RESEARCH ARTICLE OPEN ACCESS

# Ramp Secret Sharing Approach to Authentication and Data Repairing For Document Image

Mary Linda P A[1], Larry Liston[2], Remya B Nair[3], Aswathy Mohan[4], Lisha P P[5]
[1,3,4,5] M. Tech, Department of Computer Science, Model Engineering College, Thrikkakara, Ernakulam, Kerala.
[2]M.Tech, Department of Mechanical Engineering, Jyothi Engineering College, Vettikkattiri, Thrissur, Kerala.

**ABSTRACT**
Digital images are widely used to protect confidential and important information. But the problem is to provide the authentication and integrity to these digital images is a very challenging task. Therefore a new efficient authentication method is proposed for document images with verification and data self-repair capability using the Portable Network Graphics (PNG) image. Here, an authentication signal is generated for each block of a document image which, combine with the binarized block data, is transformed into several shares using the Ramp secret sharing scheme. These several binarized block data shares are then embedded into an alpha channel plane. During the embedding process, the generated share values are mapped into a range of 238-255 to yield a transparent stego-image with a disguise effect. Alpha channel is combining with the original image and converted into PNG image format. While the process of image authentication, the image block is marked as tampered, if the authentication signal generated from the current block content does not match with share that extracted from the alpha channel plane. Then using reverse Ramp scheme, two shares from unmarked blocks are collected and then data repairing is applied. Some security measures are also proposed for protecting the security of the shares hidden in the alpha channel.

***Keywords*** - Image authentication, Portable Network Graphics, Ramp secret sharing.

## I. INTRODUCTION

Digital images are widely used to protect confidential and important information. But the problem is to provide the authentication and integrity to these digital images is a very challenging task. Due to the open availability of digital image processing tools, open access of the digital data is easily possible. So changes to original data and reuse of visual material are also becoming easy. And so nowadays is very easy to create illegal copies and to change the images in such a way that the identification of big economic or human lives losses is very difficult. It is very necessary to ensure the integrity and authenticity of a digital data of images. It is very important to propose effective methods to solve this type of image authentication problem. To solve this problem secret image sharing scheme has been used. Secret image sharing method generates several shares which are then shared in the protected document image, and the protected image at receiver side is reconstructed by enough different shared shares. If part of an image is verified to be modified illegally, the changed content can be repaired. The main advantage of this method is here we don't require original image to check the integrity of received data. The integrity is checked with received image only.

In this paper, a system for authentication of document images with extra self-repair capability for fixing tampered image data is explained. Using this extra authentication signal the tampering of the data is detected. This authentication signal is calculated form binary image with 2 main values. Then the original image is transformed into a stego-image by combining it with alpha channel. While the process of image authentication the stego image is verified for its authenticity and integrity. Data modifications of the stego-image can be detected and repaired at the pixel level. Secret message is converted into n shares i.e authentication signals for embedding it in the original image; and when k of the n shares, are gathered the secret message can be recovered completely. This type of secret sharing scheme is helpful for reducing the risk of significant partial data loss.

In the proposed method the binary image authentication with repair capability is designed for grayscale images. Using secret sharing scheme the shares are generated which are distributed randomly in the image block. For this authentication signal is generated and used to calculate the shares. Alpha channel is used for transparency and for mapping this extra authentication signal.

## II. PROPOSED METHOD

The proposed method deals with image content authentication with a data repair capability for document image via the use of the Portable

Network Graphics (PNG) image. An authentication signal is generated for each block of a document image and combined with the binarized block data, which is transformed into several shares using the Ramp method. The generated shares are embedded into an alpha channel. Alpha channel plane is combining with the original image and converted into PNG image format.

During the embedding process, the computed share values are mapped into the small range of 23-255 and these values is embedding into alpha channel. In image authentication process, an image block is marked as altered if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane.

Data repairing is then applied to each altered block by a reverse Ramp secret scheme. Protecting the security of the data hidden in the alpha channel is also measured. This project proposes an authentication method that deals with the binary-like document images instead of pure binary ones and simultaneously solves the problem of image tampering.

