International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||12||Pages||7625-7629||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47, (2016):93.67, DOI: 10.18535/ijsrm/v5i12.08

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

Reddy patil 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 binarize. These binaries 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 value called share 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 not match with the current block content. So need to repair data by applied reverse Shamir secret sharing scheme.

Keywords: Data Hiding, Data repairing, PNG, Alpha Channel, Image authentication, Grayscale document image.

1. 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 thresholded 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 value 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 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) thresholdding 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 stego image extraction and verification of authenticate signal. If in case image is unauthentic it means there is a tampered block. To repaired 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, result and discussion. In section V, advantages and last section VI, conclusion.

2. Literature survey

Number of method for image authentication and hiding have been proposed in past.

[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 of this method generation of authentication signal means each block generate a two layer authentication schema
Identify the tampered block location by using the cryptographic signature.
Disadvantage of this method distortion in stego image because not it generate some noise.
No data repaired capability of tampered block.

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. A method used to find unauthorized use of digital signature. Hide a moderate amount of data. Image partition into blocks and fixed number of bits are embedded in each block by changing some pixel in block.
Advantage of this method finding unauthorized use of digital signature and it verifies tampered block location of binary image.
Disadvantage of this method distortion in stego image and also 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 of this schema embedding data by using cryptographic signature and preserve connectivity of pixel.
Disadvantage distortion in stego image and no tampering block localization capability.
No data repaired capability because it only finding a tampered block.
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 used to embed into image blocks. So need code holder for reduce image distortion. Data embed in image manipulate using pixel replacement. It has high possibility to generate noise pixel.
Advantage of this method capability of tampering blocks localization means it find out the location of tampered block.
Reduce distortion in stego image means some noise in an image.
Disadvantage of this method no data repaired capability because it only find out

3. Proposed system

Proposed work perform following steps as 1) Generation of stego image in the PNG format from a given grayscale image and Authentication of given stego-image in the PNG format.

1 Algorithms for Generation of a Stego-Image

For generation of stego image used two algorithms 1) (k,n)-Threshold secret sharing. 2) Stego image generation.

Algorithm 1: (k,n)-threshold secret sharing.

Input: secret d in the form of an integer, number n of participants, and $k \leq n$ threshold .

Output: n shares in the form of integers for the n participants to keep.

Step 1. Choose randomly a p prime number that is larger than d.

Step 2. Select $k-1$ integer values within the c_1 ,c_2……..c_{k-1} range of 0 through p-1 .

Step 3. Select n distinct real valuesx_1,x_2,……..x_n

Step 4. Use the following $k-1$ degree polynomial to compute n function values $F(x_i)$, called partial shares for $i = 1,2 \ldots \ldots \ldots n$, i.e.,

$$F(x_i)\left(d + c_1 x_i + c_2 x_i^2 + \cdots + c_{k-1} x_i^{k1}\right) \bmod \quad (1)$$

Step 5. Deliver the two-tuple $((x_i, F(x_i))$as a share to the ith participant where$i = 1,2 \ldots \ldots n$.

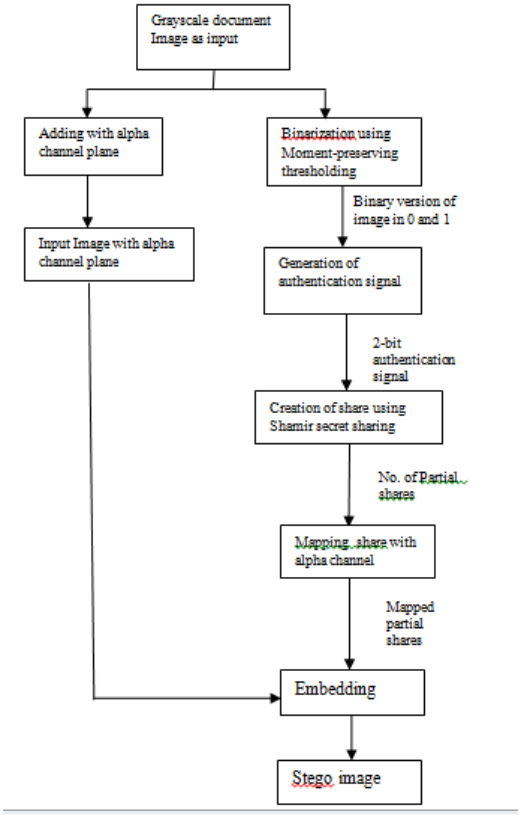

Figure 1: Embedding processes of proposed method

2 Algorithm for Stego-Image Authentication

For the authentication of stego image also used two algorithm 1)Secret recovery and Authentication of given stego image.

Algorithm 1: Secret recovery.

Input: k shares collected from the n participants and the prime p number with k both p and being those used in Algorithm 1.

Output: secret d hidden in the shares and coefficients c_i used in (1) in Algorithm 1, where $i = 1,2, \ldots . k-1$.

