AUTHENTICATION OF COLOUR IMAGES BY USING ENCRYPTED PNG IMAGE WITH DATA REPAIR CAPABILITY

Mrs. Sonal Kokate[1], Dr. Manjusha Deshmukh[2]

[1,2]*Final Year Student*

M.E. in "Electronics and Telecommunication Engineering"

Saraswati College of Engineering, Kharghar, Navi Mumbai (India)

ABSTRACT

A new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original grayscale image to form a PNG image. During the embedding process, the computed share values are mapped into a range of alpha channel values near their maximum value of 255 to yield a transparent stego-image with a disguise effect. In the process of image authentication, an image block is marked as tampered 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 tampered block by a reverse Shamir scheme after collecting two shares from unmarked blocks. Measures for protecting the security of the data hidden in the alpha channel are also proposed. Good experimental results prove the effectiveness of the proposed method for real applications.

I. INTRODUCTION

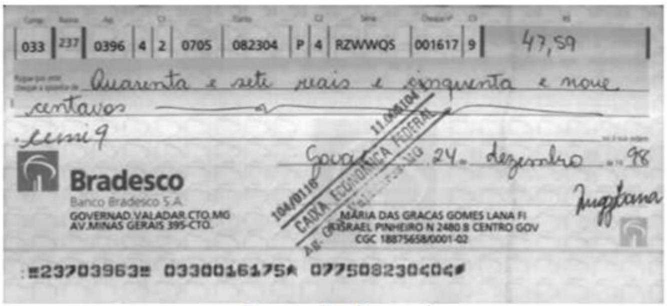
Digital images are used to preserve important information. But providing integrity and authentication to these images is a challenging task. In this era with the use of fast advanced technologies it is easy to modify the contents of these digital images. It is important to make an effective method to 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. 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 - Hsuan Tzeng 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 & 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. GRAY SCALE IMAGE AUTHENTICATION

Digital information is a form of preserving data for which authentication is necessary to overcome the tampering attacks. In multimedia applications, it is necessary to authenticate the source image which might be subjected to tampering. So, for such content authentication watermarking technique is used. It is one among the emerging fields that are used for content authentication. As, the content authentication is being the hottest topics now a days, it is necessary to assure that the delivering of image to somewhere is delivered as it is. However, with the fast advance of digital technologies it is easy to make the modifications to the images. Thus integrity of image becomes a serious concern. To solve those image authentication problem particularly digitized documents, digital signatures, tables, texts, etc., whose security must be protected. In this paper we are performing image authentication of grayscale images. Grayscale image has two gray values i.e. foreground and background. Grayscale images look like binary ones. So, we can call a grayscale image as binary like grayscale image. Binary image consists of two colors black and white. Using binary images can cause some problems. As the binary images are simple in nature many unpleasant strokes can encounters. So using grayscale images can solve the problem of visual quality which the binary one cannot do. Many conventional methods have been proposed for authentication of grayscale images. In our proposed method, the image is first watermarked and divided into shares using Shamir secret sharing scheme. Later, those shares are reconstructed using inverse Shamir secret sharing scheme and watermark has been extracted if the image is authentic. Data loss during transmission is marked as gray blocks.



033 237 0396 4 2 0705 082304 P 4 RZWWQS 001617 9 47,59

Quarenta e sete reais e cinquenta e nove centavos

Cemig

Gov[illegible] 24 dezembro 98

Bradesco
Banco Bradesco S.A.
GOVERNAD.VALADAR.CTO.MG
AV.MINAS GERAIS 395-CTO.

104/0116 CAIXA ECONOMICA FEDERAL

MARIA DAS GRACAS GOMES LANA FI
ISRAEL PINHEIRO N 2480 B CENTRO GOV
CGC 18875658/0001-02

23703963 0330016175 077508230404

Fig. 1. Gray scale cheque image.

III. IMAGE AUTHENTICATION TECHNIQUES

Before presenting and discussing various methods, we start by defining the general requirements that are essential for any authentication system. These requirements are:

Sensitivity: The authentication system must be able to detect any content modification or manipulation. For strict authentication algorithms, detection of any manipulation is required and not only content modification.

