ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Authentication of Colour Document Images with a Data Fixing Capability using Secret Sharing and Scrambling Approach

Maria Kurian, Joby A Thattil, Deepika M P

Assistant Professor, Dept. of CSE, Ilahia College of Engineering & Technology, Muvattupuzha, Ernakulam, India.

Software Architect, 12 years of Experience in IT, Ernakulam, India.

Assistant Professor, Dept. of CSE, Adi Shankara Institute of Engineering & Technology, Kalady, Ernakulam, India.

ABSTRACT: Digital imagery is protected from malicious attacks through precise authentication techniques. The authentication method proposed in this paper involves a secret sharing technique with data repair capability for colour images using PNG images. Halftoning is applied to the image channels to enable better visual quality of the recovered image. Scrambling is used along with secret sharing to enhance security. If the image is found tampered on authentication, data repair facility is utilized to retrieve the original colour image.

KEYWORDS*:* Secret Sharing,Halftoning,Scrambling.

I. INTRODUCTION

Information's can be preserved easily in the form of digital images. Visual alterations to the contents of the digital images have become very easy with the advancement of digital imaging software's. Visually imperceptible changes to images pose a great challenge in preserving the integrity of the digital image. The integrity and authenticity preservation of a digital image has become a major challenge. It is imperative to design effective methods for such authentication challenges especially of highly secured confidential document sharing. Digital images which are partially damaged or corrupted or illicitly altered should find provision to be repaired and restored. Authentication and self repairing techniques are potent tools which will help preserve and protect digitized images. Digital imagery is used in designing and transferring circuits, banking documents, military confidential documents, etc. Such transfer can lead to malicious attacks damaging the image documents partially or in whole. Methods are devised to check the integrity of the digitized image as it flows through from one target to the other.

Among different kinds of the carrier media available, digital images are the most popularly used data over the Internet. A host image, which is used, to hide the secret data is called the cover image or the carrier image. When the secret data has been embedded into the cover image, the resultant image is called the stego image. Good stego image quality can avoid arousing suspicion during data transmission. The image or message is a collection of pixels, each pixel is handled individually. Halftoning technique provides a means to handle colour images and scrambling technique is introduced to increase the level of security.

II. RELATED WORK

Several methods for binary image authentication have been proposed in the past. Wu and Liu [2] proposes an approach that can hide a moderate amount of data in general binary images including scanned text, signatures etc. The hidden data can be extracted without using the original unmarked image. The approach can be used to verify whether a binary document has been tampered or not. Yang and Kot [4] focuses on data hiding for binary images in lower level for the purpose of image authentication. Authentication watermark is a hidden data inserted into an image that can be used to detect any accidental or malicious alteration in the image. The proposed technique by Kim and Amir [5] is a watermarking scheme for binary/halftone images that detect even a single pixel alteration in the host image. Proposed scheme by Tzeng and W. H. Tsai [6] embeds authentication information into the cover image with flipping only a small number of pixels. This minimizes the visual distortion. Lee and Tsai [1] propose a method for the authentication of document images with an additional self-repair capability for fixing tampered image data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Authors	Advantages	Disadvantages
M. Wu & B. Liu	1. Manual Scoring method is automated to score pixels dynamically. 2. can embed large amount of data	1. Flippablity score lookup table may exceed the available memory size for the large neighborhoods
H.Yang & A.C Kot	1. Locating embeddable pixels in a block for different block scheme are addressed.	1. Difficult to locate tampering occurred at each block.
Hae Yong Kim & Amir Afif	1. Binary/Halftone watermarking is possible.	1. Smaller the host image the more visually noticeable will be the watermark. 2. Printed images cannot be authenticated.
C.H.Tzeng & W.H Tsai	1. Image distortion is reduced	1. There is a trade of between distortion reduction and security enhancement.
Y.Lee,H.Kim & Y.Park	1. Small distortion	1. Limited amount of embeddable data.

Table 1: Comparison table for previous methods

III. PROPOSED ALGORITHM

Data hiding which destroys the cover image and the original image along with it prevents self-repairing capability. A solution to this problem is to embed the original image data somewhere else without altering the cover image itself. An extra alpha channel in a PNG image is utilized to embed the original data image to produce the desired opaque effect for transference across the network.