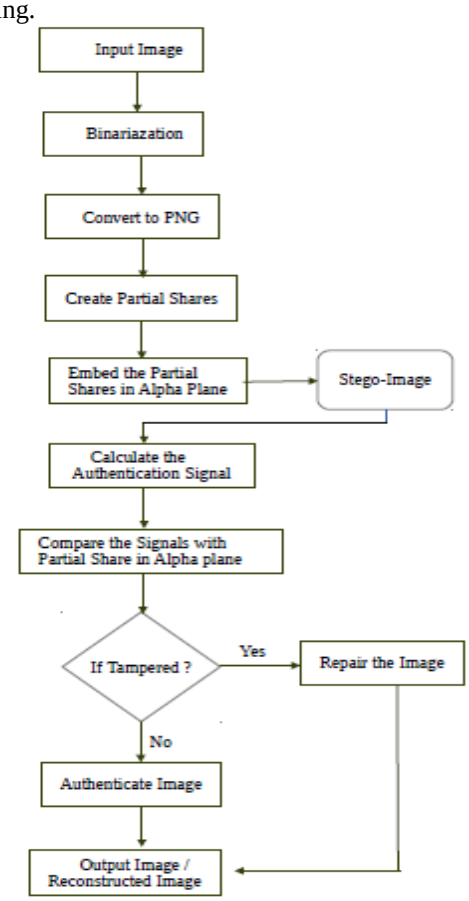



***Figure 2.1.*** Flow chart of Proposed Method

## III. RAMP SECRET SHARING METHOD

In this section we describe the Ramp secret sharing method to generate *n* shares for a group of *n* secret sharing participants from a secret integer value y for the threshold k, we can in the following way

### 1.1. Algorithm for secret share generation

**Preliminaries:**

$\oplus$ : A bitwise XOR operation
$\|$ : Concatenation of bit sequences
$n_p$ : A prime number that is $n_p \geq n$.
$w_i$ : A share given to *i*-th participant *Pi*. ($i = 0, \ldots, n-1$)
S : The secret ( $S \in \{0,1\}^{d(n_{p-1})}$ , d>0)

***Input:*** Secret S and n.
***Output:*** Shares w.

1: Let np : prime number >=n
2: Divide the S into (np - 1) pieces of d-bit segment equally
S->$S_1 \| S_2 \| S_3 \| S_4 \| S_5 \| S_6$
3: Prepare S0 as a d-bit zero sequence
4: Generate (k-1) $n_p$ - 1 of d-bit random numbers $r^j_i$
5: Execute XOR operation by the following equation

$$w_{(i,j)} = \oplus_{(h=0)}^{(k-2)} r^h_{(h-i+j)} \oplus s_{(j-i)}$$

$$= S_{j-i} \oplus r^0_i \oplus r^1_{i+j}.$$

6: Concatenate $n_p$ - 1 pieces and generate a share $w_{(i)}$

$$w_{(i,0)} \| w_{(i,1)} \| w_{(i,2)} \| w_{(i,3)} \| w_{(i,4)} \| w_{(i,5)} \| \longrightarrow w_{(i)}$$

### 1.2. Algorithm for secret share recovery

***Input:*** Shares w.
***Output:*** Secret S and n.

1: Obtain the binary matrices $G_{t0}$ , $G_{t1}$, $G_{t2}$ such that $w_i = G_i \cdot r$.

$$w_i = \left(w_{(i,0)}, w_{(i,1)}, w_{(i,2)}, w_{(i,3)}\right)^T$$

$$r = \left(r^0_0, \ldots, r^0_3, r^1_0, \ldots, r^1_4, s_1, \ldots, s_4\right)^T$$

$\mathbf{G_i = (I_4, E_i, L_{-i})}$
$I_\alpha$ : α x α identity matrix

$$E_\beta = \left(\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 0 & & & \\ \vdots & \ddots & \vdots & \vdots & & I_{n_p-\beta} & \\ 0 & \cdots & 0 & 0 & & & \\ \hline & & & 0 & 0 & \cdots & 0 \\ & I_{\beta-1} & & \vdots & \vdots & \ddots & \vdots \\ & & & 0 & 0 & \cdots & 0 \end{array}\right)$$

$$\left(\begin{array}{c|c} \vdots & \\ 1 & L_\beta \\ \vdots & \end{array}\right)$$