Robustness: Also called tolerance. The authentication system must tolerate content preserving manipulations. This property is valid just for algorithms that provide a selective authentication service.

Localization: The authentication system must be able to locate the image regions that have been altered.

Recovery: The authentication system must be able to partially or completely restore the image regions that were tampered.

Security: The authentication system must have the capacity to protect the authentication data against any falsification attempts.

Portability: The authentication system must be able to carry the signature with the protected image during any transmission, storage or processing operation.

Complexity: The authentication system must use real-time implemented algorithms that are neither complex nor slow.

[1] Strict image authentication

[2] Fragile watermarking

[3] Content-based image authentication or selective authentication

[4] Semi-fragile watermarking

[5] Image authentication by digital signatures based on the image content

IV. ADVANTAGES AND LIMITATIONS OF VARIOUS METHODS

Table presents a summarized comparison of image authentication methods discussed in this paper: methods based on conventional cryptography, fragile watermarking, and semi-fragile watermarking and on image content signatures. For each group of methods we have shown the type of the authentication tag, the dependency of this authentication tag on the image, the type of the authentication service provided, that is: strict or content-based (selective) image authentication service, the localization capacity of the altered regions,

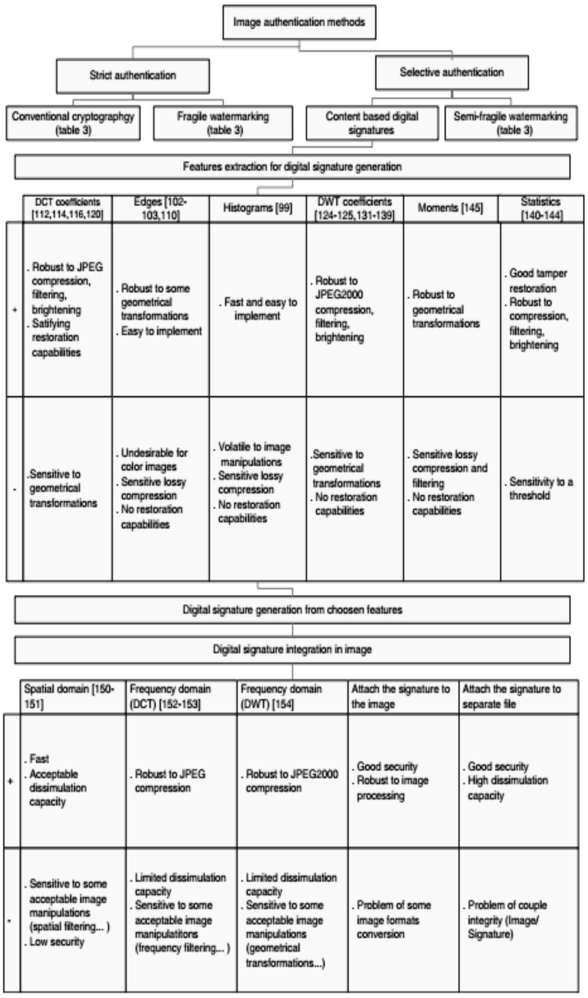


Image authentication methods
Strict authentication
Selective authentication
Conventional cryptographgy (table 3)
Fragile watermarking (table 3)
Content based digital signatures
Semi-fragile watermarking (table 3)
Features extraction for digital signature generation
Digital signature generation from choosen features
Digital signature integration in image

	DCT coefficients [112,114,116,120]	Edges [102-103,110]	Histograms [99]	DWT coefficients [124-125,131-139]	Moments [145]	Statistics [140-144]
+	. Robust to JPEG compression, filtering, brightening . Satifying restoration capabilities	. Robust to some geometrical transformations . Easy to implement	. Fast and easy to implement	. Robust to JPEG2000 compression, filtering, brightening	. Robust to geometrical transformations	. Good tamper restoration . Robust to compression, filtering, brightening
-	.Sensitive to geometrical transformations	. Undesirable for color images . Sensitive lossy compression . No restoration capabilities	. Volatile to image manipulations . Sensitive lossy compression . No restoration capabilities	.Sensitive to geometrical transformations . No restoration capabilities	. Sensitive lossy compression and filtering . No restoration capabilities	. Sensitivity to a threshold

