GREYSCALE IMAGE AUTHENTICATION AND REPAIRING

Jyoti Rao¹, Sarika Jankar²

¹, ²Department of Computer Engineering DYPIET, Pune University
jyoti.aswale@gmail.com, sarikajaankar@gmail.com

Abstract

It is very necessary to design effective methods to solve image authentication problem, particularly for images whose security must be protected. In digital documents it is necessary to provide data authentication and repairing of tampered data e.g. important documents such as certificates, scanned cheques, drawings, circuit diagrams, signed documents, design drafts etc. In this paper, a technique for authentication of images with self-repair capability for fixing tampered image data is explained. The input image is assumed to be a binary-type greyscale image with 2 main gray values. Alpha channel is combined in the greyscale image. Using the binary image, authentication signal is calculated which is then embedded in the alpha channel to create an authentic image. After embedding the authentication signal, image is encrypted. If still Content modifications of the stego-image is detected, then data is repaired at the pixel level using reverse secret sharing scheme. In case if the alpha channel is completely removed from the stego-image, the integral resulting image is regarded as unauthentic, meaning that the integrity check of the image fails. The proposed method is based on the generation of (k, n)-threshold secret sharing scheme proposed by Shamir. In this method a secret message is converted into n shares which is used as authentication signal for keeping by n participants; and when k of the n shares are collected, the secret image can be recovered without any loss[8]. This type of secret sharing scheme is helpful for reducing the risk of incidental partial data loss.

Keywords:-Alpha Channel, Secret sharing scheme, Data repair, Encryption, greyscale image

1. INTRODUCTION

The open availability of powerful digital image processing tools allows open access, changes to original data and reuse of visual materials. In fact, nowadays many people could easily create illegal copies and change images in such a way that may lead to big economic or human lives losses. These problems can be well understood with an example. A patient with a serious ill health, discovered from medical diagnostic images, may ultimately get better due to medical treatments. The medical summary of that patient involves the analysis of historic images to evaluate the succession of the sickness in time. A likely false diagnosis can put at risk the patient’s life, which is assumed to be distorted illegally, the destructed content can be repaired. This type of image content authentication and self-repair capabilities are of use for security protection of digital documents or images for important certificates, signed documents, scanned cheques, circuit diagrams, art drawings, design drafts, last will and testaments, etc. In this paper, a technique for authentication of images with extra self-repair capability for fixing tampered image data is explained. The input image is assumed to be a binary-like greyscale image with 2 main gray values. After this, the cover image undergoes malicious manipulations, compression or storage errors, such that the resultant distortions cannot be detected by the doctor. This is a case where modifications are not tolerated. It is necessary to ensure the integrity and authenticity of a digital image. It is very essential to design effectual methods to solve this type of image authentication problem. Secret image sharing scheme has been offered to solve this problem. Secret image sharing method generates several shares which are then shared in the protected image, and the protected image is reconstructed by enough different shared shares. If part of an image is verified to be distorted illegally, the destructed content can be repaired.
transparency which is transferred to PNG format and then shares are mapped with PNG format [2,4].

2. PROPOSED METHOD

The proposed method is based on the (2,6) secret sharing scheme in which random sequence of decision are made for calculation of pixel positions for embedding the shares. The alpha channel space can be utilized to embed the extra information in the image. The alpha channel embedded in the PNG image is used for creating required transparency for the image. In the proposed system the resulting alpha channel values are mapped into a range of 142 to 255. The authentication signal is generated using the optimal block size of 2 by 3 or 4 by 3 as per the size of the image (small or large size). Then these authentication signals are mapped as shares in the image. This is an image authentication method, not a secret sharing method. These embedded shares are then used for checking the integrity of the image at receiver side. For this system, input will be any type of image and output will be the Secured image/ original image without any tampering. If tampered, the system should recover it. For better performance encryption and decryption is provided. For security purpose image encryption is performed which can’t be decrypted without a key.

The given approach to secret image sharing is based on the (k, n)-threshold secret sharing method proposed by Shamir (1979). For a group of n secret sharing participants n shares are generated from a secret integer value y for the threshold k. In next part the algorithm for image authentication and repairing are explained with results.

