IJRRECS/April 2014/Volume-2/Issue-4/2182-2187 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EXPOSURE TOWARDS VALIDATION OF GRAY-SCALE DOCUMENT IMAGES

V.Sudha Rani[1], Venkatarami Reddy[2]

[1]M.Tech Student, Dept of CSE, Gitam University, Hyderabad, A.P, India

[2]Assistant Professor, Dept of CSE, Gitam University, Hyderabad, A.P, India

ABSTRACT:

In practical applications, the documents of text are regularly digitized and set aside as images of gray-scale for later on visual inspection. Document images are regularly digitized into images of gray scale by means of *two* main gray values such as the background which including for the most part of blank spaces and the foreground which includes mainly texts. A method is intended for the validation of document images by means of an additional self-repair capacity for fixing the data of tampered image. Secret sharing in addition to data hiding intended for image authentication are two inappropriate issues in the domain of information protection. The method which is introduced outcomes in a stego-image in the format of portable network graphics, which, in regular cases, will not be additionally compressed, reducing the prospect of invalid authentication caused by means of imposing operations of undesired compression on the stego-image. To expand a technique of new image authentication, in the proposed method, we combine the concepts of secret sharing in addition to data hiding intended for image authentication.

Keywords: Document images, Data hiding, Stego-image, Secret sharing.

1. INTRODUCTION:

The problem of image authentication is tricky for a binary document image for the reason that of its effortless binary nature that leads to noticeable changes subsequent to authentication signals are embedded in the

pixels of image. A superior explanation to binary image authentication has to take into description not merely the issue of security of putting off image tampering but also the requirement of maintaining the visual quality of the ensuing image [4]. Document images including texts, tables, and so on as main contents, are regularly digitized into images of gray scale by means of *two* main gray values such as the background which including for the most part of blank spaces and the foreground which includes mainly texts. The images, even though gray valued in nature, resembles binary. The images of *binary-like* gray scale document may possibly be threshold into binary ones intended for later processing, but such an operation of thresholding frequently destroys the smoothness of the boundaries of text characters, ensuing in visually disagreeable stroke appearances by means of zigzag contours [8]. Hence in practical applications, the documents of text are regularly digitized and set aside as images of grayscale for later on visual inspection. In the self-repairing of the original image information, another problem encountered is that the data to be entrenched in the *carrier* are regularly large sized. With the channel of alpha as the carrier is no more a problem since the cover image that we deal with is fundamentally binary-like, and consequently, just embedding into the carrier a version of binary of the cover image including greatly less data [1]. Through a careful plan of authentication signals, an appropriate choice of the essential authentication unit and a superior adjustment of the parameters in the scheme of Shamir, we can decrease the data volume of the produced shares successfully with the intention that more shares can be entrenched into the alpha channel plane [11]. By the proposed method, the well-built the number of shares is, the superior the resulting data repair ability. The *multiple* shares are distributed randomly into the alpha channel to permit the share data to have great chances to endure attacks and to consequently endorse the data repair ability. This is the initial method of *secret-sharing-based* authentication intended for the images of binary-like gray scale document [3]. It is also the initial authentication method intended for such document images all the way through the usage of the *PNG image*. This method is *not* a method of secret-sharing *but* a method of document image authentication.

2. METHODOLOGY:

A method is intended for the validation of document images by means of an additional self-repair capacity for fixing the data of tampered image. The *cover image of input* is supposed to be a binary-like grayscale image by means of two major values of gray. After the application of the proposed method, the cover image is altered into a *stego-image* in the format of Portable Network Graphics with an extra *alpha channel intended* for transmission on networks [9]. The receving of stego-image, may be confirmed by means of the proposed method for its validity. The modifications of integrity of the stego-image is noticed by the method at the *block* level and restored at the *pixel* level. The alpha channel is completely removed from the stego-image, the total resulting image is observed as inauthentic, implying that the fidelity confirm of the failure of image [7]. The introduced method is on the basis of scheme of so-called-threshold secret sharing in which a secret message is changed into *shares* for keeping by means of participants, and when of the shares, not essentially are assembled, the undisclosed message can be recovered *losslessly*. Such a scheme of secret sharing is constructive for reducing the hazard of incidental partial data loss. The concepts of secret sharing in addition to data hiding intended for image authentication are two inappropriate issues in the domain of information protection. In the proposed method, we combine them collectively to expand a technique of new image authentication. The scheme of secret sharing is used in the developed system not only to hold authentication signals in addition to image content information but also to assist repair tampered data all the way through the usage of shares [2]. A distress in the self-repairing of interfered information at the parts of attacked image is that, subsequent to the original data of the cover image are entrenched into the image itself for use in the later repairing of data, the cover image is ruined in the first place and the original information are no longer obtainable for the repairing of data, consequences' in an inconsistency [12]. A result to this difficulty is to set in the original image information *elsewhere* devoid of altering the cover image. The method proposed is to put into practice the solution to make use of the *extra* alpha channel in an image of portable network graphics to set in the original image data. The alpha channel of the image of PNG image is initially used for creating a required degree of precision for the image.