	Spatial domain [150-151]	Frequency domain (DCT) [152-153]	Frequency domain (DWT) [154]	Attach the signature to the image	Attach the signature to separate file
+	. Fast . Acceptable dissimulation capacity	. Robust to JPEG compression	. Robust to JPEG2000 compression	. Good security . Robust to image processing	. Good security . High dissimulation capacity
-	. Sensitive to some acceptable image manipulations (spatial filtering...) . Low security	. Limited dissimulation capacity . Sensitive to some acceptable image manipulatitons (frequency filtering...)	. Limited dissimulation capacity . Sensitive to some acceptable image manipulations (geometrical transformations...)	. Problem of some image formats conversion	. Problem of couple integrity (Image/ Signature)

Fig. 2. Classification of image authentication methods; plus sign indicates advantages; minus sign indicates disadvantages.

as well as the possibility of restoration of image corrupted regions. Algorithms are also grouped according to the authentication tag that is used, and references are included. It can be noticed that one principal property of an image authentication system, the detection of malevolent manipulations, is not included in this table for the following reason: All described methods can detect malevolent manipulations. Moreover, the robustness against content preserving manipulations is not offered by the first two categories since they provide a strict authentication services and do not tolerate any modification to the original image. According to this summary table, algorithms performances are very similar. In fact, most of algorithms offer acceptable detection and localization of image manipulations while restoration performances still need to be improved. For strict authentication applications, where no modification to the original image is allowed, fragile watermarking algorithms perform better than algorithms based on conventional cryptography. Fragile watermarking algorithms offer high detection and localization capabilities. Moreover, some of them could provide an acceptable restoration level of damaged regions. On the other hand, selective authentication methods tolerate some desired manipulations while detecting any malevolent operations. Semi-fragile algorithms show good results for detecting and locating any malevolent manipulations while providing acceptable reconstruction performances. Unfortunately, their tolerance against desired manipulations includes mainly compression, noise addition and rotation by small angles, whereas, many of the desired manipulations need to be tolerated in practice. Since algorithms based on digital signature show more interesting results, we present them and compare their performances along with references in Fig. Figure presents a classification of image authentication methods with a detailed comparison of signature content-based methods. The comparison is made according to two important properties: the domain from which features are extracted to provide a content-based signature and the domain used to dissimulate or attach this signature. Moreover, for the sake of simplicity, only the most important weakness and strength for each group are highlighted. Every image-extracted feature used to generate the image signature has its weakness and force. The comparison of these features, their weaknesses and forces, help choosing the right method for a specific application. For example, if an application needs to tolerate compression with JPEG or JPEG2000 standard, the DCT domain or DWT domain, respectively, are best suited to generate the signature. If geometrical transformations need to be tolerated, the use of moments would be the best choice. If restoring the damaged data is important, statistical features could help well. Moreover, they are able to survive lossy image compression and a predefined set of content preserving manipulations (filtering, brightening...). On the other hand, using edges for content-based signature is undesirable for color images since one may change colors without affecting edges. This could result in an error where an image is declared authentic while some undesirable changes were introduced to it. Dissimulating signatures or attaching them to the image depends on the application and user requirements. A big dissimulation capacity and a high security can be achieved by attaching the signature to the image or to a separate file. However, the latter solution suffers from the problem of ensuring the couple image-signature integrity.

V. PROBLEM DEFINITIONS

The image authentication problem is difficult for a binary document image because of its simple binary nature that leads to perceptible changes after authentication signals are embedded in the image pixels. Such changes will arouse possible suspicions from attackers. A good solution to such binary image authentication should thus take into account not only the security issue of preventing image tampering but also the necessity of keeping the visual quality of the resulting image. In this paper, we propose an authentication method that deals with binary-like grayscale document images instead of pure binary ones and simultaneously solves the problems of image tampering detection and visual quality keeping.

VI. ADVANTAGES OF THE PROPOSED METHOD

The proposed method has several other merits, which are described in the following:

1) Providing pixel-level repairs of tampered image parts-As long as two untampered partial shares can be collected, a tampered block can be repaired at the pixel level by the proposed method. This yields a better repair effect for texts in images because text characters or letters are smaller in size with many curved strokes and need finer pixel-level repairs when tampered with.