2.1 Image Authentication and Data Repairing

2.1.1 Generating Stego-Image

This algorithm describes how the stego image is generated and stored in the PNG format.

Algorithm: Generation of a stego-image in PNG format from a given greyscale image.

Input: An image in greyscale S with two major gray values, and a secret key K.

Output: A stego-image S in the PNG format with relevant information embedded, including the authentication signals and the data for repairing.

Step A: Generation of authentication signals

(i) (Converting the Input image to Binary form) S is converted to obtain two representative gray values g1 and g2. compute T = (g1 + g2)/2. T is used as a threshold to convert S into binary form, such that the binary version S=G with 0 indicative of g1 and 1 indicative of g2.

(ii) (Conversion of the cover image into the PNG format) Convert S into a PNG image with additional alpha channel plane S by creating a new image layer.

(iii) A 2 by 3 block B of S is scanned in raster scan with pixels p1,p2... p6.

Step B: Design and Embedding of Shares

(v) (Creating data for secret sharing) p1 through p6 is concatenated to form an 6-bit string, divide the string into two 4-bit segments, and convert the segments into 2 decimal numbers m1 and m2, respectively.

(vi) (Generation of Partial Share) For secret sharing scheme explained above values are set as follows

(a) d = m1=0p1p2p3,c1 = m2=0p4p5p6
(b) x1 to x6 = Random generator is used for random values of X in the range of 0 less than xi less than 17 [1];

(d) following equation is executed as a (2, 6)-threshold secret sharing scheme [8] to generate six partial shares q1 through q6

\[ q_i = F(x_i) = (d + c_0 x_1 + c_1 x_2 + ... + c_{k-1} x_{k-1}) \] ………….(1)

Where i = 1, 2.... 6.

(vii) (Map the partial shares) Adding 142 to each of q1 through q6, resulting in the new values of q1 , through q6 , respectively, which fall in the nearly transparency range of 142 through 254 in the alpha channel plane Sα.

\[ qd_i = q_i +142; \]

(viii) (Embedding of shares at random pixels) Use the key K to choose randomly 6 pixels in but outside the current block , which are not selected so far in this step and in the raster scan order change the six pixels values by the six partial shares qd1 through qd6 generated above.

Fig. 1 Stego image from greyscale image & binary image

(ix) If there exists any unprocessed block in Sb, then go to (ii), if not, take the final S in the PNG format as the preferred stego-image Sα. After execution of (vii) the above algorithm, they become q1 through q6 , respectively, which all fall into an interval of integers ranging from 142 to 254.
Consequent embedding of q1 to q6 in such a narrow distance into the alpha channel plane means very alike values will appear everywhere in the image block, resulting in an almost consistent transparency effect, which will not stimulate notice from an attacker.

![Diagram of share embedding](image)

**Figure 2:** Embedding of 6 shares generated for a given block, shares are embedded in randomly selected pixels outside the block.

![Diagram of Stego image Authentication process](image)

**Figure 3:** Stego image Authentication process including verification and Self-repairing.
2.1.2. STEGO-IMAGE AUTHENTICATION

A complete algorithm describing the stego-image authentication process, including both verification and self-repairing of the original image content, is described in Fig. 3.

**Algorithm:** Authentication of a stego-image.

**Input:** A stego-image $S$, the representative gray values $g_1$ and $g_2$, and the secret key $K$.

**Output:** Marked tampered image $S_r$ and data repaired if possible.

Part 1: Drawing out the embedded two representative gray values.

Step 1: (Stego-image to Binary form conversion)

Compute $T = (g_1 + g_2)/2$ and use it as a threshold to convert $S$ into Binary Form, yielding the binary version $S_b$ of $S$ with "0" representing $g_1$ and "1" representing $g_2$.

Part 2: Stego-image authentication.

Step 2: (Start looping) Take in a raster-scan order an unprocessed block $B_b$ from $S_b$ with pixel values $p_1$ through $p_6$, and find the 6 pixel values $q_{d1}$ through $q_{d6}$ of the corresponding block $B_{b'}$ in the alpha channel plane $S_{a'}$ of $S'$.

