Shamir Secret Sharing Method for Authentication of Colored Document Image with Self Repair Capability

Miss. Pradnya Kadam[1] Miss. Nishigandha Khandagale[2] Miss. Poonam Yadav[3] Prof. Sarla A.Chimegawe[4]
[1,2,3]Student [4]Professor & Guide
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]IOK-COE, PUNE

Abstract— In this paper we proposed a new authentication method which is based on secret sharing technique with self repair capability. In this paper, we take color image then each block of that image genarate the authentication signal. Then we apply the Shamir secret sharing method. In that method each block of image are transfered into several shares. Then we apply alpha channel plane for PNG image formation. After that that PNG image is encrypted using chaotic logistic map and forms the stego image. This stego image is received by the receiver. If the image is tampered then we used the Reverse Shamir secret algorithm and repair that tampered image and get the original image.

Key words: Shamir secret sharing algorithm, Reverse Shamir secret algorithm, Logistic map, Alpha channel plane

I. INTRODUCTION

A. About The Project:

Digital images are used to preserve important information. But providing authentication to these images is challenging task. In this paper we use of fast technology it is easy to modify the contents of this digital image. Particularly for document images such as important certificates, scanned checkes, art drawings, signed documents, circuit diagram etc.

In this project, we take input as a color image. Then each block of that image creates the authentication signal. Then we used the shamir secret sharing method, in that method authentication signals are combined with binarized block content is transformed into several shares. Then we add the new transparent layer on that image that is called alpha channel plane which form the PNG image. This PNG image is transformed into stego image by using chaotic logistic map. In that map, the encryption is done. This stego image is send to the receiver. After that the receiver checks for the authentication to verify that the image is tampered or not. If the image is tampered then we apply Reverse Shamir secret algorithm to repair that image.

B. Domain of the Project:

Domain of our project is "Image Processing". In this project we use shamir secret algorithm for generating the authentication signal and creating several shares. We convert the color image into PNG format by using the alpha channel plane. Then we use the chaotic logistic map for encryption and to generate the stego image. If this image is tampered then we use the reverse shamir secret sharing algorithm and it having the data repair capability.

C. Existing System:

To digitally identify authorized image we have watermarking techniques available. But its found that watermarking techniques are not as reliable to use for authentification because these can be removed by softwares available. Hence we are using the colored technique which helps in digitally identifying and preventing image with data repairing capability.

D. Proposed System

In this project we proposed a new authentication schema based on a Shamir secret technique. In this approach we apply the Shamir secret algorithm to generate the authetication signal of a color document image. We add a new layer which is called alpha channel plane to create PNG image. And it is used for security purpose. After that we encrypt the image using logistic map and create the stego image. This stego image is received by the receiver and then he checks the authentication. If image is tampered then it is recovered by the Reverse shamir secret algorithm and get the original image.

II. SYSTEM ARCHITECTURE

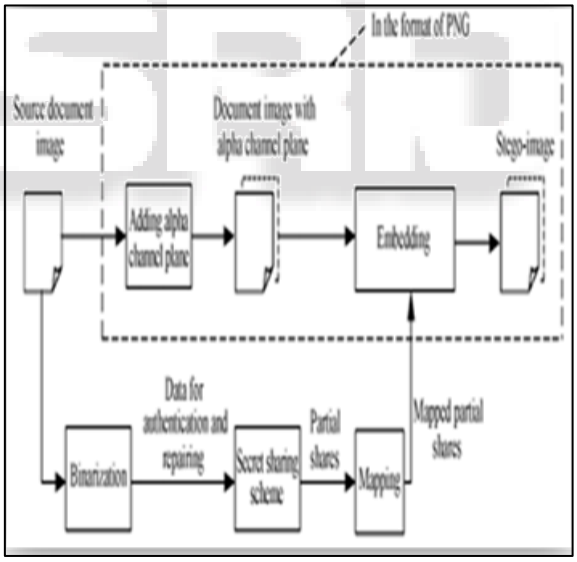


Fig. 1: System architecture for Sender side

In above figure,we take the source document image as input image(i.e color image).Then each block of that image creates the authentication signal and that signals are combined with binarized block content which is transfered into several shares using Shamir secret algorithm. Then we add the alpha channel plane on that image which creates the PNG image. Then that PNG image is encrypted using chaotic logistic map and creates the stego image.

