *(k-1)*-degree polynomial to compute *n* function values, *F(xi)* called the *partial shares* for *i=1,2,……,n, i.e.*, ***F(xi)=(d+c1xi+c2xi2+…+ck-1xik-1)modp … . .(1)***
Step 5*:* Deliver the 2-tuple *(xi,F(xi))* as a *share* to the *ith* participant where *i=1,2,……,n.* The *k* coefficients, namely *d* and *c1*through *ck-1* in *Equation. (1)* above, it is essential to gather at least shares from the *n* participants to form *k* equations of the form of *Equationn. (1)* to solve these *k* coefficients in order to recover the secret *d*. This describes the term *threshold* for *k* and the name *(k,n) -threshold* for the Shamir method [7]. Below is a description of the just-mentioned equation-solving process for secret recovery.

Algorithm 2: Secret recovery
***I*nput**: *k* shares which are collected from the *n* participants and the prime number *p* with both *k* and *p* being those utilized in Algorithm 1.
Output: secret *d* hidden in the shares and coefficients *ci* used in *Equationn. (1)* in Algorithm 1, where *i=1, 2… k-1.*
Step 1*:* Use the *k* shares *(x1, F(x1)), (x2, F(x2))… (xk, F(xk))* to setup ***F(xj) = (d+c1xj+c2xj2+…+ck-1xjk-1)modp …..(2)*** where *j=1, 2 …k.*
Step *2*: Solve the *k* equations above by Lagrange's interpolation to obtain *d* as follows.

$$d=(-1)^{k-1}\left[F(x_1)\frac{x_2x_3\ldots x_k}{(x_1-x_2)(x_1-x_3)\ldots(x_1-x_k)}+F(x_2)\frac{x_1x_3\ldots x_k}{(x_2-x_1)(x_2-x_3)\ldots(x_2-x_k)}+\cdots+F(x_k)\frac{x_1x_2\ldots x_{k-1}}{(x_k-x_1)(x_k-x_2)\ldots(x_k-x_{k-1})}\right]_{\mathrm{mod}p}.$$

Step 3: Compute through by expanding the following equality and comparing the result with (2) in Step 1 while regarding variable in the equality below to be in (2):

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

In the secret recovery algorithm Step 3 is additionally added for the purpose of computing the values of parameters in the proposed method. In remaining applications, only the secret value need be recovered, this step can be eliminated.

3. Authentication of the image And Data Repairing

Here we are Generating the stego Image for Binarazitation to receiver. 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 the 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. Two block diagrams for generating PNG image with self repairing capability are shown below:

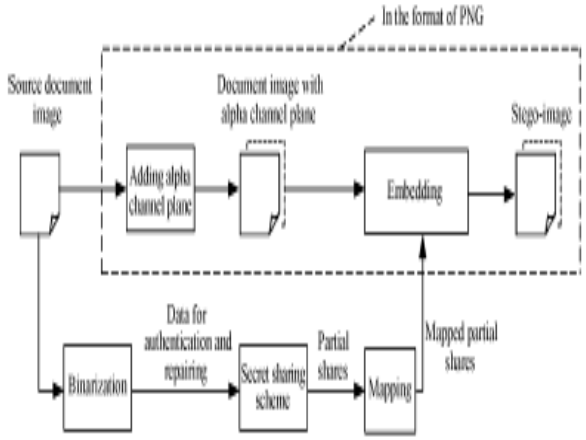

Figure 1: Illustration of creating a PNG image from a grayscale document image and an alpha channel.

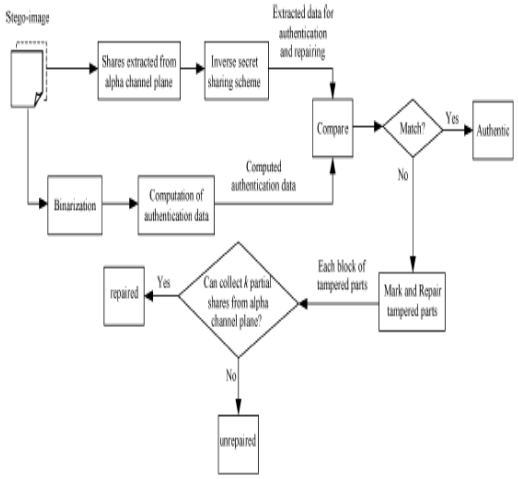

Figure 2: Authorization procedure including verification and self-repairing of a stego-image in PNG format.

4. Results

Figure 3: Authorization result of an image of a Cheque in PNG format (a) Original cover image. (b) Binarized imageof original image. (c) original image combined with alpha channel. (d) Original image in Stego PNG format.

