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

***Abstract*—In this paper we proposes a new authentication method which is based on secret sharing technique and logistic map with repairing capability of data, via the use of the Portable Network Graphics image. In this approach each block of a grayscale document image generate an authentication signal, which combine with binarized block content, is transformed into several shares using Shamir secret sharing scheme. The shares generated from the binarized block contents are then embedded into an alpha channel plane. The original grayscale image combine with alpha channel plane to form a PNG image; this PNG image encrypted by using chaotic logistic map to form a stego image. Stego image received in the receiver side is decrypt and checks the authentication. If the authentication process fails then repairing is done in each tampered block, after collecting two shares from unmarked block using reverse Shamir scheme. Security of data provided by sharing of data in the alpha channel and encrypting the stego image.**

***Index Terms*—Image authentication, secret sharing, data repair, PNG (Portable Network Graphics), encryption, logistic map.**

I. INTRODUCTION

Digital images are used to preserve important information. But providing integrity and authentication to these images is a challenging task. In this era with the use of fast advanced technologies it is easy to modify the contents of these digital images. It is important to make an effective method to solve image authentication problem [1] [2], particularly for document images such as important certificates. Scanned checks, art drawings, signed documents, circuit diagrams, design drafts, testaments etc.

In the case of binary document images, it is difficult to authenticate because of its simple binary nature that lead to perceptible changes after authentication signal are embedded in the image pixel. So in this paper we are performing authentication of grayscale document images. Gray scale images are looking like a binary image, because of this reason it is called as binary like gray scale image. Grayscale images overcome the visual quality problem of binary images.

In this paper we are proposing a new method for authentication of document images with a supplementary self repairing capability for fixing tampered image data. The input cover image is taken as binary like grayscale image.

Manuscript received May, 2012.

Mrs. S Kavitha Murugesan, Head of the department, Department of computer science Vedavyasa Institute of Technology, Malappuram, India.

Mr. Shanavas K A, M Tech computer science student, Vedavyasa Institute of Technology, Malappuram, India.

After applying the proposed method, the input cover image is transformed into PNG format, with scrambled form in a supplementary alpha channel for transmission on networks or archiving in database. By using proposed method the stego-image retrieved or received may be verified for its authenticity. Integrity modification of the stego- image can be detected by the method at the block level and repaired at the pixel level. In case the alpha channel is totally destroyed from the stego-image, the entire resulting image is regarded as inauthentic, that means fidelity check of the image failed. The proposed method is based on (t, n) threshold secret sharing scheme proposed by Shamir [3] and also with encryption based on chaotic logistic map [4]. By secret sharing scheme the secret message is transformed into n shares, and when t of the n shares is collected the secret message can be recovered without data loss. Using logistic map we generate a random key, by this key the PNG image formed with alpha channel plane is scrambled, and made ready for transmission. For highly confidential document image transmission this authentication method can be used, this method provides two layers of security to the document by keeping shares in the alpha channel and encrypting the PNG image. Secret sharing helps the reconstruction of tampered image content and encryption scrambles the image thereby hiding the data's of the document image.

Gray scale document image + Alpha channel plane= PNG image.

Several methods for image authentication have been proposed in the past. Chih-HsuanTzeng and Wen-Hsiang Tsai [5] proposed, Authentication with embedding special codes. Embedding randomly-generated codes, into the blocks of a given cover image, producing a stego-image. Authentication is achieved by verifying the codes in the blocks of a given stego image. H. Yang and A. C. Kot [6] proposed a method for Authentication with cryptographic signature and block identifier provides a two layer image authentication in which the first layer provides the overall authentication by hiding the cryptographic signature (CS) of the image and the localization of the tampering is obtained from the second layer by embedding the block identifier (BI) in the "qualified" or "self-detecting" macro-blocks (MBs). M Wu and B. Liu[7] proposed Authentication by manipulating flippable pixels. In this method images are partitioned into blocks and significant amount of data will be embedded into each block maintaining a block based relationship and without introducing noticeable artifacts. Che-Wei Lee and Wen-Hsiang Tsai [8] proposed a secret sharing based method for authentication of grayscale document images.

This method provides data repairing capability via the use of PNG image. Niladri B. Puhan, Anthony T. S. Ho[9] proposed authentication using Perceptual Modeling , estimates the distortion resulting from flipping of a pixel by finding the curvature-weighted distance difference (CWDD) measure between original and watermarked contour segments.