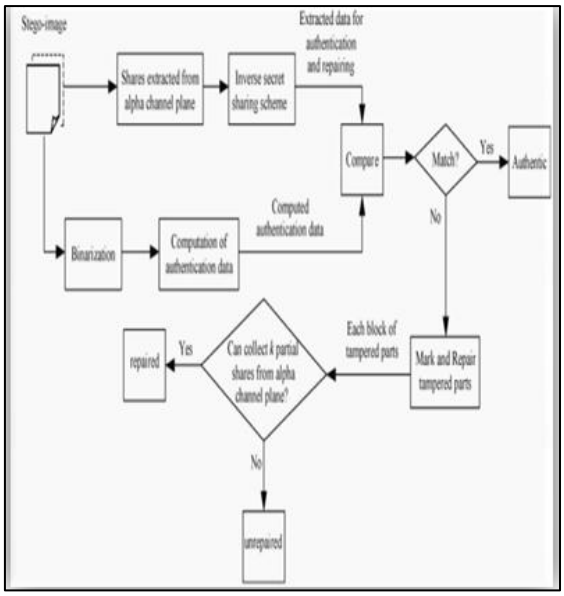


Fig. 2: System architecture for receiver side

At the receiver side, this stego image is received by the receiver and then receiver checks for the authentication of the image to verify that the image is tampered or not. Then we apply the Reverse or inverse shamir secret algorithm. Then it collects the partial shares from alpha channel plane and repairs that share and get the original image.

III. ALGORITHM

A. *Shamir Secret Algorithm:*

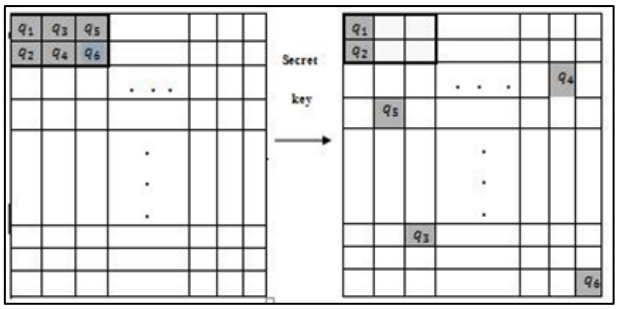
- I/P: Take a secret say an Integer number S and n number of participants with threshold (min requirement) t <= n.
- O/P: n number of shares. (One for each participant)

1) Steps:
1) Take a secret key s and threshold value t.
2) Create partial shares for each participant.
3) Select n unique real values (like 2 4 6 …)let them called as y1,y2….yn and give to partial shares.

1) *Stego Image Generation:*

- I/P : A Colored Image E and secret key K
- O/P : Stego Image in PNG with encrypted format (Authentication Signal & Data required for repairing)
- Part 1: Authentication Signal Generation

1) Step 1: Binarization of input image into by using Moment preserving threshold (ie automatic threshold selection). To convert image to binary form that forms cover image.
2) Step 2: Convert cover image into PNG image with an alpha channel plane which creates new layer of 100% opacity and combine it with Colored Image E using image processing software package.
3) Step 3: (In loop) take a raster scan (rectangular pattern of image capture and reconstruction) of order 2*3 block in img with pixels p1, p2….p6.
4) Step 4: Generate 2 bit Authentication signal say b1 and b2 where b1 = p1 exor p2 exor p3 and b2 = p4 exor p5 exor p6.