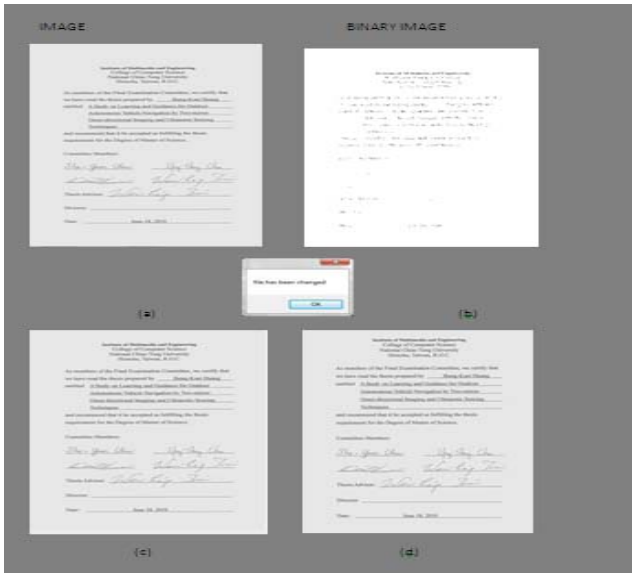

Figure 4: Authorization result of a document image of a Cheque in the form of PNG tampered image with image editor. (a) Original cover image (which is edited one). (b) Binarized image of edited image. (c) Alpha channel plane of edited image. (d) Edited image which is in Stego PNG format**.**

Table1: Comparison of document image authentication methods.

	Distortion in stego-image	Tampering localization capability	Repair capability	Reported authentication precision	distribution of authenticated image parts	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 [8]	Yes	Yes	No	64×64 block	Entire image	Pixel replacement
Proposed method	No	Yes	Yes	2×3 block	Entire image	Alpha channel pixel replacement

Comparison of the capability of the proposed method with those of four existing methods is shown in Table1. All the proposed method will create alteration in the stego-image during the authentication process. More significantly, only the proposed method has the capability of repairing the tampered parts of an authenticated image.

5. Conclusion

A new blind image authentication technique with an information repair capability for binary-like grayscale document images based on secret sharing technique has been proposed. The generated authentication signal and also the content of a block are converted into partial shares by using shamir technique, that are then dispersed in a well designed way to make a stego image with in the PNG format. The unwanted opaque result visible within the stego-image returning from embedding the partial shares has been excluded by mapping the share values into a low range of alpha channel values close to their most transparency value of 255. In the procedure of image block authentication, a block within the stego-image has been thought to be having been tampered with if the computed authentication signal doesn't match that extracted from corresponding partial shares within the alpha channel plane. Experimental results have been shown to prove the efficiency of the proposed method.

6. Future Scope

Future studies could also be directed to decisions of alternative block sizes and connected parameters (prime range, coefficients for secret sharing, range of authentication signal bits, etc.) to boost data repair effects. Applications of the projected technique to the authentication and also the repairing of attacked color pictures may be conjointly tried.

References

[1] Che-Wei Lee and Wen-Hsiang Tsai "A Secret-Sharing-Based Method for Authentication
[2] of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability", Student Member, IEEE, , Senior Member, IEEE, January 2012.
[3] H. Y. M. Liao and C. S. Lu, "Multipurpose watermarking for image authentication and protection," IEEE Trans. Image Process., vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[4] A.C. Kot and H. Yang, "Pattern-based data hiding for binary images authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.
A.M. Tekalp,G. Sharma, E. Saber and M. U. Celik, "Hierarchical watermarking for secure image authentication with localization," IEEE Trans. Image Process., vol. 11, no. 6, pp. 585–595, Jun. 2002.
[5] S. H. Sun, D. G. Xu, and Z. M. Lu, "Multipurpose image watermarking algorithm based on multistage vector quantization," IEEE Trans. Image Process., vol. 14, no. 6, pp. 822–831, Jun. 2005.
[6] Y. Park, H.Kim, and Y. Lee "A new data hiding scheme for binary image authentication with small image distortion," Inf. Sci., vol. 179, no. 22, pp. 3866–3884, Nov. 2009.
[7] B. Liu and M. Wu, "Data hiding in binary images for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.
[8] W.H.Tsai and C.H.Tzeng, "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.

Author Profile

P. Sujitha received the bachelor's degree in Computer Science & Engineering in 2011 from Jntu Anantapur. She is currently pursuing the master's degree in CSE in the college of JNTUACEP.

Sri G.Murali He is an associate professor at the Jntu college of Engineering, Pulivendula, Kadapa, Andhra Pradesh, India. He has eight years of experience. He published so many national and international papers. His research interests include computer networks, quantum computing and Cloud Computing.