IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Authentication of Grayscale Images and Data Repairing Using Secret Sharing Method

Kimaya Phadtare[1], Niharica Nakure[2], Sharon Anthony[3], Vijayalaxmi Jagdale[4], Professor Sunil Rathod[5]

BE Student, Computer Department, Dr. D Y Patil School of Engineering, Pune, India [1, 2, 3, 4]

Professor, Computer Department, Dr. D Y Patil School of Engineering, Pune, India[5]

Abstract: To protect classified& important data digital images are used. Providing authentication, veracity and data safety to these digital images seems to be difficult. In current practices of giving security and authentication, conventional watermarking schemes are in use. Cryptography is taken up in these techniques which prove to be of no use in granting protection from hackers tampering the information. This paper puts forth a new proficient authentication method for grayscale document images making use of the Portable Network Graphics (PNG) image and data repair capability. Each block of a grayscale document image generates an authentication signal in this method and then, by using Shamir secret sharing scheme, authentication signal and binarized block content is pooled and altered into multiple numbers of shares after which they come together and combine into an alpha channel plane becoming the PNG image. This resulting layer is then formed into a stego image. For authentication purposes this stego image is sent to the receiver. If the received grayscale image is tampered, reverse Shamir's secret method is applied to repair the tampered image.

Keywords: Data repair capability, grayscale document image, Cryptography, Portable Network Graphics (PNG) image, Shamir secret sharing scheme, Alpha layer, stego image.

I. INTRODUCTION

Authentication of the digital credentials are needed in a huge variety of application areas such as legal documents, official documents alongside significant records such as fax insurance and personal records which is afterward digitized and stocked. Amplified computerized technologies make it easy to influence digital images without noticing changes, ensuing unlawful tampering of over send images.

Effective ways should be designed to solve the image authentication dilemma, especially when it comes to images of the classified data. Therefore, uncovering of forged image is of chief concern. Image processing is a practice that entails the study and manipulation of a digitized image to develop its level of brilliance. Shamir's secret algorithm is used in this paper for providing the authentication signal and obtaining several shares 'k'. In this epoch, usage of enhanced technologies, it is likely to modify the data of these digital images.

Hence it is required to look after its hypothecation. For binary document images, it is hard to authorize because of its clear-cut binary nature which directs to traceable alterations after authentication signal are engraved in the image pixel. This gives us the perfect reason to propose authentication of grayscale document images.
Grayscale images are known to be high resolution binary images, ergo it is also called as binary like gray scale image. These images modify the visual quality restriction of binary certificates. In the following paper, a new procedure is used for confirmation of document images with an added self data repairing capacity for fixing tampered images. The input image is received as binary like grayscale image.

II. RELATED WORK

The related work gives us the information and techniques that are required to implement the proposed paper. We have studied the following listed existing papers to get a better understanding of the algorithms used. Most of the existing systems show a variety of schemes for authentication of grayscale document images. One such scheme put forward by Pradnya Kadam [1] recommends Shamir's secret sharing scheme for the authentication purposes and the reverse Shamir's secret scheme for data repairing.

Similarly K.M.Aldar [2] proposes the method of binarization for gaining the grayscale illustration of the image. The image is used in the system which executes authentication with use of alpha channel and Shamir's secret sharing scheme creating a stego- image which gives severe cover up of data. This is how the authentication of jpeg and PNG images is accomplished.

The analysis of the techniques used for the authentication of grayscale images, for instance, Shamir's secret sharing scheme, is studied by Che-Wei Leethe [3] His proposed technique shows the usage of Shamir's secret sharing method and Stegnography for the authentication and extreme concealment or encryption of the data.

Ms. K.Siva Shalini [4] proposed a system which executes authentication of the document images by implementing Shamir's secret sharing scheme in which the RGB image is taken as input and creates a stego image as the output providing a high cover of the data. A Secure Authentication method for Grayscale document images 'has been proposed by M. Mahalakshmi [5], involving the implementation of alpha channel, providing security for input image.