Step 3: (Extraction of the secreted authentication signal) to extract the six bits hidden as authentication signal $q_d$ from $B$ follow the steps:

1. Subtract 142 from each of the untampered $q_{d1}$ and $q_{d2}$ partial shares of $B_b$. With the shares $(x_i, q_i)$ and $(x_j, q_j)$ as input, solve the 2 equations by Lagrange’s interpolation [8] to obtain the 2 values $d$ and $c_1$ (the secret and the coefficient value, respectively).

2. Now convert this $d$ and $c_1$ into two 4-bit binary values, and then an 8-bit string is formed by concatenating these binary values [8].

Step 4: (Matching the secreted and computed authentication signals and marking of tampered blocks)

Calculate the $q_{1}$ to $q_{6}$ values for 2 by 3 block of $S_b$. Match the new calculated $q_{1}$ to $q_{6}$ with old embedded (in alpha channel) $q_{1}$ to $q_{6}$ and if any variance occurs, mark $B_{b'}$, the corresponding block $B$ in $S$, and all the partial shares embedded in $B$ as tampered.

Step 5: (Repairing of the tampered part)

If possible using the binary values of $d$ & $c_1$ find pixels $p_1$ through $p_6$.

Check the tampered pixels then try to repair the values using the extracted binary $b$ & $c_1$.

Put $g_1$ if pixel value is $1$ & $g_2$ if pixel value is $1$ in received $S$ image. If sufficient i.e. 2 untampered authentication signal ($q_i, q_j$) is available then only repairing is possible. If all the signals are tampered, repairing is not possible.

Step 6: (Exit loop)

If there is any unprocessed block in $S_b$, then go to Step 2; otherwise, go on.

3. RESULTS AND DISCUSSION

The security of the information embedded in the stego image can be improved by using the randomization of the constant values of $x_{1}$ to $x_{6}$ used in step 6 of algorithm 2.1.1. If the values of $x_{1}$ to $x_{6}$ is used from 1 to 6, $(1,q_1)$ and $(2,q_2)$ can be forged[2]. So it is possible to generate a counterfeit authentication signal. In proposed system random values within the range of 0 to 17 are used. So the possibility of correctly guessing all these values for all the $m \times n / 6$ blocks in a stego-image can be approximately $1/[(17 \times 16 \times 15 \times 14 \times 13 \times 12)] m \times n / 6$.

The following diagram explains the original image output & the changed image output. In right part image is changed / deleted which is repaired at the receiver side. Though it is not possible to repair the image successfully it detects the tampering correctly. But if someone changes the bits within the range of mid then it is not possible to detect the tampering.

**CONCLUSIONS**

An image authentication method along with a data repair capability for binary-like greyscale images i.e. black and white based on secret sharing is explained. Both the generated authentication signal and the content of a block are transformed into partial shares by the Shamir method, which are then distributed into an alpha channel plane to create a stego-image in the PNG format. Here to avoid the security constraint random values of $X_{1}$ through $X_{6}$ are used. For self-repairing the content of a tampered block, the reverse Shamir scheme is used to calculate the original form of the block from any 2 untampered shares. It may possible that embedded alpha channel gets tampered, so to avoid this the encryption and decryption of stego-image is provided. A measure for enhancing the protection of the data embedded in the alpha channel plane is also specified.
REFERENCES


[6] Improvements Of Image Sharing With Steganography And Authentication Ching-Nung Yang, Tse-Shih Chen, Kun Hsuan Yu, Chung-Chun Wang Department Of Computer Science And Information Engineering, National Dong Hwa University, Sec. 2, Da Hsueh Rd., Hualien, Taiwan Received 22 October 2005;


Figure 4: a] original image b] image changed with Photoshop c] changed image with original Authentication signal d] Repaired image of fig.c
[10] Younho LEE, Junbeom HUR, Heeyoul KIM, Nonmembers, Yongsu PARK and Hyunsoo YOON Members
"A NEW BINARY IMAGE AUTHENTICATION SCHEME WITH SMALL DISTORTION AND LOW FALSE NEGATIVE RATES" IEICE Transaction on communication, VOL E90-B No.11 Nov 2007