INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Color Image Integrity Verification Using Shamir's Secret Sharing Scheme

Gnaneshwar G.
M.Tech (Software Engineering), Department of Information Science
P.E.S. Institute of Technology, Bangalore, Karnataka, India

Abstract:
A Novel watermarking technique to verify the integrity of the lossless color image (BMP image) using Shamir's (k,n)-threshold Secret-Sharing Scheme via the use of Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of color image which is transformed into several shares using Shamir's secret sharing scheme. The coefficients of the polynomial used by the Shamir's method are used as carriers to carry given authentication signals. The partial shares are embedded into an alpha channel plane. The alpha channel plane is then combined with the original lossless BMP color image to form a PNG image. Undesired white noise created in the resulting transparent stego-image is removed by carefully mapping the computed share values into a range of alpha channel values near their maximum value of 255 in the embedding process. In the process of verifying the integrity of the image the authentication signals are computed from the current block which is then compared with the extracted shares from the alpha channel plane for the corresponding block. If the authentication signals doesn't match then that block is marked as tampered. The proposed image authentication method possesses the merits of losslessness during image verification, high sensitivity to image alterations, good tampering localization capability, and very low false acceptance and rejection ratios. Experimental results proving the effectiveness of the proposed methods are also included.

Keywords: *Alpha channel, color image authentication, data hiding, fragile watermarking, secret sharing, portable network graphics (PNG) image, tamper detection, tamper localization*

1. Introduction

DIGITAL image is a form for preserving important information. However, with the fast advance of digital technologies, digital images can be easily and illegally duplicated and manipulated. It is easy to make visually imperceptible modifications to the contents of digital images. Digital image authentication and integrity verification have become a popular research area in recent years. It is desirable to design effective methods to solve this kind of image authentication problem [1], [2], [3] particularly for images of documents whose security must be protected.

Data Hiding is a process of a process of embedding information into a certain digital file that acts as a host. Through data hiding techniques, information such as authentication signals can be embedded into a digital file for the purpose of verifying the integrity or fidelity of the file [1], [2], [3], [4]. In the application of copyright protection, an owner of a digital file can use data hiding techniques to embed a visible or invisible digital watermark into the file content to claim the ownership of the content [5], [6], [7], [8]. Another application of data hiding is covert communication [9], [10] in which people hide a secret message into a cover file, resulting in a stego-file; and a receiver of the latter can extract the hidden message from the stego-file to complete the communication.

In addition, *Information sharing* was proposed to protect the security of the concerned data by transforming a secret message into several shares which are then distributed to a number of participants to keep. Sucha secret sharing scheme issue full for reducing the risk of incidental data loss and advantageous for keeping a balance among the participants: only when all the shares or a sufficient number of them are collected from the participants can the secret message be recovered correctly. This concept of secret sharing was proposed first by Shamir [11]. Conventionally, data hiding and information sharing aret wo irrelevant issues in the domain of information security.

2. Existing Techniques

In the literature, many data hiding methods exploring the spatial domain and frequency domain of images [12], [13], [14], [15], [16] have been proposed. Bender et al. [12] proposed the technique of least-significant-bit (LSB) replacement, in which a secret message is embedded in the least significant bits of image pixel values. Mielikainen [13] proposed a modified LSB replacement method which embeds as many bits as the conventional method, but changes less pixel values. Yang et al. [14] proposed an adaptive k-LSB substitution method in which larger values of k are adopted in the edge areas of the cover image and smaller ones are used for the

smooth areas. Wang et al. [15] transformed image block contents into coefficients in the frequency domain by the discrete cosine transform (DCT) and embedded secret bits by modifying the magnitude relations between the AC values of image blocks. Besides data embedding techniques using the DCT, the discrete wavelet transform (DWT) [17] and the discrete Fourier transform (DFT) [18], [19] have also been used.

From another view point, different types of images and files can be used as cover media for developing data hiding [20], [21]. In [21], Lee and Wu proposed a lossless data hiding method for palette-based images, which adjusts palette colors and image data to embed secret data and side information for reconstruction of the original image content. Lee and Tsai [9] hid data into PDF files' characters by using special ASCII codes. Liu [10] made use of the change tracking function in Microsoft Word to hide data by a document degeneration technique.

In this paper, in addition to the aforementioned spatial domain, frequency domain and palettes of images for use in data hiding, we try to explore a new embeddable space for data hiding, aiming at providing more data hiding capacity, better quality of the resulting stego-image and stronger applicability. As a result, the PNG image with the alpha channel plane is found to be capable of meeting these requirements mentioned previously. Specifically, in the information-sharing-based data hiding method proposed in this study, a PNG image is used as the cover image in which the alpha-channel value of each pixel is set to be 255 initially. That is, the cover image is a totally transparent color one at the beginning of the proposed data hiding process. The authentication signals calculated by taking six pixels at a time is transformed into shares by the Shamir's secret sharing method, which is then embedded into the alpha-channel plane of the PNG image. Coefficient parameters involved in the Shamir method are used as carriers of the data to be hidden in the proposed method. A prime number used in the method, which is found to dominate the resulting visual quality and data hiding capacity of the stego-image, is properly selected. Also, a mapping function is designed for adjusting the alpha-channel values to create uniform transparency in the alpha-channel plane, resulting in an imperceptible effect in the stego-image. The original R, G, and B channels are untouched so that the original image appearance revealed by the color information of these three channels is kept.