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Table 1: Existing techniques at glance

Sr No.	Paper	Author	Implementation methods used
1	Shamir Secret Sharing Method for Authentication of Colored Document Image with Self Repair Capability	Miss. Pradnya Kadam.Miss. Nishigandha Khandagale. Miss. Poonam Yadav Prof. Sarla A.Chimegawe	Shamir's Secret Scheme for image authentication.
2	Image authentication for png and jpeg images with data repair capability	Mr.K.M.Aldar, Prof.A.N.Mulla	Binarization and Alpha channel plane, Shamir Secret Algorithm.
3	A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image with a Data Repair Capability	Che-Wei Lee, IEEE and Wen-Hsiang Tsai,	Shamir's secret sharing method and Steganography
4	Authentication of grayscale document images using shamir secret sharing scheme.	Mrs.G.Niranjana,Ms.K.Siva Shalini	Image authentication through Shamir Secret Scheme
5	A Secure Authentication Method for Grayscale Document Images	M.Mahalakshmi, C.Callins Christiyana	Alpha Channel Plane, Steganography, Secret Sharing Scheme
	Secure Image Authentication of a Grayscale Document using Secret Sharing Method and Chaotic Logistic Map with Data Repair Capability	S Kavitha Murugesan, Shanavas K A	Design and embedding of shares
7	A Secret Data Hiding and Repairing of Grayscale Document Images with Generation of Authentication Signals	Reddypatil Ashwini G1, Prof. V.R.Chirchi2	Embedding phase &Extraction Phase In the proposed system
8	Authentication of Gray Scale Document Images via the Use of PNG Image with Data Repairing	P. Sujitha1, G. Murali2	(k,n)-threshold secret sharing

Later on, this image goes through the authentication system which uses Shamir's secret sharing scheme. Stegnongraphy is used to obtain a stego image. In this way secure authentication for grayscale document images is implemented here. Secure Image Authentication of a Grayscale Document using Secret Sharing Method and Chaotic Logistic Map with Data Repair Capability' is a paper proposed by S Kavitha Murugesan and Shanavas K A [6]. In this paper, an authentication system for grayscale images is put forth which uses secret Shamir and chaotic logistics mapping for security and data repair capability, respectively. This method has the embedment and design of shares used effectively.

A Secret Data Hiding and Repairing of Grayscale Document Images with Generation of Authentication Signals paper shows us the efficient usage of Embedding phase & Extraction Phase in the proposed system. The authors Reddypatil Ashwini and Prof. V.R. Chirchi [7] have proposed a system for authentication for grayscale images with the generation of authentication signal and also the repair capability successfully. Authentication of Gray Scale Document Images via the Use of PNG Image with Data Repairing' paper proposes a method where the authentication is provided using the Png images with data repair capability. P.Sujitha and G. Murali [8] have used the (k, n)-threshold secret sharing method which is used in provided the security and recovers the original image.

III.PROPOSED SYSTEM IMPLEMENTATION

Proposed system is mainly divided into two phases:

1] Embedding phase
2] Extraction phase

1] EMBEDDING PHASE CONSISTS OF THE FOLLOWING PROCESSES:

Image collection: Images are composed from diverse obtainable databases. One separate database is reserved for the proposed work. Images from this database are needed to be sent to the authentication system consisting of the alpha channel plane and Shamir's secret algorithm. The system also has the ability of embedding of the image which will later form in the PNG format.

Data Pre-processing: Pre-processing being the primary step in the validation of image, this phase is essential to enhance the quality of the image for making the feature extraction phase more dependable. Noise is one of the most frequent troubles in image processing for which techniques such as binarization and median filtering are taken into consideration. RGB images are the input acceptable images transformed to Gray-scale images by using algorithms such as Shamir's secret scheme in order to gain the embedded stego image.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Binarization: A method of binarizing an image by removing brightness (density) as a trait from the image is binarization. On the selection of a pixel in an image, a sort of sensitivity is added to and/or subtracted from the value relating to the Y value of the chosen pixel to set a threshold value range. On selection of another pixel, the sensitivity is again added to or subtracted from the value

Input Image Adding with Alpha Channel Plane: By combining with alpha channel plane and obtaining a new image layer, an input grayscale document image transforms in a PNG image.