A binary image can be divided into shares; can then be stacked together to approximately recover the original image. It has not been used, unfortunately, primarily because the decryption process does a severe degradation in image quality in terms of loss of resolution and contrast. Usage is also further hampered by the lack of proper techniques for handling restoration of tampered color images effectively. In this paper, we have developed a new technique which enables color images to be restored while maintaining its visual quality. With the use of halftoning scheme we have restored images to near original, proven by the stunning ratios generated. Scrambling technique is used to enhance the security feature.

The proposed method is based on threshold secret sharing scheme proposed by Shamir in which a secret message is transformed into n shares for keeping by n participants. The authentication process of the stego image includes both verification and self repairing of the original content. The authentication process involves matching the authentication signal against that extracted from the shares embedded in the alpha channel. If a block is found tampered data repairing is applied by reverse Shamir's scheme. The secret sharing scheme is used not only to carry authentication signals and image content data but also in helping repair tampered data through the use of shares. The usage of the alpha channel solves the issue of size factor on the carrier.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

IV. WORKING

PNG image formation with scrambling

A PNG image is created from a binary like colour document image with an alpha channel plane. Three planes are extracted from the colour document image, those being R, G, B planes. Halftoning is used to binarized the R, G, B planes. A raster scan of the binarized image generates pixels which are used to create the 2-bit authentication signal. The extra alpha channel in the PNG image is used to embed the original image which prevents the alteration of the original image. Data for authentication and repairing are computed from the binarized version and taken as input into the Shamir secret sharing scheme to generate secret shares. Generated secret shares are mapped into partial shares which fall in the nearly total transparency range. The partial shares generated are embedded into the alpha channel plane. The process of embedding involves embedding two pixels into a block for each plane and the rest are randomly embedded using the key. The alpha channel generated for the red plane is attached with the original image. Likewise the alpha channel generated for the G and B plane are attached to a black and white image respectively. This generates the stego image for each of the planes separately. Scrambling technique is applied on the stego image generated for the plane with the original image with a key.