2) Having higher possibility to survive image content attacks- By skillfully combining the Shamir scheme, the authentication signal generation, and the random embedding of multiple shares, the proposed method can survive malicious attacks of common content modifications, such as superimposition, painting, etc., as will be demonstrated by experimental results subsequently described.

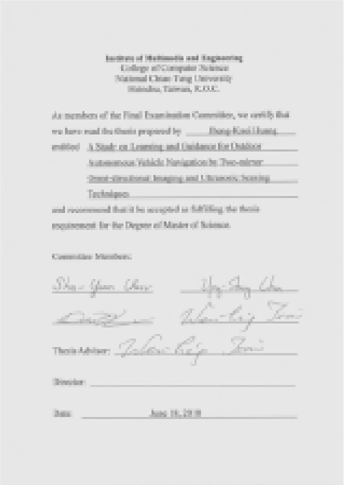
3) Making use of a new type of image channel for data hiding- Different from common types of images, a PNG image has the extra alpha channel plane that is normally used to produce transparency to the image. It is differently utilized by the proposed method for the first time as a carrier with a large space for hiding share data. As a comparison, many other methods use LSBs as the carriers of hidden data.

4) Causing no distortion to the input image- Conventional image authentication methods that usually embed authentication signals into the cover image itself will unavoidably cause destruction to the image content to a certain extent. Different from such methods, the proposed method utilizes the pixels' values of the alpha channel for the purpose of image authentication and data repairing, leaving the original image (i.e., the grayscale channel) untouched and thus causing no distortion to it. The alpha channel plane may be removed after the authentication process to get the original image.

5) Enhancing data security by secret sharing- Instead of hiding data directly into document image pixels, the proposed method embeds data in the form of shares into the alpha channel of the PNG image. The effect of this may be regarded as double-fold security protection, one fold contributed by the shares as a form of disguise of the original image data and the authentication signals and the other fold contributed by the use of the alpha channel plane.

VII. PROPOSED METHOD

A method for the authentication of document images with an additional self-repair capability for fixing tampered image data is proposed. The input cover image is assumed to be a binary-like grayscale image with two major gray values like the one shown in Fig. After the proposed method is applied, the cover image is transformed into a stego-image in the Portable Network Graphics (PNG) format with an additional alpha channel for transmission on networks or archiving in databases. The stego-image, when received or retrieved, may be verified by the proposed method for its authenticity. Integrity modifications 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 removed from the stego-image, the entire resulting image is regarded as inauthentic, meaning that the fidelity check of the image fails. The proposed method is based on the so-called (k,n) -threshold secret sharing scheme proposed by Shamir in which a secret message is transformed into shares for keeping by participants, and when of the shares, not necessarily all of them, are collected, the secret message can be lossless recovered. Such a secret sharing scheme is useful for reducing the risk of incidental partial data loss.



Institute of Multimedia and Engineering
College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.

As members of the Final Examination Committee, we certify that we have read the thesis proposed by Jhong-Kai Huang entitled A Study on Learning and Guidance for Outdoor Autonomous Vehicle Navigation by Two-mirror Omni-directional Imaging and Ultrasonic Sensing Techniques and recommend that it be accepted as fulfilling the thesis requirement for the Degree of Master of Science.

Committee Members:

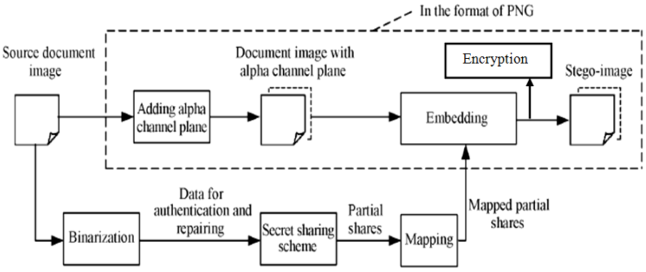
Thesis Advisor:

Director:

Date: June 18, 2008

Fig. 3. Binary-like grayscale document image with two major gray values.

Design Technologies



Block Diagram

Fig. 4. Creating a PNG image from a grayscale document image and an alpha channel.