II. ALGORITHM FOR CREATING SECRET SHARES

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

Input: Take secret c in the form of an integer, number n of participants and threshold t ≤ n.

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

Step1: Choose a random prime number p larger than c.

Step2: select t-1 integer values $m_1, m_2, \ldots \ldots m_{t-1}$ range of 0 through p-1.

Step3: Select n distinct real values $y_1, y_{2,\ldots\ldots} y_n$

Step 4: Use the following (t-1) degree polynomial to compute n function values f(y_j), called partial shares for j=1,2…..n

$$f(y_j) = (c + m_1 y_j + m_2 y_j^2 + \cdots + m_{t-1} y_j^{t-1}) mod p \ldots. (1)$$

Step5: Deliver the two tuple $(y_j, f(y_j))$ as a share to the j^{th} participant where j=1, 2, 3……n.

There are t coefficients denoted c and m_1 through m_{t-1} . To collect t shares from the n participants to form t equation to recover secret c. The following describes the equation for solving the process of secret recovery.

B. Algorithm 2: Secret recovery of shares

Input: Select t shares from the n participants and the prime number p with both t and p

Output: Secret c hidden in the shares and coefficients m_j used in (1) where j=1, 2, 3,….. m- 1.

Step1: Use the t shares

$(y_1, f(y_1)), (y_2, f(y_2)), \ldots. (y_t, f(y_t))$ to set up

$$f(y_j) = (c + m_1 y_j + m_2 y_j^2 + \cdots m_{t-1} y_j^{t-1}) mod p \ldots. (2)$$

Where j=1, 2 ,…… t

Step2: Solve the t equations above by Lagrange's interpolation to obtain t as follows.

$$\mathbf{c}=(-1)^{t-1}[f(y_1)\frac{y_2 y_3 \ldots\ldots y_t}{(y_1-y_2)(y_1-y_3)\ldots\ldots(y_1-y_t)}$$

$$+f(y_2)\frac{y_1 y_3 \ldots\ldots y_t}{(y_2-y_1)(y_2-y_3)\ldots\ldots(y_2-y_t)}+\ldots.+$$

$$f(y_t)\frac{y_1 y_2 \ldots\ldots y_{t-1}}{(y_t-y_1)(y_t-y_2)\ldots\ldots(y_t-y_{t-1})}] \mathbf{mod\ p}$$

Step3: Compute m_1 through m_{t-1} by expanding the following equality and comparing the result with (2) in step 1 while regarding variable y in the equality below to be y_j in (2)

$$f(y) = [f(y_1)\frac{(y-y_2)(y-y_3)\ldots\ldots(y-y_t)}{(y_1-y_2)(y_1-y_3)\ldots\ldots(y_1-y_t)}$$

$$+f(y_2)\frac{(y-y_1)(y-y_3)\ldots\ldots(y-y_k)}{(y_2-y_1)(y_2-y_3)\ldots\ldots(y_2-y_t)}+\ldots+$$

$$f(y_t)\frac{(y-y_1)(y-y_2)\ldots\ldots(y-y_{t-1})}{(y_t-y_1)(y_t-y_2)\ldots\ldots(y_t-y_{t-1})}] \mathbf{mod\ p}$$

In the above algorithm step 3 is used for the purpose of computing the values of parameter m_j in the proposed method. In other application if only secret value c need be recovered, this step can be eliminated.

III. IMAGE AUTHENTICATION AND DATA REPAIRING

In image authentication and data repairing, we create a PNG image from a binary type grayscale document image E with an alpha channel plane. Then the actual image E is converted into binary form by moment preserving threshold [10] which is denoted as E_b . This E_b is taken as an input to Shamir's secret sharing scheme to generate n secret shares. The mapped secret shares are embedded into alpha channel plane to produce an imperceptibility effect. Then, the mapped secret shares are embedded randomly into alpha channel plane. The PNG image crated is then encrypted by chaotic logistic map [4]. Embedded shares providing security and repairing capability, encryption gives extra security by scrambling the PNG image. Two block diagram describing the proposed method are shown in figure 1 and 3.