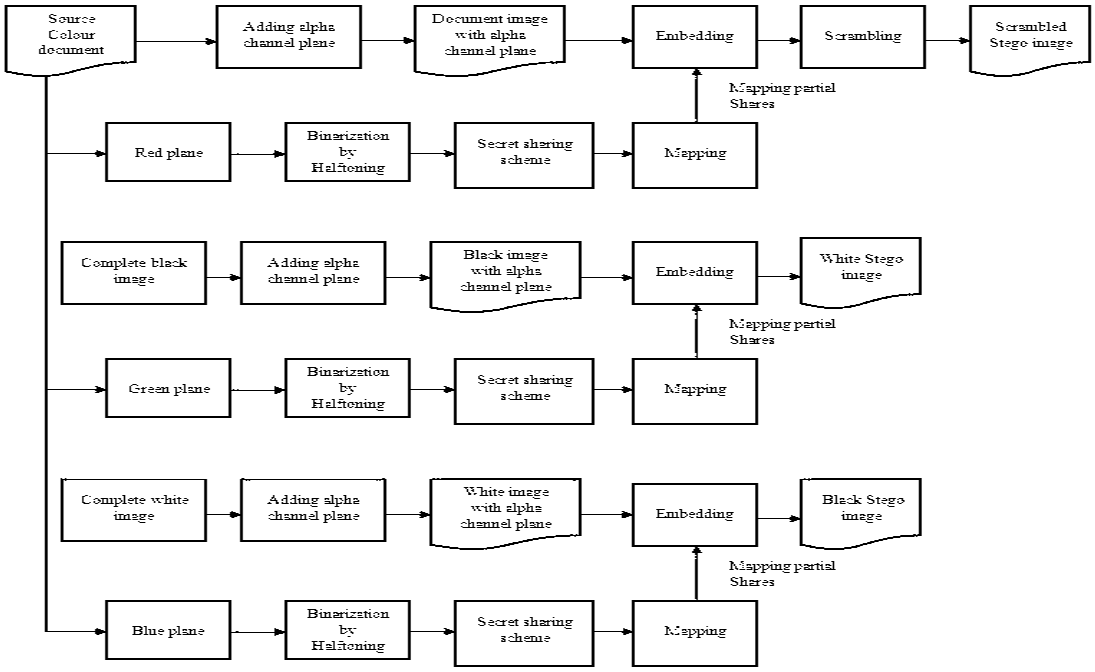

Fig.1. Illustration of creating a NG image

Authentication and self repairing of stego image

The Authentication process of the stego image includes both verification and self repairing of the original content. The scrambled stego image is descrambled with the help of the key. Three channels are extracted and binarized with the help of halftoning. The authentication signals are computed for the planes. The shares are extracted from the alpha channel of the three stego images and inverse secret sharing is applied to generate the authentication signals. Matching of the authentication signals is performed and those that mismatch are marked as tampered individually from the three planes. Those blocks which are marked as tampered in the alpha channel are used to repair the data that is corrupted in the original image. Inverse halftoning is applied to repaired images of the individual planes. Three of the images from the respective planes are combined to give the original colour document image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

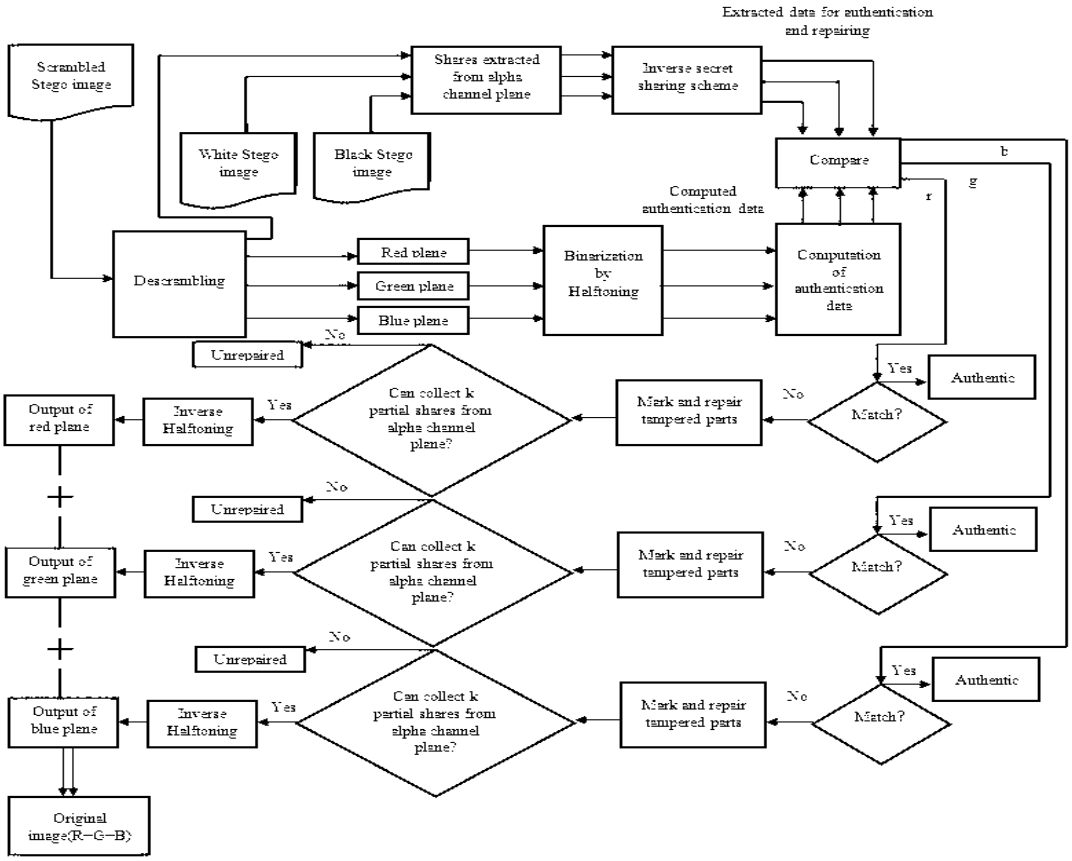

Fig 2: Authentication process including verification and self-repairing of stego-image

