A Secret Data Hiding and Repairing of Grayscale Document Images with Generation of Authentication Signals

Reddypatil Ashwini G[1], Prof. V.R.Chirchi[2]

[1]PG Student, MBES College of Engineering Ambajogai
[2]Asst.Professor, PG Department, MBES COEA.

Abstract- With fast advance digital technology image processing is fastest and secure area of research and technology. To hiding a data and repairing with generation of authentication signal are big challenges. To overcome a problem of security a new method is used a secret data hiding and repairing of grayscale document images with generation of authentication signals. An authentication signal is generated for each 2x3 block of input grayscale document image. For generation of authentication signal a grayscale document image content need to binarized. These binarize content transferred into number of share by using Shamir secret sharing scheme. A new plane is used for data hiding called alpha channel plane. This plane adding input grayscale document image to form a Portable Network Graphics (PNG) image which is easy to communication in network. At the time of embedding computed secret values called shares mapped with range of alpha channel plane values. At the receiver side process of image authentication one of the block of image marked as tampered if authentication signal of extracted from alpha channel plane not match with the current block content. Need to repaired tampered block by applied reverse Shamir secret sharing scheme.

Index Terms- Data Hiding, Data repairing, PNG, Alpha Channel, Image authentication, Grayscale document image.

I. Introduction

Accessing of Internet has become part of many people in day today life. A use of Internet is publically there is no privacy. Transferring a secure data over an Internet is risky. Solving these problems of data security a digital image is used to store secret information. In fast digital technology how to manage security and authentication of a digital image now a challenge. It need to required implement an effective method to solve this type of authentication problem [1]-[2], for a purpose of protection of document images. If part of image is verified and distorted the content illegally, the destructed contents are repaired by using authentication and self repaired capability. An input grayscale document images, which includes legal documents, important certificate, drawings, digital signature, design draft etc. Input image is assumed to be a binary like grayscale document image, which has mainly two gray values. One gray value represent background of image and other represent foreground of image. Grayscale document image divides background and foreground by selecting a threshold value. Above the threshold value represent binary 1 and below the threshold value represent binary 0.such an image look like gray values but binary in nature. Input grayscale document image adding with alpha channel plane to form a PNG image. Alpha channel plane provide transparency to input image. It also provides large space for hiding shares. Generation of authentication signal to each block and create a number of shares by using Shamir secret sharing (k, n) threshold scheme [7].Mapping of these shares with the range of value alpha channel plane. After mapping input grayscale document image transfer into stego image. At the receiver side process of stego image extraction and verification of authentication signal. If in case image is unauthentic it means there is a tampered block. To repaired these tampered block by applying reverse Shamir secret sharing scheme.

This paper is organized as follows: In section II, Literature Survey of paper. In section III, explained proposed method. In section IV, advantages proposed method. In section V, application and last section VI, conclusion.

II. LITERATURE SURVEY

Number of method for image authentication and hiding have been proposed in past. Some are explain as follows.

[1]Yong and Kot [3], proposed a two layer binary image authentication schema. First layer targeted as overall authentication and second layer is used to find out tampered block location. Input image partitioned into number of block. Authentication achieved by hiding cryptographic signature and localization of tampering achieved by embedding block identifier in each block.

Advantage: -Generation of authentication signal.
-Identify the tampered block location.

Disadvantage: -Distortion in stego image.
-No data repaired capability.

2] Wu and Liu [4], proposed a data hiding in binary image, embedding of data manipulate by using flippability of pixels. Flip black pixel into white and white into black. Proposed method used to find unauthorized use of digital signature. Hide a moderate amount of data in image. Image partition into number blocks and fixed number of bits are embedded in each block by changing some pixel in block.

Advantage: -Finding unauthorized use of digital signature.

- It verifies tampered block location of binary image.

Disadvantage: -Distortion in stego image.
-No data repaired capability.

3] Later Yong and Kot [5], proposed a pattern based data hiding method for binary image. It aims to preserving the connectivity of pixel. Flippability of pixel is determined and watermark is adaptively embedded in block. It preserves connectivity of neighboring pixel. Data embedding manipulate using pixel flippability.