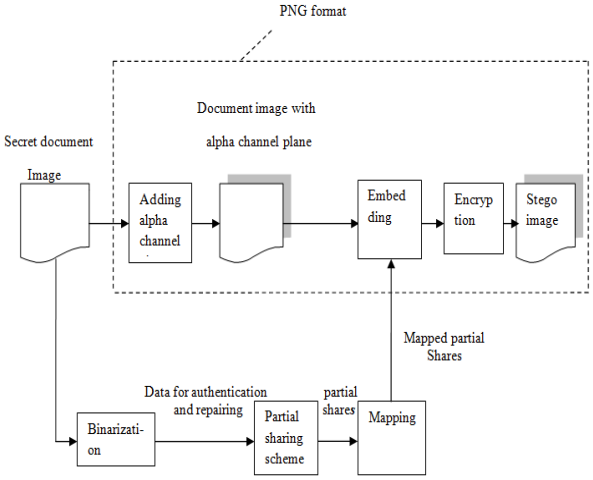


Fig 1: Creating a PNG image from grayscale document image and alpha channel

A. Algorithm for Stego-Image Generation

The following algorithm describes the generation of stego-image of the proposed method.

Algorithm 3: Generating stego image in PNG format from a given grayscale image.

Input: A grayscale image document E with two major gray values and secret key K.

Output: Stego image E' in PNG with encrypted format, relevant data embedded, including the authentication signal and the data used for repairing.

Part 1: Authentication signal generation.

Step1 (Binarization of input image) Moment preserving threshold [3] applied E to obtain two representative gray values g_1 and g_2. Computing the average of g_1 and g_2 to obtain the threshold value. Use this threshold to binarize E, yielding a binary version of E_b.

Step2 (Conversion of cover image into PNG format) Convert E into PNG image with an alpha channel plane E_α by creating new image layer with 100% opacity and no color as E_α and combining it with E using an image processing software package.
Step3 (Starting of loop) Take in an unrefined raster scan order of 2*3 block B_b in E_b with pixels $p_1, p_2 \ldots . p_6$.
Step 4(Authentication signal generation) Generate 2-bit authentication signal L=$b_1 b_2$with b_1=$p_1 \oplus p_2 \oplus p_3$ and b_2=$p_4 \oplus p_5 \oplus p_6$

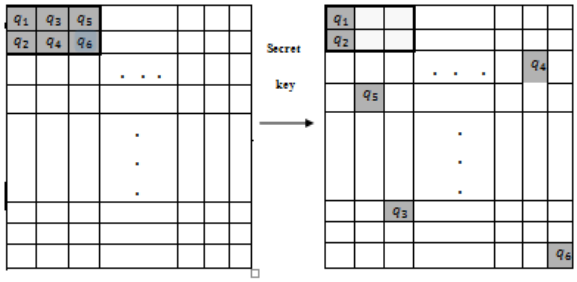
Part 2: Design and embedding of shares.

Step5 (Creation of data for secret sharing) concatenate the 8 bits of $b_1, b_2$and $p_1$through p_6 form an 8-bit string, divide this string into two 4-bit segments, and convert the segment into 2 decimal numbers a_1 *and* a_2 respectively.
Step6 (Generation of partial shares) Set p, m_j, and y_j the following value apply eqn. (1) of Algorithm 1, 1) p=17 (the smallest Prime number larger than 15); 2) c=$a_1$and m_1= a_2 ; and 3) y_1=1,y_2=2,……y_6=6. Perform algorithm 1 as a (2, 6) threshold secret sharing scheme and generate six partial shares $r_1$through r_6 using the following equations:

$$r_j = f(y_j) = (c + m_1 y_j) \bmod p \quad \ldots\ldots\ldots\ldots (3)$$

Where j= 1, 2 ,…. 6
Step7 (Mapping of partial shares) Add 238 to each of $r_1$through r_6, resulting in the new value of r_1' through r_6' respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane E_α.
Step 8 (Embedding two fractional shares in the current block) Take block B_α in E_α corresponding to B_b inE_b, select the first two pixels in B_α, in the raster scan order and replace their values by r_1' and r_2' respectively.

Step 9 (Embedding remaining partial shares at random



6 shares created for a block 2 shares embedded at the current block and 4 at random pixels out of the block

Fig 2. Pictorial representation of 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 .

pixels) Use key K to select randomly four pixels in E_α but outside B_α , not the first two pixels of any block; in the raster scan order, and replace four pixels values by the remaining four partial shares r_3' through r_6' generated above, respectively.
Step10 (End of loop) If their exist any unprocessed block in E_b , then go to step 3 otherwise take the E in the PNG format.