V. PSEUDO CODE

1. Formation of PNG image

Step 1: Three planes of the colour document image I is get extracted
Step 2: Binarization of three planes by halftoning
Step 3: Segment the binarized red plane into 2×3 blocks
Step 4: Create authentication signals for each block, s=a1a2
Step 5: Generate partial shares with the help of secret sharing, qi=F(xi)=(d+c1xi) mod p
Step 6: Map the partial shares, Add 238 to each of q1, q2,… q6 to get q'1, q'2, q'3,q'4,q'5,q'6
Step 7: Embed two partial shares in the current block q'1, q'2
Step 8: Embed remaining partial shares at random positions of alpha channel q'3,q'4,q'5,q'6
Step 9: Repeat the same for entire plane
Step 10: Embedded alpha channel is attached with the Original image
Step 11: Generated stego image is scrambled with the help of a key
Step 12: Generate a black and white image of the same size of original image
Step 13: Segment the binarized green plane into 2×3 blocks
Step 14: Create authentication signals for each block, s=a1a2 where
Step 15: Generate partial shares with the help of secret sharing, qi=F(xi)=(d+c1xi) mod p
Step 16: Map the partial shares, Add 238 to each of q1, q2,…, q6 to get q'1,q'2,q'3,q'4,q'5,q'6
Step 17: Embed two partial shares in the current block q'1,q'2
Step 18: Embed remaining partial shares at random positions of alpha channel q'3,q'4,q'5,q'6

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Step 19: Repeat the same for entire plane
Step 20: Embedded alpha channel is get attached with the white image
Step 21: Segment the binarized blue plane into 2×3 blocks
Step 22: Create authentication signals for each block, s=a1a2 where
Step 23: Generate partial shares with the help of secret sharing, qi=F (xi) = (d+c1xi) mod p
Step 24: Map the partial shares, Add 238 to each of q1, q2,…, q6 to get q'1,q'2,q'3,q'4,q'5,q'6
Step 25: Embed two partial shares in the current block q'1,q'2
Step 26: Embed remaining partial shares at random positions of alpha channel q'3,q'4,q'5,q'6
Step 27: Repeat the same for entire plane
Step 28: Embedded alpha channel is get attached with the black image

Algorithm 1: PNG image formation algorithm

2. Authentication and self-repairing of the Original Image Content

Step 1: Descramble the stego image and extract the three planes
Step 2: Binarization of three planes by halftoning
Step 3: Segment the binarized planes
Step 4: Compute authentication signals, s'=a1'a2'
Step 5: Extract the shares from alpha channel of all the three stego images
Step 6: Subtract 238 from rest of shares
Step 7: Apply the inverse secret sharing
Step 8: Extract authentication signals, s=a1a2for each block
Step 9: Matching of the hidden and computed authentication signals, s=s'
Step 10: Extract from remaining partial shares and repeat the same
Step 11: If the authentication signals get match then it is authenticated
Step 12: If not collect the k partial shares and repair the tampered regions
Step 13: If not possible to repair remain as untampered same for all the three planes
Step 14: After repairing of the three planes apply inverse halftoning for three planes
Step 15: Combine the three planes and get the original image

Algorithm 2: Authentication and self repairing algorithm

VI. SIMULATION RESULTS

System testing is the process of performing a variety of tests on a system to explore functionality of the system or to identify problems. System testing is required before and after a system is put in place. Testers often try to "break the system" by entering data that may make the system to malfunction or return incorrect information. System testing is a more limited type of testing; it seeks to detect defects both within the "inter-assemblages" and also within the system as a whole. When testing is performed a series of systematic procedures are referred.