Generation of authentication signals: We use the procedure of image binarization for the authentication of signals that switches the input color image into a format that is readable by the computer. To acquire two representative gray values namely g1 and g2, by averaging values of the RGB, these binarized images are used with moment preserving threshold.

Creation and embedding of shares: The shamir's secret algorithm divides the images into equal number of blocks. Each block contains of six shares, two shares out of the six are embedded in the current block with other four shares being embedded randomly at selected pixels outside the block. This process is known as 'Mapping'. Stego-image is obtained after mapping and sent to the receiver.

Embedding: Subsequent step is to embed the shares of each block of the grayscale image into alpha channel plane. Values of generated shares are mapped with alpha channel plane for the transparency range of alpha channel plane. A block in alpha channel is taken with an image corresponding to block of binary image, then choose the first two pixels in alpha channel and embed the image with the pixels of binary image. Last four pixels are embedded using a key. This process goes on until end of number of blocks.

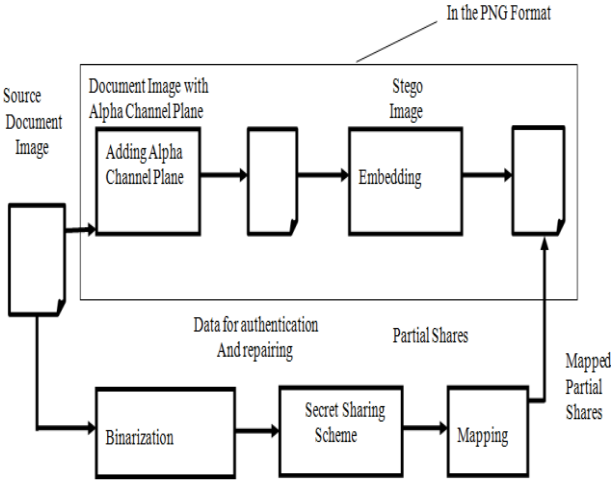

Figure 1(a): System architecture (sender side)

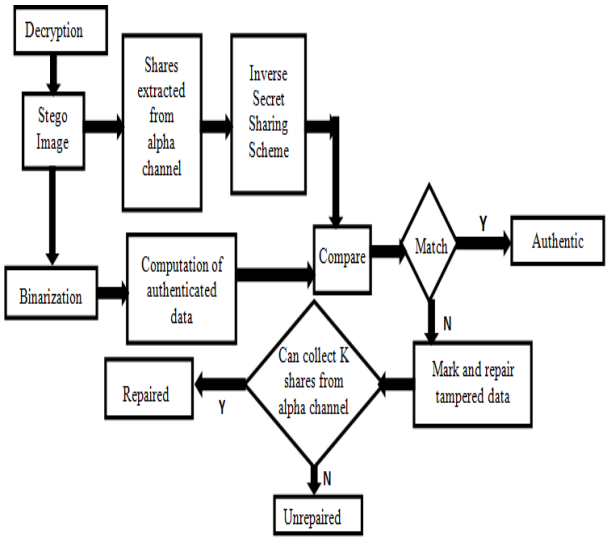

Figure 1(b): System architecture (receiver side)

IV. ALGORITHM USED

2] EXTRACTION PHASE CONSISTS OF THE FOLLOWING PROCESSES:

Authentication and verification of a stego-image: Two Gray level values are used to produce a secret key. Binarized Stego image and the authentication signals gained from it are weighed against the extracted data for validation. The alpha channel plane of given stego image is useful in repairing. The block is valid and verified when it matches the original source document image or else in the other case the recovery algorithm is used to obtain the repaired image from tampered image.

Self-repairing Capability of Tampered Block: If particular block is tampered it means that two shares which were embedded in the current alpha channel plane are changed or lost. For mending, out of the six partial shares of stego image choose two shares of input image which are not ruined. These shares help to apply reverse secret sharing scheme and repair tampered blocks.

Two algorithms are used inShamir Secret Sharing method which is as follows:

Algorithm 1:
An input secret d in form of an integer is converted into shares and then they are dispensed to n participants and the threshold of k <= a prime number p should be considered. Choose arbitrarily, a prime number p which superior than d. Select k-1 integer values a1, a2…..ak-1 within the range of 0 to p-1. Later on partial shares are created. It's needed to collect at least k shares from n participants to form k equations to recover the secret d.