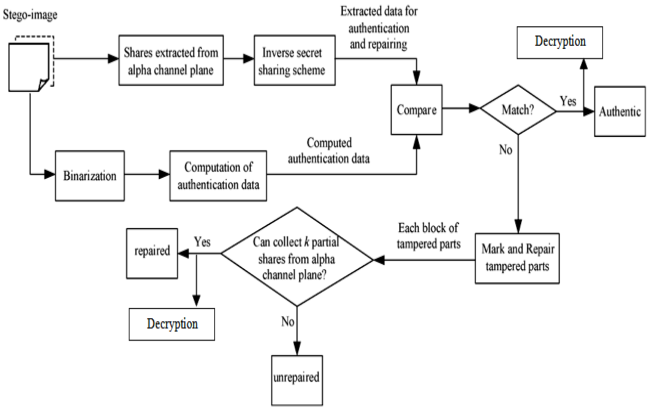

Stego-image
Shares extracted from alpha channel plane
Inverse secret sharing scheme
Extracted data for authentication and repairing
Decryption
Compare
Match?
Yes
Authentic
No
Binarization
Computation of authentication data
Computed authentication data
Each block of tampered parts
Mark and Repair tampered parts
Can collect k partial shares from alpha channel plane?
Yes
repaired
Decryption
No
unrepaired

Fig. 5. Authentication process including verification and self-repairing of a stego image in PNG format.

VIII. MATHEMATICAL EQUATIONS

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

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

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

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

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

Step 3. Select n distinct real values $x_1, x_2 \ldots. x_n$.

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

$$F(x_i) = (d + c_1 x_i + c_2 x_i^2 + \ldots. + c_{k-1} x_i^{k-1}) \bmod p \qquad (1)$$

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

Since there are k coefficients, namely, d and c_1 *through* c_{k-1} *in (1)* above, it is necessary to collect at least k shares from n participants to form k equations of the form of *(1)* to solve these k coefficients in order to recover secret d. This explains the term threshold for k and the name (k, n) - threshold for the Shamir method. Below is a description of the just-mentioned equation-solving process for secret recovery.

Algorithm 2: Secret recovery

Input: k shares collected from the n participants and the prime number p with both k and p 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

$(x_1, F(x_1)), (x_2, F(x_2)) \ldots, (x_k, F(x_k))$

To set up

$$F(x_j) = (d + c_1 x_j + \ldots.. + c_2 x_j^2 + \ldots\ldots + c_{k-1} x_j^{k-1}) \bmod p \quad (2)$$

Where $_{j = 1, 2 \ldots k.}$

Step2. Solve the k equations above by Lagrange's interpolation to obtain d as follows:

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

Step 3. Compute c1 *through* c_{k-1} by expanding the following equality and comparing the result with (2) in Step 1 while regarding variable x in the equality below to be x_j *in* (2):

$$F(x) = \Bigg[\frac{F(x_1)\quad (x - x_2)(x - x_3)\ldots(x - x_k)}{(x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_k)} + \frac{F(x_2)\quad (x - x_1)(x - x_3)\ldots(x - x_k)}{(x_2 - x_1)(x_2 - x_3)\ldots(x_2 - x_k)} + \ldots + \frac{F(x_k)\,(x - x_1)(x - x_2)\ldots(x - x_{k-1})}{(x_k - x_1)(x_k - x_2)\ldots(x_k - x_{k-1})} \Bigg] \bmod p$$

In the above algorithm is additionally included for the purpose of computing the values of parameters c_i in the proposed method. In other applications, if only the secret value d need be recovered, this step is eliminated.

IX. 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 I with two major gray values and secret key K.

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

Stage 1: Authentication Signal Generation.

Step1 (Binarization of input image) Moment preserving Threshold applied I 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 binaries I, yielding a binary version of I_b.

Step2 (Conversion of cover image into PNG format) Convert I into PNG image with an alpha channel plane I_α by creating new image layer with 100% opacity and no color as I_α and combining it with I using an image processing software package.

Step3: (RSA Algorithm) Encryption

Choose two large prime numbers p, q.