Part 3: PNG image encryption.

Step11. (Encryption of the PNG image) Encrypt the PNG image using chaotic logistic map [4], take the final E in PNG with encrypted format as the desired stego-image E' .

The prime number p used here is17, so the values of $r_1$through$r_6$yield by equation (3) are between 0 and 16.After executing step 7 of above algorithm, they become r_1' and r_2' respectively. Which all fall into the small interval of integers ranging from 238 to 254 with a width of 17 (the value of the prime number). Consequent embedding of r_1' through r_2' in a narrow interval into the alpha channel plane means that very alike values will appear everywhere in the plane, resulting in a nearly uniform transparency effect, which will not stimulate notice from an attacker.

We choose prime number to be17 in the above algorithm because, if it was chosen instead to be larger than 17, then the above mentioned interval will be enlarged and the values of r_1' through r_6' will become possibly smaller than 238, creating visually whiter stego image . In contrast, the 8 bits mentioned in steps 5 and 6 above are transformed into two decimal numbers $b_1 and b_2$with their maximum values being 15(step 5 above) , which are forced to lie in the range of 0 through p-1 (step 2 in algorithm 1). Therefore p should not be chosen to be smaller than 16, i.e.; p=17 is the best possible answer.

B. Algorithm for Stego-Image Authentication

The following algorithm describing the proposed stego image authentication process, including both verification and self-repairing of original image content.
Input: A stego image E' with gray values g_1 and g_2 and secret key K used in algorithm 3.

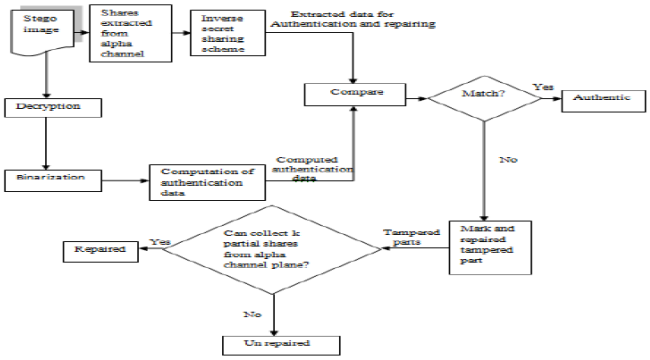


Fig 3: Verification and self-repairing of stego image for the process of image authentication.

Output: Image E_r with tampered blocks marked and their data repaired if possible.

Part 1: Decryption of stego image and extraction of the two representative gray values.

Step 1 (Decryption of stego image) Decrypt the stego image by the random key used in the encryption.
Step2 (Conversion of decrypted image into binary form) Compute T=$(g_1 + g_2)/2$, using this threshold value to Convert E' into binary form $E_b'$with "0" representingg_1 and "1" representingg_2.

Part 2: Stego image authentication.

Step 3 (Start loop) Take in a raster scan order an unprocessed block B_b' from E_b' with pixel values p_1 through p_6 and find six pixel values r_1' through r_6' of the corresponding block B_α' in the alpha channel plane E_α' of E'.
Step4 (Drawing out of secret authentication signal) The following steps perform to extract the hidden 2-bit authentication signal L=$b_1 b_2$ from B_α' .

(1) Subs tract 238 from each of $r_1' and r_1'$to obtain 2 partial shares r_1 and r_2 of B_b' , respectively.
(2) With shares (1,r_1) and (2,r_2) as input, perform Algorithm 2 to extract the two values c and m_1 (secret and first coefficient value) as output.

(3) Transform c and m_1 into two 4 bit binary values , concatenate them to form an 8-bit string S, and take the first 2 bits of S to compose the hidden authentication signal L=$b_1 b_2$.

(4)

Step 5 (Computation of authentication signal from the current block content) Compute 2 bit authentication signal $L^{'}=b_1^{'}b_2^{'}$ from values p_1 through p_6 of six pixels of $B_b^{'}$ by $b_1^{'}=p_1 \oplus p_2 \oplus p_3$ and $b_2^{'}=p_4 \oplus p_5 \oplus p_6$.