2: Execute the Gaussian Elimination and obtain the matrix M

$$G = \left(\begin{array}{c|c} G_{t_0} \\ G_{t_1} \\ G_{t_2} \end{array} I_{12}\right) = \left(\begin{array}{ccc|ccc} I_4 & E_{t_0} & L_{-t_0} & 1 & & \\ I_4 & E_{t_1} & L_{-t_1} & & \ddots & \\ I_4 & E_{t_2} & L_{-t_2} & & & 1 \end{array}\right)$$

$$\Downarrow \text{Gaussian Elimination on } GF(2)$$

$$G' = \left(\begin{array}{ccc|c} & * & & * \\ \hline \emptyset & \emptyset & I_4 & M \end{array}\right).$$

Solving the system of equation for $S_1$, $S_2$ $S_3$, $S_4$

3: Execute the following operation and obtain the secret

( $S_1$, $S_2$ $S_3$, $S_4$) = M. $W_i$

## IV. GENERATION OF A STEGO-IMAGE

The algorithm for describing the generation of a stego-image in the PNG format is presented as follows:

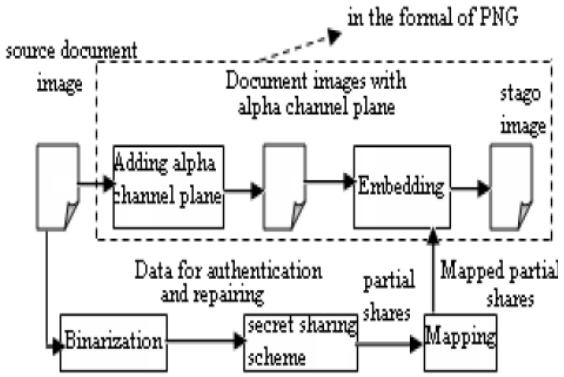



***Figure 4.1.*** Generation of a stego-image

### 1.3. Algorithm for generation of stego-image.

***Input:*** Input image I with two gray value and a secret key k.

***Output:*** Stego-image $I_0$ in PNG format with relevant data embedded, including the authentication signal and the data used for repairing.

1: Resize the image with width and height as multiple of 6 so as make sure all pixels come within a block completely.

**Part 1: Authentication signal generation**.

2: Input image Binarization**.** Apply the moment-preserving technique to obtain two major values of the image Z1 and Z2 where Z1 represents binary value of 1 ad Z2 represents 0. Calculate the threshold used to binarized the image using the formula T= (Z1+Z2)/2

3: Save the binarized image as Ib.

4: Transform the input image into PNG format along with alpha channel. Let all the pixels have the values of alpha channel as 255. Let the image be IALPHA.

5: Take the raster scan of unprocessed blocks of size 2x6 with values P1,P2....P6 from the image Ib.

6: Creation of authentication signal. Generate a 2-bit authentication signal s=a1a2
where a1 = P1 xor P2 xor P3 and a2 = P4 xor P5 xor P6

**Part 2: Design and embedding of shares.**

7: Concatenate the values a1, a2, P1 to P6 to form a 8-digit string containing only 0s and 1s and convert into decimal equivalent of these numbers.

9. Let S be the decimal equivalent of these number.

10: Add 238 to the values of Q1 through Q6, resulting in a new value $Q1^1$ through $Q6^1$ so as to get their values in the near transparency zone.

11: Obtain the corresponding block at the alpha channel of the image IALPHA. Embed the first two values $Q1^1$ and $Q2^1$ in the same block at the first column of the block of alpha channel.