Advantage: - Embedding data by using cryptographic signature.
-preserve connectivity of pixel.

Disadvantage: - Distortion in stego image.
- No tampering block localization capability.
-No data repaired capability.

4] Tzeng and Tsai method [6], proposed a new approach to authentication of binary image authentication for multimedia communication. It randomly generates an authentication codes. These codes are useful for embed into image blocks. To hold authentication code need of code holder for reduce image distortion. Data embed in image manipulate using pixel replacement. It has high possibility to generate noise pixel.

Advantage: - Capability of tampering blocks localization.
- Reduce distortion in stego image.

Disadvantage: -No data repaired capability.

III. PROPOSED SYSTEM

In past proposed methods has some problem to remove these problems, in this paper a method for authentication signal generation and also self repaired capability of tampered block is proposed.

Proposed system mainly divides into two phases:
1] Embedding phase
2] Extraction phase

1] Embedding Phase: Input is a grayscale document image with two major gray values and secret key is used embed remaining shares. Output is a stego image in the PNG format with data embedded and also the authentication signal and data used for repairing .Figure 1, shows the embedding process.

Binarization: By applying moment–preserving thresholding [8], to input image to obtain a two representative gray values. Using these values calculate a threshold to binarize input image, yielding a binary version with represent two binary values 0 and 1.

Input Image Adding with Alpha Channel Plane: An input grayscale document image transfer into a PNG image by adding with alpha channel plane and creating a new image layer with 100% opacity.

Generation of Authentication Signal: Take an input image which is gray values but binary in nature. Take an unprocessed raster scan order 2x3 block of binary image with pixels i.e. six pixels in each 2x3 block.EX-OR first three pixels and later remaining three pixels generate 2-bit authentication signal.

Creation of Shares: Take a generated 2-bit authentication signal as input. Concatenate the authentication signal with the pixels to form an 8-bit string which divides into two 4-bit segments. Apply Shamir secret sharing scheme generate number of partial shares.

Mapping of Shares: Generated partial shares mapped with range of values in alpha channel plane.

Embedding: Next step is to embed the generated shares of each block of grayscale document image into alpha channel plane. Mapping values of generated share with alpha channel plane which is nearly to the transparency range of alpha channel plane. Take a block in alpha channel image corresponding to block of binary image, select the first two pixels in alpha channel image embed with the pixels of binary image. Remaining four pixels embedded using a key. This process continues until end of number of blocks.

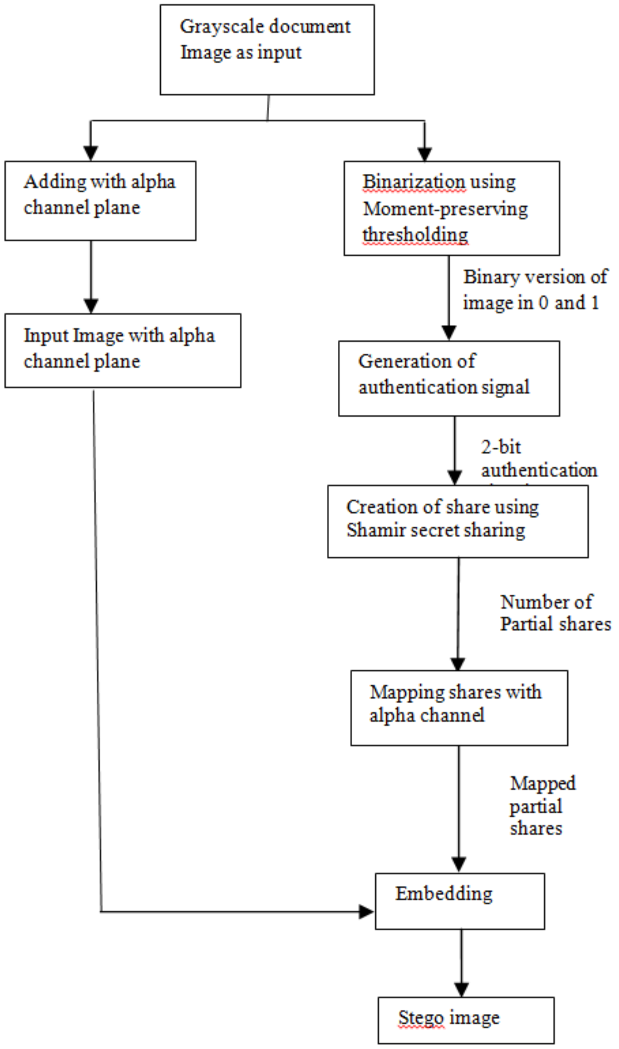
Grayscale document Image as input
Adding with alpha channel plane
Binarization using Moment-preserving thresholding
Binary version of image in 0 and 1
Input Image with alpha channel plane
Generation of authentication signal
2-bit authentication
Creation of share using Shamir secret sharing
Number of Partial shares
Mapping shares with alpha channel
Mapped partial shares
Embedding
Stego image