Step 6 (Comparison of computed authentication signal with hidden shares and making the tampered block) Matching L and $L^{'}$ by checking if $b_1=b_1^{'}$ and $b_2=b_2^{'}$ and if any mismatch occurs mark $B_b^{'}$, the corresponding block $B^{'}$ in $E^{'}$ and all the partial shares embedded in $B_\alpha^{'}$ as tampered.

Step 7(End loop) If there exist any unprocessed block in $E_b^{'}$ then go to step 3, otherwise continue.

Part 3: Self-repairing of the original image content

Step8 (Drawing out of the remaining partial shares) For each block $B_\alpha^{'}$ in $E_\alpha^{'}$, execute the following step to extract the remaining 4 partial shares r_3 through r_6 of the corresponding block $B_b^{'}$ in $E_b^{'}$ from blocks in $E_\alpha^{'}$ other than $B_\alpha^{'}$.

(1) Use key K to collect the four pixels in $E_\alpha^{'}$ in the same order as they were randomly selected for $B_b^{'}$ in step 9 of the algorithm 3, and take out the respective data $r_3^{'}, r_4^{'}, r_5^{'}, r_6^{'}$ embedded in them.

(2) Subtract 238 from each of $r_3^{'}$ through $r_6^{'}$ to obtain r_3 through r_6, respectively.

Step 9 (Repair the tampered regions)For each block $B^{'}$ in $E^{'}$ marked as tampered previously, execute the following steps to repair if it possible.

(1) From the six partial shares r_1 through r_6 of block $B_b^{'}$ in $E_b^{'}$ corresponding to $B^{'}$ (two computed in step 4(1) and four in step 8(2) above), choose two of them, say r_k and r_l which are not marked as tampered , if possible.

(2) With shares (k,r_k) and (l,r_l) as input , perform Algorithm 2 to extract the values of c and m_1 (secret and first coefficient value)as output.

(3) Transform c and m_1 into two 4 bit binary values, and concatenate these 2 binary values to form an 8-bit string $S^{'}$

(4) Take the last six bits $a_1^{'}, a_2^{'}, \ldots, a_6^{'}$ from $S^{'}$, and check their binary values to repair the corresponding tampered pixel values $z_1^{'}, z_2^{'}, \ldots, z_6^{'}$ of block $B^{'}$ by the following way: if $a_j^{'}$=0, set $z_j^{'}=g_1$; otherwise set $z_j^{'}=g_2$; where j=1,2…6.

Step10. Take the final $E^{'}$ as the desired self –repaired image E_r.

IV. MERITS OF PROPOSED SYSTEM

Along with being capable of data repairing and being blind in nature. The proposed method has several other merits which are described as following.

1. Higher data security and possibility to survive image content attacks: Due to the use of encryption the data become scrambled, therefore the hackers doesn't see the document data, and also by the use of sharing method , the proposed method can survive malicious attacks of common content modification, such as super imposition, painting etc
2. Providing pixel level repairing of tampered image parts: After collecting two non tampered partial shares, we can repair the tampered block at the pixel level.
3. Making the use of new type of image channel for data sharing: Rather than common type of image a PNG image has the extra alpha channel plane , which is normally used to produce transparency of the image .

V. CONCLUSION

We have proposed a secure authentication scheme for grayscale document images by the use of secret sharing method and chaotic logistic map. In this scheme security is provided by, secret sharing and encryption. Using Shamir secret sharing method both the generated authentication signal and the content of a block are transformed into partial shares. Which are then distributed in an elegant manner into an alpha channel plane to create a PNG image. This image is encrypted by using chaotic logistic map and forms a stego image. In the authentication process, if it seen that the data is tampered then self-repairing is done in the content of the tampered block by reverse Shamir scheme. This method enhances the security by embedding the data in the alpha channel plane and encrypting the PNG image.

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. DurgaBhavani1st *Int'lConf 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 Technology*2005.
10. W.H. Tsai, "Moment-Preserving thresholding: a new approach." *Computer Vision, Graphics, and Image Processing*, vol. 29, no.3, pp.377-393, 1985.

AUTHORS PROFILE

Mrs. S Kavitha Murugesan, BE, ME working as head of the department in computer science Departmet at Vedavyasa Institute of Technology, Malappuram, India. She is perusing PhD in the field of Data mining

Mr. Shanavas K A, B.Tech, doing M Tech in computer science and engineering at Vedavyasa Institute of Technology Malappuram, India.