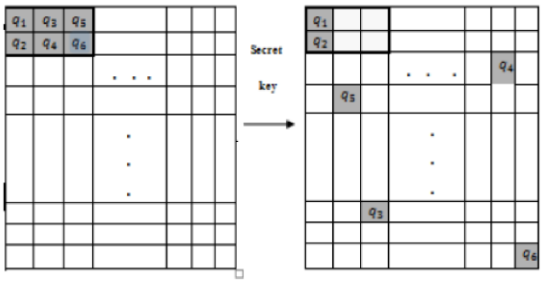



***Figure 4.2.*** Embedding 6 shares generated for a block, 2 Shares embedded in current block and the other 4 in 4 randomly selected pixels outside the block, with each selected pixel not being the first 2 one in any block

12: Using the key , spread the remaining 4 values $Q3^1$ , $Q4^1$, $Q5^1$ and $Q6^1$ in the different pixels alpha channel of the image. Make sure while embedding randomly, none of the values are overwritten and the first column of other blocks are never used for this spreading.

13: if there exist any unprocessed block in Ib then go to step 5

14: Take final I in the PNG format as the desired stego-image I0

.

## V. AUTHENTICATION OF A STEGO-IMAGE

A complete algorithm describing the proposed stego-image authentication process including verification of the original image content is described below

**1.4. Algorithm for verification of stego-image.**
***Input***: Stego-image $I_0$ with gray values Z1 and Z2 and secret key K.
***Output:*** Image with tampered blocks marked.

1: Verify whether the image has alpha channel. If not, discard the whole image as unauthentic and request for retransmission of original image.

2: Input image Binarization**.** Apply the moment-preserving technique to obtain two major values of the image Z1 and Z2 where Z1 represents binary value of 1 ad Z2 represents 0. Calculate the threshold used to binarized the image using the formula T= (Z1+Z2)/2

3: Save the binarized image as Ib.

4: Take the raster scan of unprocessed blocks Bb from Ib with pixel values P1,P2....P6 and find the six pixel $Q1^1$ through $Q6^1$ of the corresponding block BALPHA in the alpha channel IALPHA of Ib.

5: Subtract 238 from each of $Q1^1$ and $Q2^1$to obtain two partial shares Q1 and Q2 and of Bb respectively.

6: Extraction of authentication from the BALPHA . s=a1a2

7: Computation of the authentication signal from the current block Bb. $s^1 = a1^1 . a2^1$
where $a1^1$ = P1 xor P2 xor P3 and $a2^1$ = P4 xor P5 xor P6

8: Compare the authentication signal s and $s^1$

9: if s and $s^1$ matches then mark the block as authenticated and move to the next block else mark the block as tampered and proceed to the next block.

10: After all blocks are processed we obtain the image with all the tampered blocks IMARK.

## VI. REPAIRING OF A STEGO-IMAGE

A complete algorithm for repairing the tampered block verification of the original image content is described below

**1.5. Algorithm for repairing tampered block.**
***Input***: Image with tampered blocks marked.
***Output:*** Image Ir which has the pixels repaired.

1: Subtract 238 from these alpha channel values to obtain the shares.

2: Obtain raster scan of block B of size 2x6 from I and check whether block is marked.

3: If not, proceed to the next block by marking this block as repaired.

4: If yes, choose 2 shares out of 6 shares which are preferably from a block that are marked untampered.

5: Using reverse ramp secret sharing, obtain the secret values S.

6: Convert the decimal equivalent to binary. Concatenate the binary values to form the 8-digit string.

7: Take each digit from the 8-bit string and convert to gray value as follows:

8: If the value is 0 then replace the corresponding pixel in the block of the image by Z2 else by Z1