Algorithm 2:
The input for secret recovery are k shares which are collected from n participants, the prime number p with both k and p both being those used in algorithm-1.
The secret d is buried in the shares.
Image Authentication and Data Repairing use the following algorithm:

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Algorithm 3:
The Generation of Stego Image in PNG format from a given grayscale image: A grayscale document image I is the input and has two major gray values with the secret key k. Generation of authentication signal comprises image binarization, altering the cover into PNG format and creation of legalized signals. Construction and embedding of shares is completed by Partial share generation, then mapping of the partial shares, embed two of the partial shares in the current block and the residuals are embedded at random pixels.

Algorithm 4:
Authentication of a given stego image in the PNG format. First Remove the two embedded representative gray values and binarized the stego image. Then verify of the Stego image. Lateral match the unseen and computed authentication signals and mark the tampered block. Self-repairing of the tampered areas is then completed by applying the Reverse Shamir Secret Algorithm.

V. EXPERIMENTAL RESULT

The image given below shows the usage of secret image sharing method with the results of recovered images. When compared, there is no error between the original image and recovered image. An input binary grayscale image is passed in order to generate n secret shares on using Shamir's secret sharing scheme. Mapped secret shares are merged with alpha channel plane to create a PNG image. Figure 2 shows the original colour image to be processed.

Figure 2 shows the original colour image to be processed.

Figure 2: Original Image

Figure 2(a) shows the input original image which has been converted into binary grayscale after the binarization process.

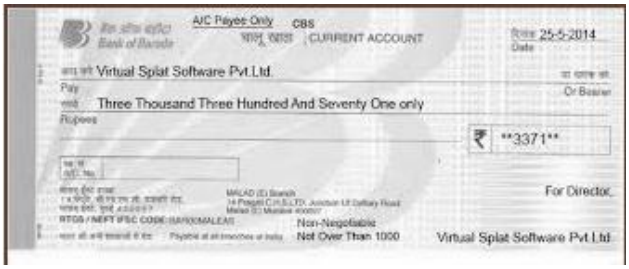

Figure 2(a): Binary grayscale input in PNG format

Figure 2(b) shows the generation of stego image that can be verified by the proposed method for its verification and validation.

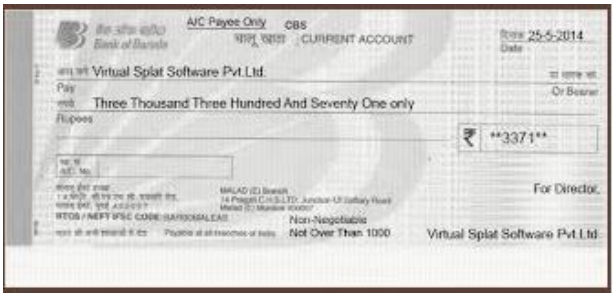

Figure 2(b): Stego image

Figure 2(c) shows how the sourcedocument image has been tampered and modified by the malicious attacker.

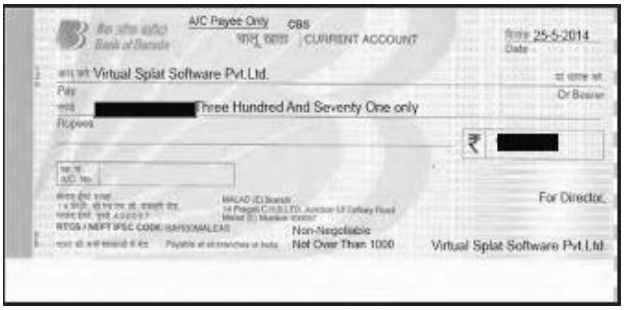

Figure 2(c): Modified image

Figure 2(d) shows how the image has been corrupted by adding noise into it which leads to the distortion of the original image.