- Part 2: Design and Embedding of shares

5) Step 5: Creation of data for secret sharing.
Here we concatenate 8 bits ie b1 b2 and p1,p2…p6 which gives 8 bit String then divide this string into two 4bit segments and convert those segments into 2 decimal numbers d1 and d2 resply.
6) Step 6: Generation of partial shares.
Here we use Shamir's Secret Sharing Scheme to generate six partial shares. say r1….r6.
7) Step 7:Mapping of partial shares.
Here we add a number to each of r1…..r6 and call it as mr1….mr6. which fall in nearly total transparency range in alpha channel plane.
8) Step 8: Embedding.
Here we select first two shares from alpha channel plane in raster scan order corresponding to first two shares in img and replace them with mr1 and mr2.
9) Step 9: Then we embed remaining shares in random such that each selected shares(pixels) not being the first 2 one in any block.(ie don't select same 2 pixels from other block) And replace other four pixels by mr3 to mr6.
10) Step 10: if there is unprocessed block then go to Step 3 otherwise take img in PNG format.

- Part 3: PNG image encryption

Here we encrypt the PNG image using chaotic logistic map and generate Stego image

2) *Stego Image Authentication Algorithm:*

This is executed At Receiver's end

- I/P: Stego Image and Secret Key K used .
- O/P: Image with tampered blocks and their data repaired if possible.
- Part 1: Decryption and extraction of three representative RGB value

1) Step 1: Decrypt Stego Image by random key used in encryption.
2) Step 2: Convert decrypted image into binary form .

- Part 2: Stego Image Authentication

3) Step 3: Take a raster scan on unprocessed block of and find six partial shares (pixels) r1…r6 in alpha channel plane of Stego Image .
4) Step 4: Take out the 2 bit secret Authentication signal

Here we subtract the number we added in Step 7 of Algorithm 3 from each mr1….mr6 to obtain r1….r6.

3) *Algorithm:*

Secret recovery of shares to extract two values secret S and m1 as output.(Reverse Shamir Secret) Part1:

Now Transform S and m1 into 4bit binary values and concat them to form 8bit String, take first 2 bits of string to get hidden authentication signal b1 b2.

5) Step 5: Compute the 2bit authentication signal from p1…p6.

Generate 2 bit Authentication signal bt1 and bt2 where bt1 = p1 exor p2 exor p3 and bt2 = p4 exor p5 exor p6.

6) Step 6: Compare b1 b2 with bt1 bt2 by checking if b1=bt1 and b2=bt2. If match found then we are good.. Else the image is tampered.

7) Step 7: (In loop)if there exist any unprocessed block in stego img then continue with Step 3 otherwise continue with Step 8. .

4) *Algorithm:*

Reverse Shamir Secret Part 2:

8) Step 8: Take out the remaining partial shares that we have distributed in Step 8 of Algorithm 3. For each block execute following steps to extract 4 partial shares r3 to r6.

Use key K to collect the 4 pixels (partial shares) in alpha channel plane of stego img in the same order. As they were randomly selected in Step 9 of algorithm 3. And take out the respective data mr3…mr6 embedded in them. Subtract the number we added in Step 7 of Algorithm 3 from each mr3….mr6 to obtain r3….r6

9) Step 9: What image we get is as the desired self-repaired image.

IV. Advantages of Proposed System

1) Higher data security: Due to encryption, the data becomes scrambled, so the hacker cannot see the data. And by using Shamir secret scheme the proposed method survives the malicious attacks.
2) Providing pixel level capability to the tampered image parts:

V. Mathematical Model

A. *Set Theory:*

Sr. No	Description
1	Let 'S' be the system S={ } S={SI.....} Set S is divided into 4 modules S= {S1, S2, S3, S4} S1= Login module S2= Image size verification Module(sender module or encryption module) S3=store and download Module S4=Image repair module(decryption module)
2	Login module: S1={Input, Output}

Table 5.2.1: Mathematical model

1) *Login Module:*
   1) Identify the inputs for S1,
   – Inputs = {X1}
   – X1= Request for User
   2) Identify the output for S1.
   – Outputs = {Y1}
   – Y1= Provide a service