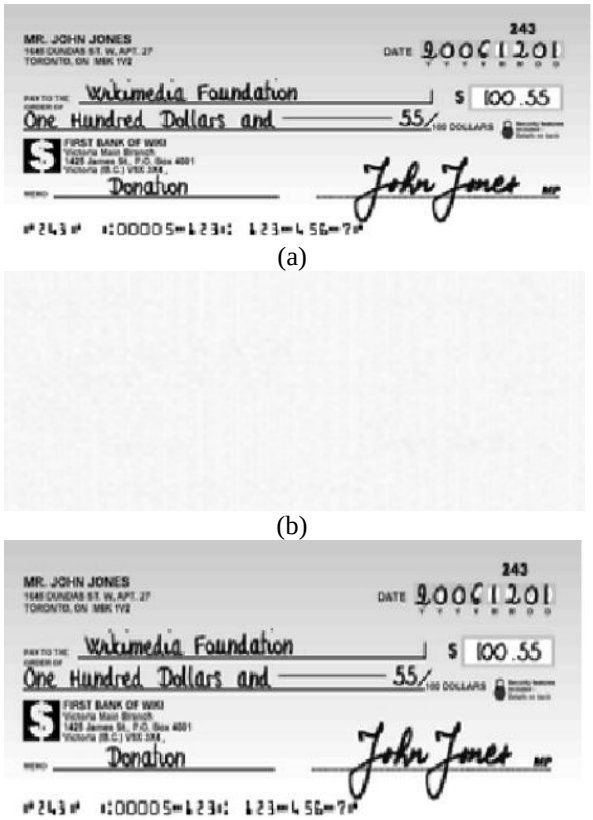
9: Proceed to the next block till the complete image is processed.

## VII. ADVANTAGES OF PROPOSED SYSTEM

- Providing pixel-level repairs of tampered image parts.
- Having higher possibility to survive image content attacks.
- Making use of a new type of image channel for data hiding.
- No distortion to the input image.

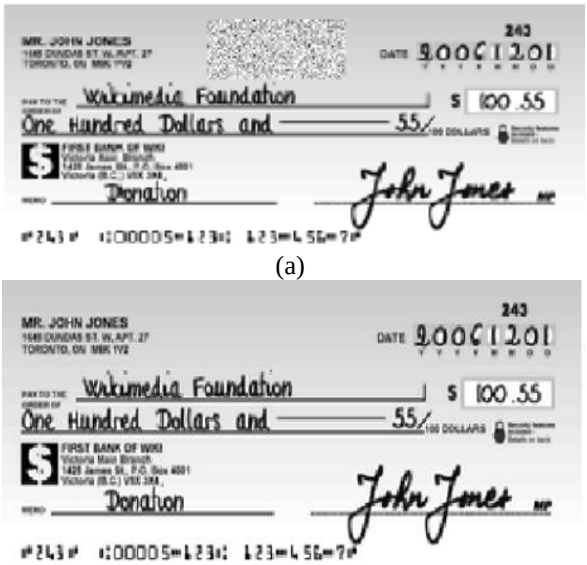
## VIII. EXPERIMENTAL RESULT

For editing the image three common operations are used. They are superimposing, noise and painting. Experimental result using a document images are shown below:



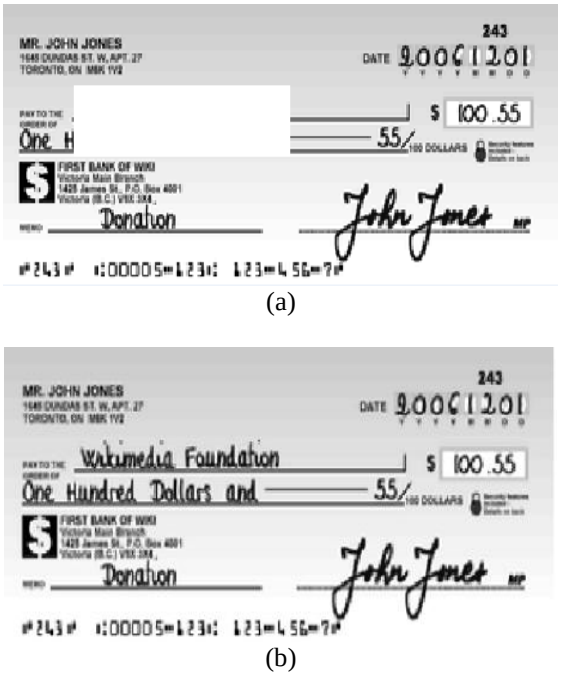

(a) (b) (c)

***Figure 9.1.*** Experimental result of a document image of a sign.(a) Original Image (b) Alpha channel plane after embedding the share between the range of 238-255 (c) Stego-image with alpha channel in PNG format