Embedding of information into the alpha channel will generate *random* transparency in the ensuing PNG image, generating an objectionable opaque effect [5].

3. AN OVERVIEW OF IMAGE AUTHENTICATION:

A Portable network graphics image is created from a grayscale document image binary-type by means of an alpha channel plane in the proposed method. The original image may be considered as a *grayscale channel plane* of the image of portable network graphics. Data for authentication and restoring are subsequently computed from besides taking as input to the Shamir technique of secret sharing to make shares of secret. The values of share are next mapped into minute range of alpha channel values near the value of utmost precision to generate an effect of imperceptibility [10]. Ultimately, the mapped secret shares are arbitrarily entrenched into the alpha channel intended for the function of endorsing the protection of security in addition to the capabilities of data repair. The block diagram describing the proposed method is shown fig1. For carrying data intended for authentication and repairing, while the alpha channel plane is used no destruction will take place to the input image in the procedure of authentication [6]. Conventional methods of image authentication regularly give up component of image contents, for instance least significant bits or flappable pixels, to hold data used for authentication. The proposed method outcomes in a stego-image in the format of portable network graphics, which, in regular cases, will not be additionally compressed, reducing the prospect of invalid authentication caused by means of imposing operations of undesired compression on the stego-image.

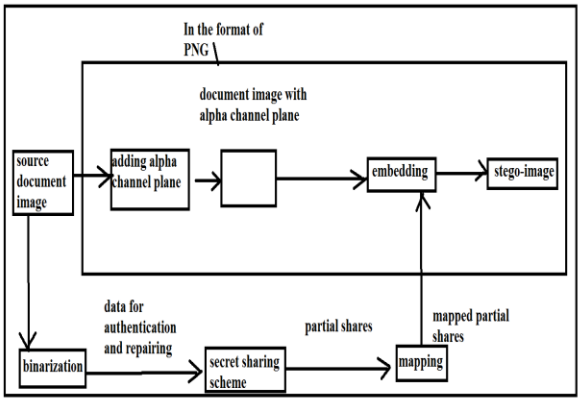

Fig1: An overview of creating a PNG image from the document image of gray-scale as well as an alpha channel.

4. CONCLUSION:

For the validation of document images by means of an additional self-repair capacity for fixing the data of tampered image, a

method is introduced. Subsequent to the application of the introduced method, the cover image is altered into a *stego-image* in the format of Portable Network Graphics with an extra *alpha channel intended* for transmission on networks or archiving in databases. On the basis of scheme of so-called-threshold secret sharing, the proposed method is introduced in which a secret message is changed into *shares* for keeping by means of participants, and when of the shares, not essentially, are gathered and the undisclosed message is recovered *losslessly*. The introduced method put into practice the solution to make use of the *extra* alpha channel in an image of portable network graphics to set in the original image data. By the proposed method, the well-built the number of shares is, the superior the resulting data repair ability. From a grayscale document image binary-type by means of an alpha channel plane in the proposed method, a Portable network graphics image is created.

REFERENCES

[1] Y. Lee, H. Kim, and Y. Park, "A new data hiding scheme for binaryimage authentication with small image distortion," *Inf. Sci.*, vol. 179,no. 22, pp. 3866–3884, Nov. 2009.

[2] H. Yang and A. C. Kot, "Pattern-based data hiding for binary imagesauthentication by connectivity-preserving," *IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007.

[3] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for imageauthentication and protection," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[4] C. C. Lin and W. H. Tsai, "Secret image sharing with steganographyand authentication," *J. Syst. Softw.*, vol. 73, no. 3, pp. 405–414, Nov./ Dec. 2004.

[5] M. Wu and B. Liu, "Data hiding in binary images for authenticationand annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[6] C. H. Tzeng and W. H. Tsai, "A new approach to authentication ofbinary images for multimedia communication with distortion reductionand security enhancement," *IEEE Commun. Lett.*, vol. 7, no. 9, pp.443–445, Sep. 2003.

[7] M. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp, "Hierarchicalwatermarking for secure image authentication with localization," *IEEETrans. Image Process.*, vol. 11, no. 6, pp. 585–595, Jun. 2002

[8] H. Yang and A. C. Kot, "Binary image authentication with tamperinglocalization by embedding cryptographic signature and block

identifier,"*IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec.2006.

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

[10] H. Y. Kim and A. A?f, "Secure authentication watermarking forhalftone and binary images," *Int. J. Imag. Syst. Technol.*, vol. 14, no.4, pp. 147–152, 2004.

[11] W. H. Tsai, "Moment-preserving thresholding: A new approach,"*Comput. Vis. Graph. Image Process.*, vol. 29, no. 3, pp. 377–393, Mar.1985.

[12] Z. M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose image watermarkingalgorithm based on multistage vector quantization," *IEEE Trans. ImageProcess.*, vol. 14, no. 6, pp. 822–831, Jun. 2005.

[13] Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authenticationscheme with small distortion and low false negative rates," *IEICE Trans. Commun.*, vol. E90-B, no. 11, pp. 3259–3262, Nov. 2007.