Figure 1: Embedding processes of proposed method

2] Extraction Phase: In this phase receiver side receive stego image and check stego image authentication, including both verification and self-repairing of the original image content. It is reverse procedure of embedding phase. Input as a stego image with two representative gray values and a secret key. Output is marked tampered block and their data repaired if possible. Figure 2, shows extract phase.

Image Authentication and Verification: At the receiver side stego image is received which is grayscale image but binary in nature .Every 2x3 blocks are verified separately. Take a binary block with unprocessed raster scan order with pixel values and corresponding block in alpha channel plane. Extract first two shares from alpha channel plane by apply reverse Shamir secret scheme [7], extract two bit authentication signal in alpha channel plane also compute the authentication signal from binary block of stego image. Compare an extracted authentication signal of alpha channel with computed authentication signal of stego image. If compare values not match then block marked as tampered and if match then stego image is authentic. If marked block has capability to self repaired then sends that block for repairing.

Self-repairing Capability of Tampered Block: If particular block is marked as tampered it implies two shares embedded in the current alpha channel plane is modified or lost. For repairing the six partial share of stego image and choose two shares of input image which is not tampered. Using these shares apply reverse secret sharing scheme repaired tampered blocks.

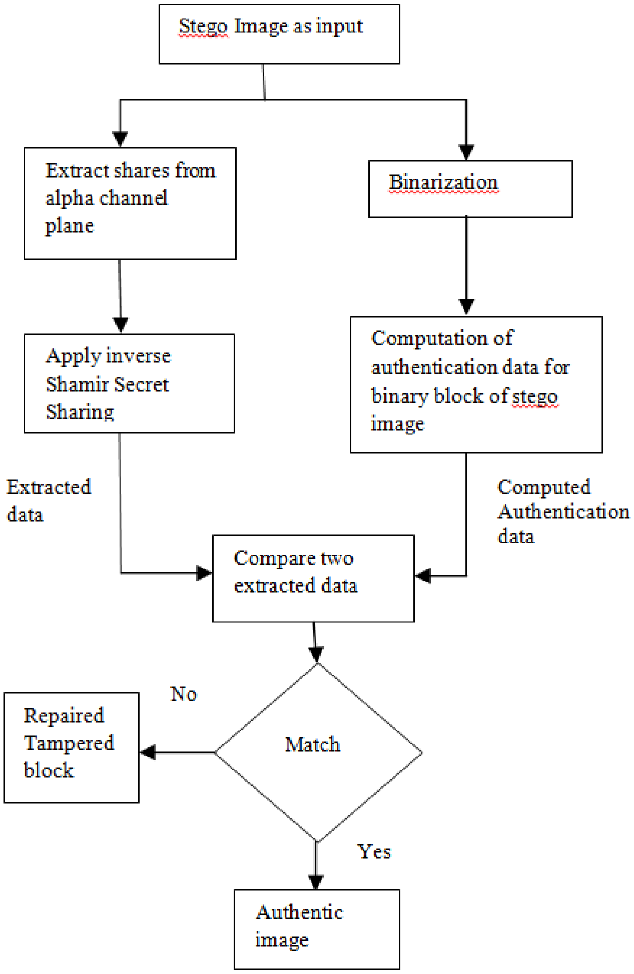
Stego Image as input
Extract shares from alpha channel plane
Binarization
Apply inverse Shamir Secret Sharing
Computation of authentication data for binary block of stego image
Extracted data
Computed Authentication data
Compare two extracted data
No
Repaired Tampered block
Match
Yes
Authentic image

Figure 2: Extraction process of proposed system

IV. ADVANTAGES

The proposed method used to data repairing and generating authentication signal but some other advantages, which are explain as following.