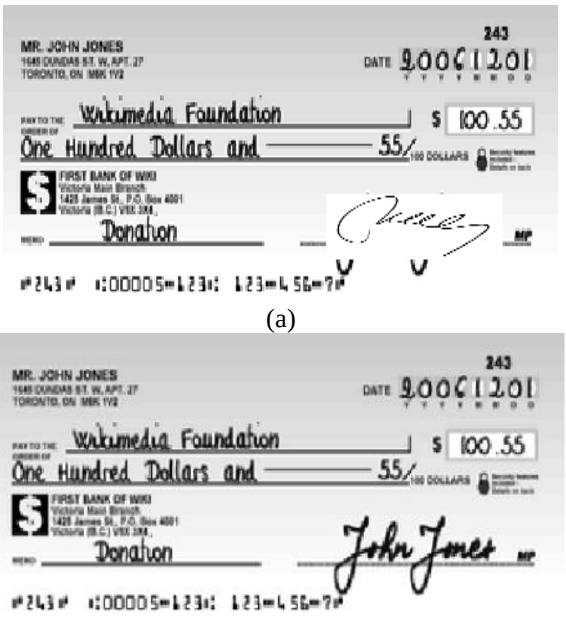

(a) (b)

***Figure 9.2.*** Authentication result of a document image of a check in the form of PNG attacked by added noises.(a) Tampered image with added noises. (b) Data repair result.




(a) (b)

***Figure 9.3.*** Authentication result of a document image of a check in the form of PNG attacked by painting. (a) Tampered image with painting. (b) Data repair result.




(a) (b)

***Figure 9.4.*** Authentication result of a document image of a check in the form of PNG attacked by superimposing. (a) Tampered image with superimposing. (b) Data repair result.

***Table1:*** Comparison of document image authentication methods.

| | Distor-tion in stego-image | Tamper-ing local-ization capabil-ity | Repair capabil-ity | Reported authentica-tion precision | distribu-tion of authenti-cated image parts | Manipula-tion of data embedding |
|---|---|---|---|---|---|---|
| Wu & Liu [4] | Yes | No | No | Macro-block | Non-blank part | Pixel flippabil-ity |
| Yang & Kot [5] | Yes | Yes | No | 33×33 block | Non-blank part | Pixel flippabil-ity |
| Yang & Kot [6] | Yes | No | No | Macro-block | Non-blank part | Pixel flippabil-ity |
| Tzeng & Tsai [8] | Yes | Yes | No | 64×64 block | Entire image | Pixel replace-ment |
| Pro-posed method | No | Yes | Yes | 2×3 block | Entire image | Alpha channel pixel replace-ment |

## IX. CONCLUSION

A secret sharing method for a binary grayscale document images has been proposed. With this approach if the document has been illicitly tampered, it has ability to identify the tampered block and has the self-repair capability by using Ramp secret sharing method. The undesired opaque effect visible in the stego-image coming from embedding the partial shares has been eliminated by mapping the share data into a range of alpha channel values near their maximum transparency value of 255.

## X. FUTURE SCOPE

The possible Future studies take several directions, including choice of alternative block sizes and connected parameters (prime value range, value for secret sharing, range of authentication signal bits, etc.) to enhance data repair effects. Some security measures for enhancing the protection of the data embedded in the alpha channel plane is also specified. Applications of the proposed method for authentication and repairing of attacked color images, and block based owner validation may also be applied

## REFERENCES

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

[2] Wen-Ai Jackson and Keith M.Martin, "A Combinatorial Interpretation of Ramp Schemes.'', *Australasian Journal of Combinatorics*, vol. 14, pp. 51-60,1996

[3] Chang-Chou Lin, Wen- Hsiang Tsai, "Secret Image Sharing With Steganography And Authentication" Department Of Computer And Information Science, National Chiao Tung University, Hsinchu 300, Taiwan,; Accepted 20 July 2003.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] C. H. Tzeng and W. H. Tsai, "A new approach to authentication of binary images for multimedia communication with distortion reducduction and security enhancement," *IEEE Commun. Lett.*, vol. 7, no. 9, pp. 443–445, Sep. 2003.