2) *Image Size Verification Module (Sender or Encryption Module):*
   1) Identify the inputs for S2,
   – Inputs = {X2, X3}
   – X2= User login
   – X3=Authentication
   2) Identify the output for S2.
   – Outputs = {Y2, Y3}
   – Y2= Download authorized data
   – Y3=Download decoy document

3) *Store and Download Module:*
   1) Identify the inputs for S3,
   – Inputs = {X4}
   – X4= Client communicate with server
   2) Identify the output for S3.
   – Outputs = {Y4}
   – Y4= Give the corresponding java classes for JSP file

4) *Image Repair Module (Decryption Module):*
   1) Identify the input for S4,
   – Inputs={X5}
   – X5=Get the tampered image
   2) Identify the output for S4,
   – Outputs={Y5}
   – Y5=Repair the image and get original image.

VI. Result Analysis

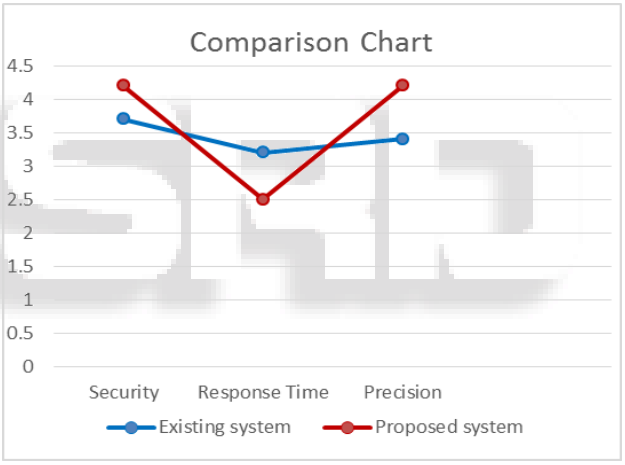


Fig. 3: Comparison Chart

Security	3.7	4.2
Response Time	3.2	2.5
Precision	3.4	4.2

Table 1: Comparison table

VII. Future Enhancement

Now we are only using images for data reparing. In future we will use data behind the image. And this data will repair using algorithm. We will also use video hiding behind the images

VIII. Conclusion

In this paper, we propose a authentication method with a data repair capability for color images based on secret sharing. An authentication signal is generated for every block of each grayscale channels of RGB image. This blocks are combined with binarized block content and tranformed to several shares using shamir secret scheme.

And at receiver side we used Reverse shamir secret scheme to repair the tampered image.

IX. ACKNOWLEDGEMENT

We thank Dr. Damodar Garkal (Principal IOKCOE Pune) for providing necessary facilities to carry out the work. We are very thankful to Prof. Sarla A.Chimegawe (Assistant Professor) for her useful guidance.

REFERENCES

[1] M. U. Celik, G. Sharma, E. Saber, and A.M. Tekalp, "Hierarchical watermarking for secure image authentication with localization," IEEE Trans. Image Processing, vol.11, no.6, pp.585-595, june.2002.
[2] C Yu, X Zhang "Watermark embedding in binary images for authentication", IEEE Trans. Signal Processing, vol.01, no.07, pp.865-868, September. 2004.
[3] A. Shamir, "How to share a secret," Commun. ACM, vol.22, no.11, pp.612-613, Nov, 1979.
[4] P. Jhansi Rani, S. DurgaBhavani1stInt'1Conf on Recent Advances in Information Technology RAIT-2012.
[5] Chih-HsuanTzeng and Wen-Hsiang Tsai, "A new approach to authentication of Binary image for multimedia communication with distortion reduction and security enhancement. IEEE communication letters VOL.7.NO.9 2003
[6] H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," IEEE Signal Processing Letters, vol. 13.
[7] 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.
[8] 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.
[9] Niladri B. Puhan, Anthony T. S. Ho "Binary Document Image Watermarking for Secure Authentication Using Perceptual Modeling" IEEE International Symposium on Signal Processing and Information Technology2005.
[10] W.H. Tsai, "Moment-Preserving thresholding: a new approach." Computer Vision, Graphics, and Image Processing, vol. 29, no.3, pp.377-393, 1985.