1] **No distortion in stego image**: In conventional image authentication methods embedding of authentication signal into an input image it is not avoid generation of output stego image distortion. Different from a previous used method a proposed method used an alpha channel for purpose of image authentication and data repairing, leaving the original image untouched so there is no distortion in stego image.

2] Tampered block localization and repaired capability: In past methods only tampered block localization capability but proposed method has tampered block localization and repaired capability. It finds the tampered block location marked block as tampered and repaired a tampered block of image. By using reverse Shamir secret scheme.

3] Use of new type channel for data hiding: Different from common type of images, a PNG image is used. An alpha channel plane is adding with an input image it produce transparency. First time used a carrier as an alpha channel plane with large space for data hiding.

4] Enhancing data security: By using Shamir secret sharing increases data security. Hiding data directly into document image pixel, in proposed system embed data in the form shares these shares mapped with the alpha channel plane of PNG image. Effect of this provides double security. First it divides data into number of shares and generation of authentication signal and second is by the use of alpha channel plane which provide transparency to input image.

5] Less possibility attack: By use of secret sharing scheme and adding authentication signals, and randomly embed the partial shares with adding a key.

V. APPLICATION

A proposed system is used in number of places where security is important. Image content authentication and repaired capabilities are useful for security protection of digital documents in many fields, such as in banking system, multinational companies, CBI.

VI. CONCLUSION

Above explanation and literature review we conclude that a proposed system useful for security of digital documents. It provides a double security by using alpha channel and generating authentication signal to each block. Also data divides into number of shares by using Shamir secret sharing scheme. It distribute authentication signal into entire image part. At the embedding process generated authentication signal and shares mapped with range of value alpha channel plane. After embedding generate a stego image which is in PNG form. At the process of stego image authentication image block marked as tampered it means image content modified. Tampered blocks are repaired by applying reverse Shamir secret sharing.

REFERENCES

[1] M. U. Celik, G. Sharma, E. Saber and A. M. Tekalp, “Hierarchical watermarking for secure image authentication with localization,” IEEE Trans. on Image Processing, vol. 11, no. 6,pp. 585–595, June 2002.

[2] C. S. Lu and H. Y. M. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Trans. on Image Processing, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.

[3] H. Yang and A. C. Kot, “Binary image authentication with tampering localization by embedding cryptographic signature and block identifier,” IEEE Signal Processing Letters, vol. 1 no. 12, pp. 741–744, Dec. 2006.

[4] M. Wu and B. Liu, “Data hiding in binary images for Authentication and annotation,” IEEE Trans. on Multimedia, vol. 6,no. 4, pp. 528–538, Aug. 2004.

[5] H. Yang and A. C. Kot, “Pattern-based data hiding for binary images authentication by connectivity-preserving,” IEEE Trans. on Multimedia, vol. 9, no. 3, pp. 475–486, April 2007.

[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 Communications Letters, vol. 7, no. 9, pp. 443–445.

[7] A. Shamir, “How to share a secret,” Communication of ACM, vol. 22, pp. 612–613, 1979.

[8] W. H. Tsai, "Moment-preserving thresholding: a new approach," Computer Vision, Graphics, and Image Processing, vol. 29, no. 3, pp. 377-393, 1985

AUTHORS

First Author – Reddypatil Ashwini G. has completed B.E. degree in computer engineering from Pune University and persuing M.E.in computer networking from BAMU University Aurangabad, reddyashu89@yahoo.com.
Second Author – Prof.Mrs.V.R.Chirchi is working as assistant Professor in PG Department of MBES college of Engineering Ambajogai.