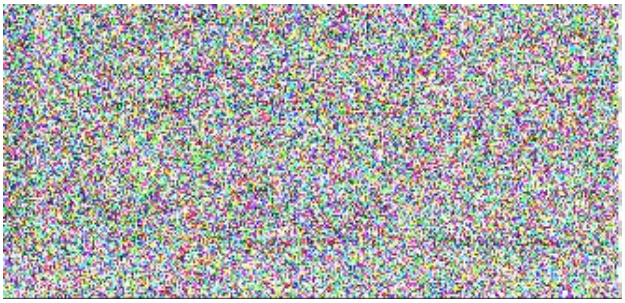

Figure 2(d): Noise image

Figure 2(e) shows the implementation of reverse shamir's secret algorithm where the tampered image has been repaired and the original image is recovered.

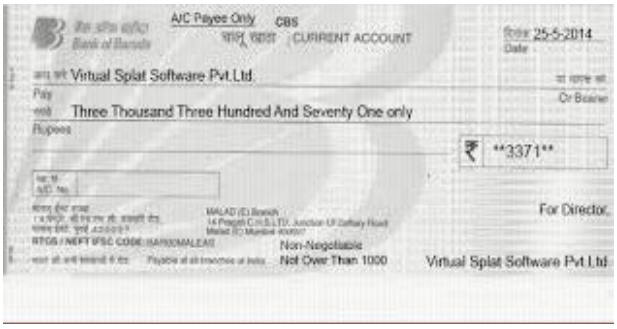

Figure 2(e): Recovered image

Figure 2(f) shows that the image has been repaired successfully.

DOI 10.17148/IJIREEICE.2016.4567

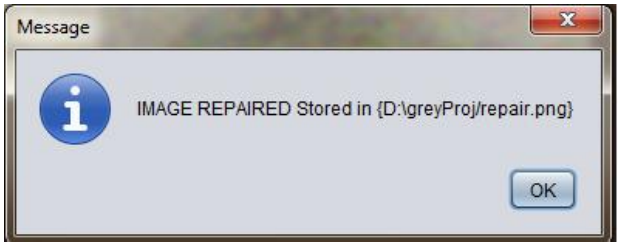

Figure 2(f): Image repaired dialog box

Table-2: Experimental Result

Image ID	Image size	No.of blocks	Type of attacks	No.of tampered blocks	No.of repaired blocks
1	225*225	8400.0	noising	8400.0	8400.0
2	152*332	8360.0	tampering	298.5	298.5

Peak signal to noise ratio(PSNR): 7.702293264477631

VI. FUTURE SCOPE

Future studies could also be directed to assessments of unconventional block sizes and connected parameters (prime range, coefficients for secret sharing, range of authentication signal bits, etc.) to advance data repair effects. Appliance of the projected method for authentication and for repairing the attacked color pictures may be tried together.

VII. CONCLUSION

In this paper, we put forward an authentication method and data repair capability for colour images based on Shamir's secret sharing. For each block of each grayscale channels of RGB image, an authentication signal is generated. These blocks are joined with binarized block data and modified to numerous shares using Shamir's secret scheme. And at receiver side, Reverse Shamir secret scheme to repair the tampered image is used. In this way original image is recovered.

REFERENCES

[1] Authentication of grayscale document images using Shamir secret sharing scheme. 1Mrs.G.Niranjana, M.Tech (Asst.prof), 2Ms.K.Siva Shalini, M.Tech .International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 1 –Nov 2013.

[2] Shamir Secret Sharing Method for Authentication Of Colored Document Image with Self Repair Capability Miss. Pradnya Kadam1 Miss. Nishigandha Khandagale2 Miss. Poonam Yadav3 Prof. Sarla A.Chimegawe4 .IJSRD-International Journal for Scientific Research & Development Vol. 3, Issue 02, 2015.

[3] 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 data repair capability" IEEE Trans. Image Processing., vol.21, no.1, january.2012.

[4] Image Authentication For PNG And JPEG Images with Data Repair Capability Mr.K.M.Aldar1, Prof.A.N.Mulla2. International Journal of Advance Research In Science And Engineering. IJARSE, Vol. No.3, Issue No.8, August 2014.

[5] A Secure Authentication Method for Grayscale Document Images IM.Mahalakshmi, IIC.Callins Christiyana. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014).

[6] Authentication Method for Document Type Colour Images with Data Repair Capability Miss. AshwiniV. Kurzekar, Dr. A. R. Mahajan. International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5), 2014.