	Distortion in stego image	Tampering localization capability	Repair capability	Reported authentication precision	Distribution of authenticated image parts	Manipulation of data embedding
M. Wu & B. Liu	Yes	No	No	Macro block	Non-blank part	Pixel Flippablity
H.Yang & A.C Kot	Yes	Yes	No	33x33 block	Non-blank part	Pixel Flippablity

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Hae Yong Kim & Amir Afif	Yes	No	No	Reported authentication precision	Non-blank part	Pixel Flippablity
C.H.Tzeng & W.H Tsai	Yes	Yes	No	Macro block	Entire image	Pixel Flippablity
Proposed method	No	Yes	Yes	2x3 block	Entire image	Alpha channel pixel replacement

Table 2: Comparison of document image authentication methods

Item	Test description	Test result pass/ fail	NCPR	UACI	PSNR
Test case 1	Colour,708x310	Pass	93.07	34.5	25.89
Test Case 2	Colour,256x256	Pass	94.70	34.57	26.21
Test Case 3	Gray,708x310	Fail	……	……..	……..

Table 3: Ratio Comparison

Item	Test description	Detection ratio
Test case 1	Colour,708x310 Equating authentication signal	88.91
Test case 2	Colour, 708x310Equating authentication signal + six pixels	100

Table 4: Experimental improvements

VII. CONCLUSION AND FUTURE WORK

A well defined alpha channel in the PNG image helps to embed shares and transfer them across a network. The self repairing capability of a tampered stego image with the partial shares embedded in the alpha channel is a great advantage. The main advantage is that it provides pixel level repairement of tampered image parts, so that if distortion happens to the original image it can be recovered. It also makes use of a new type of image channel for data hiding. This avoids hiding of information in the original image. Having higher possibility to survive image content attack, enhancing the data security by using secret sharing scheme. Inverse halftoning technique generates better visual quality images of tampered image. Scrambling technique is used to enhance the security of the process. Colour images are hence secure and restoration is effective. Detection ratio was improved. PSNR has considerably improved by using the inverse halftoning method. The proposed method has resolved many outstanding issues from the past. The use of the alpha channel reduces the size overload on the carrier and also provides a medium to store the original image thereby helping in the self repair capability. Comparison study of the PSNR ratios between various halftoning techniques can be done to ascertain the effectiveness of the chosen technique. Data repair effects can be improved by choosing different block sizes and adjusting related parameters like (prime number, coefficients for secret sharing, number of authentication signal bits, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

REFERENCES

1. Che-Wei Lee and Wen-Hsiang Tsai, "A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability"IEEE Transactions on Image Processing, Vol. 21, no. 1, January 2012
2. 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.
3. H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Process. Lett. vol. 13, no. 12, pp. 741–744, Dec.2006.
4. 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.
5. H. Y. Kim and Amir Afif, "Secure authentication watermarking for halftone and binary images," Int. J. Imag. Syst. Technol., vol. 14, no. 4, pp. 147–152, 2004.
6. 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., Sep. 2003.
7. Y. Lee, J. Hur, H. Kim, Y. Park, and H. Yoon, "A new binary image authentication scheme with small distortion and low false negative rates," IEICE Trans. Commun., vol. E90-B, no. 11, pp. 3259–3262, Nov. 2007.
8. W. H. Tsai, "Moment-preserving thresholding: a new approach," Computer Vision, Graphics, and Image Processing, vol. 29, no. 3, pp. 377-393, 1985.
9. C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Trans. on Image Processing, vol. 10, issue. 10, pp. 1579–1592, Oct. 2001.

BIOGRAPHY

Maria Kurian is a Research Assistant Professor in the Computer Science Engineering Department, Ilahia College of Engineering and Technology, Affiliated to Mahatma Gandhi University, Kottayam. She received Master of Technology(M.Tech.) degree from Adi Shankara College of Engineering.

Joby A Thattil is a Software Architect and has worked in many leading MNC's in India and in the US. He has over 12 years of experience in the IT field. He is a B.E from Bharadhidasan University.

Deepika M P is a Research Assistant Professor in the Computer Science Engineering Department, Adi Shankara Institute of Engineering and Technology, Affiliated to Mahatma Gandhi University, Kottayam. She received Master of Technology(M.Tech.) degree in Software Engineering. Pursuing PhD in Visual Crytpograhy from CUSAT.