Step 1. Use the k shares

$$(x_i, F(x_i)), (x_2, F(x_2)), \ldots \ldots, (x_k, Fx_k)) \text{ to}$$

$$\text{Setup, } F(x_j)(d + c_1 x_j + c_2 x_j^2 + \cdots + c_{k-1} x_j^{k-1}) \bmod p \qquad (3)$$

Step 2. Solve the equations above by Lagrange's interpolation to obtain d as follows [10]

$$d = (-1)^{k-1}\left[F(x_1)\frac{x_2, x_3 \ldots . x_k}{(x_1 - x_2)(x_1 - x_3) \ldots \ldots (x_2 - x_k)} + \cdots F(x_k)\frac{x_1\, x_2 \ldots . x_k}{(x_k - x_1)(x_k - x_2) \ldots (x_k - x_{k-1})}\right] \bmod p$$

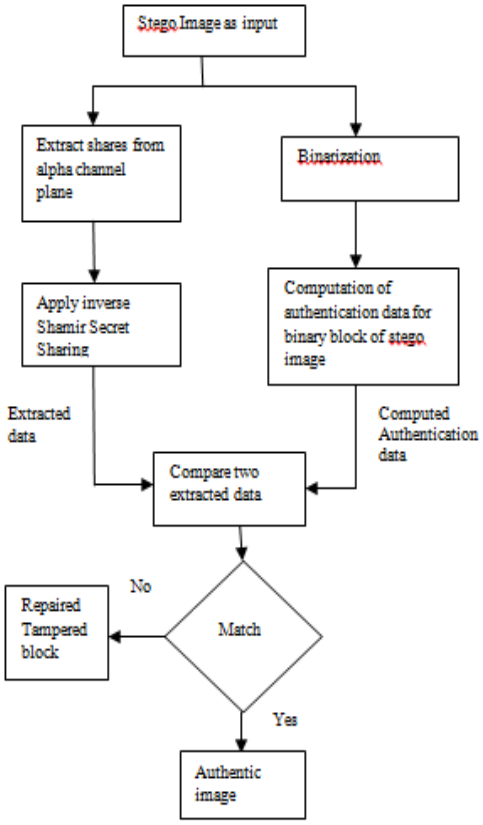

Figure 2: Extraction process of proposed system

4. Results and discussion

Proposed method results are compared by the following parameter no.of tampered blocks, no. of detected blocks, no. of repaired blocks, false acceptance ratio, false rejection ratio as Shown in table 1 and 2**.**

Table1: Result of attack using superimposing

Total no. of block	No. of tampered block	No.of detected blocks	No. of repaired blocks	False acceptance ratio	False rejection ratio
36400	16.67	100	98.72	0	0
36400	24.64	100	94.86	0	0
36400	42.48	100	79.40	0	0

Following points are noted from figure 3.

-In first image no. of tampered block ratio decrease no. of detected blocks will hundred percent, repaired block ratio cannot be correctly the result just noise.

- Second case tampered block detected more than the first but repaired ratio decrease.

-In third case tampered block repaired more but data repaired result become worse when tampered are grow.

-Note that detection ratio all are 100% due to alpha channel and false acceptance and rejection ratio zero.

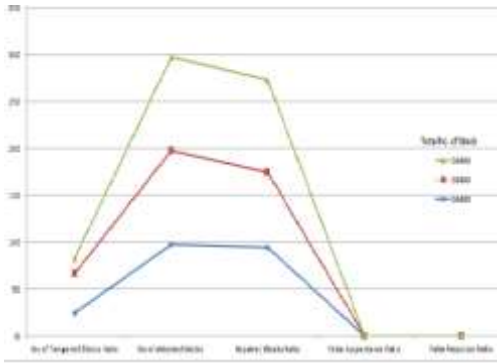

Figure 3: Result of three images attack using superimposing

Table 2: Result of attacks using painting

NO.o.f blocks	No. of tampered blocks	No. of detected blocks	No. of repaired blocks	False acceptance ratio	False rejection ratio
36400	3.36	1.63	0.92	4	0
36400	4.12	2.06	1.13	7	0
36400	5.07	2.43	1.39	15	0

Following points noted from figure 4:

-It is noted that when stego image is tampered with by painting, which does not change content of alpha channel plane .

-The hidden authentication signals and data of repairing are not destroy.

-Detection ratio more compared to previous method and false acceptance ratio change because there is probability of ¼ of erroneous block authentication to occur because 2 bit created as signal for block authentication.

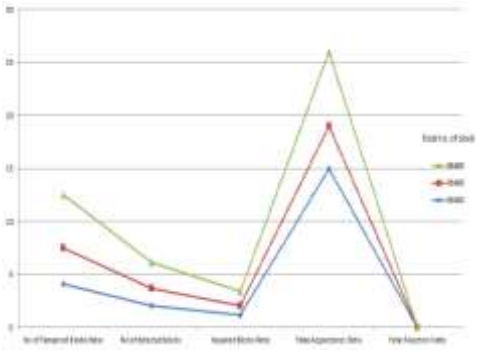

Figure: 4 Result of three images attack using painting

5. Advantages

1] **No image 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. Original image there is no distortion

2] **Tampered block localization and repaired capability:** It finds the tampered block location and marked block as tampered and repaired a tampered image part pixel level. Two unhampered partial shares are chosen and repaired tampered block.

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 share 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.

6. Conclusion

Above explanation 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. Proposed system more secured than the previous system.

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. 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
9. W. H. Tsai, "Moment-preserving thresholding: a new approach," *Computer Vision, Graphics, and Image Processing*, vol. 29, no. 3, pp. 377-393, 1985
10. C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," J. Syst. Softw., vol. 73, no. 3, pp. 405–414, Nov./ Dec. 2004

AUTHORS

First Author- Reddy patil 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@gmail.com.

Second Author- Prof.Mrs.V.R.Chirchi is working as assistant Professor in PG Department of MBES college of Engineering, Ambajogai.