Generate two very large mersenne prime numbers as

$$m = 2p - 1 \text{ and } n = 2q - 1 \qquad (3)$$

Calculate

$$c = m * n. \qquad (4)$$

Calculate the value of Φ using the formula

$$\Phi(c) = (m-1) * (n-1) \qquad (5)$$

Generate the public key 'e' such that it is co prime with Φ(c).

Find the value of private key 'd' such that

$$(d * e) \equiv 1 \bmod \Phi(c) \qquad (6)$$

Read plaintext in the form of binary data and store it in an array (L).

Perform Le mod c (on each element of an array L) to get cipher text

Step4: (Starting of loop) take in an unrefined raster scan order of 2*3 block Bb in Ib with pixels p1 , p2…..p6

Step5: (Authentication signal generation) generate 2-bit authentication signal

$$s = a_1a_2 \text{ with } a_1 = p_1 \oplus p_2 \oplus p_3 \text{ and } a_2 = p_4 \oplus p_5 \oplus p_6 \qquad (7)$$

Step3 (Starting of loop) Take in an unrefined raster scan order of 2*3 block Bb in Ib with pixels p1 , p2…..p6

Step4 (Authentication signal generation) Generate 2-bit authentication signal $s=a_1a_2$ with $a_1=p_1 \oplus p_2 \oplus p_3$ and $a_2=p_4 \oplus p_5 \oplus p_6$.

Stage 2: Design and Embedding of Shares.

Step5 (Creation of data for secret sharing) concatenate the 8 bits of a1, a2 and p1 through p6 form an 8-bit string, divide this string into two 4-bit segments, and convert the segment into 2 decimal numbers m1and m2 respectively.

Step6 (Generation of partial shares) Set p, ci, and xi the following value apply eqn. (1) of Algorithm 1, 1) p=17 (the smallest Prime number larger than 15); 2) d=m1and c1= m2; and 3) x1=1, x2=2 …x6=6. Perform algorithm 1 as a (2, 6) threshold secret sharing scheme and generate six partial shares q1 through q6 using the following equations:

$$qi = F(xi) = (d + c1xi) \bmod p \qquad (8)$$

Where i= 1, 2… 6

Step7 (Mapping of partial shares) Add 238 to each of q1through q6, resulting in the new value of q1’ through q6’ respectively, which fall in the nearly total transparency range of 238 through 254 in the alpha channel plane Iα’.

Step 8 (Embedding two fractional shares in the current block) Take block Bα in Iα corresponding to Bb in Ib , select the first two pixels in Bα in the raster scan order and replace their values by q1 ′ and q2 ′ respectively.

Step 9 (Embedding remaining partial shares at random pixels) Use key K to select randomly four pixels in Iα but outside Bα , not the first two pixels of any block; in the raster scan order, and replace four pixels values by the remaining four partial shares q3′ through q6′ generated above, respectively.

Step10 (End of loop) If their exist any unprocessed block in Ib , then go to step 3 otherwise take the I in the PNG format.

Stage 3: PNG Image Encryption.

Step11 (Encryption of the PNG image) Encrypt the PNG image using chaotic logistic map, take the final I in PNG with encrypted format as the desired stego-image I′.

The prime number p used here is 17, so the values of q1 through q6 yield by equation (8) are between 0 and 16. After executing step 7 of above algorithm, they become q1′ through q6′ 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 q1′ through q6′ 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 be 17 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 q1′ through q6′ 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 m1 and m_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.

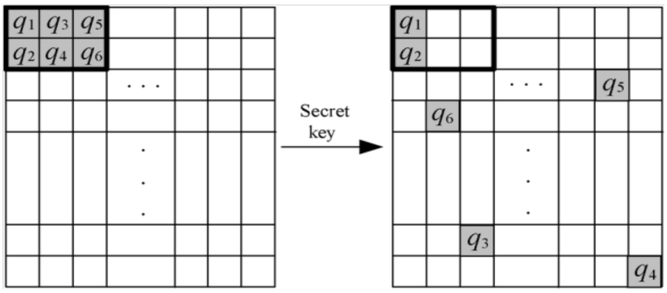


Fig. 6. Illustration of embedding six shares created for a block:
Two shares embedded at the current block, and the other four in four randomly selected pixels outside the block, with each selected pixel not being the first two ones in any block.

X. 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. DurgaBhavani1Int’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.