3. Proposed System

In the proposed system the concepts of data hiding and information sharing are used for the application of image authentication. An input image with RGB channels (BMP image) which needs to be protected is first transformed into a PNG image, by using any image editing software, with the alpha channel values all set initially set to 255. The BMP image is processed next by dividing the pixels of image into blocks of six pixels each and color dependent authentication signals are generated for each block. These signals are taken as input to Shamir's secret sharing scheme to generate six partial shares out of which any two shares are then embedded into the alpha channel plane of the PNG image to create a stego-image. This stego-image is then transferred over the network to the other communicating party. At the receiving end, the stego-image can be verified for its integrity by generating the authentication signals from the color values of six pixels of each block of the image In the proposed system the concepts of data hiding and information sharing are used for the application of image authentication. An input image with RGB channels (BMP image) which needs to be protected is first transformed into a PNG image, by using any image editing software, with the alpha channel values all set initially set to 255. The BMP image is processed next by dividing the pixels of image into blocks of six pixels each and color dependent authentication signals are generated for each block. These signals are taken as input to Shamir's secret sharing scheme to generate six partial shares out of which any two shares are then embedded into the alpha channel plane of the PNG image to create a stego-image. This stego-image is then transferred over the network to the other communicating party. At the receiving end, the stego-image can be verified for its integrity by generating the authentication signals from the color values of six pixels of each block of the image and this is compared with the extracted authentication signals of the corresponding blocks which were embedded in the alpha channel plane of the stego-image. If the authentication signals match then that block of pixels in the image are not tampered. If the authentication signals does not match then that block of pixels in the image is marked as tampered. Fig 1 illustrates the process of authentication signals generation and embedding in the proposed color image authentication method, and Fig 2 illustrates the image verification process of the propose method. Detailed explanation of the generation of authentication signal and image verification process is discussed in Algorithm 1 and Algorithm 2 respectively.

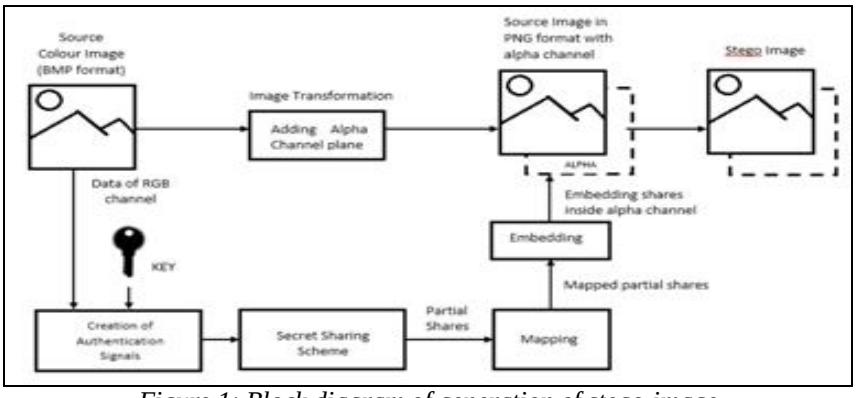

Figure 1: Block diagram of generation of stego-image

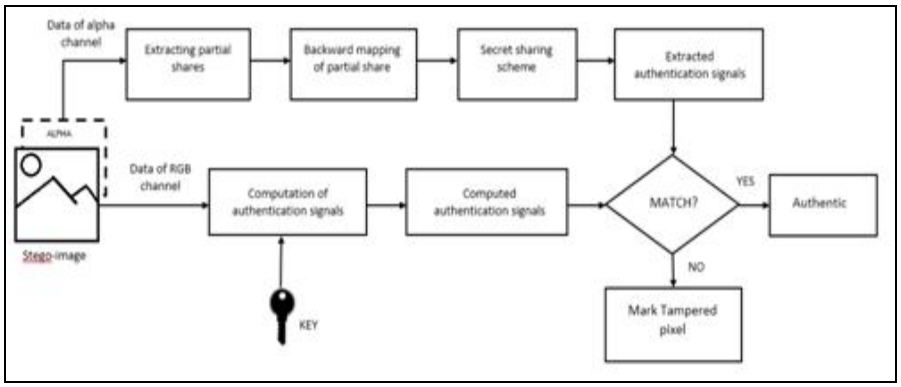

Figure 2: Block diagram of stego-image verification process

Algorithm 1: Authentication signal generation and embedding process

- **Input:** Color image I in BMP format and secret key K.
- **Output:** Stego-image I' in PNG format with authentication signals embedded inside.

Steps:

Step 1. (*Transforming the source colour image in BMP format into PNG format*) Transform I into a PNG image with an alpha channel plane by creating a new image layer with 100% opacity and no color and combining it with I to form $I_a$using an image processing software package.

Step 2. (*Initialization and beginning of looping*) Take in a raster-scan order 2X3 block B of image I with six pixels p_1, p_2, … p_6 from I, and use K as the seed for a random number generator to get a number sequence $S=S_1, S_2, S_3$.

Step 3. (*Creation of authentication signals*) For each of p_1, p_2… p_6, denoted as p_i, perform the following steps.

3.1 Take the R, G, and B values of p_i, denoted as V_R, V_G, and V_B, respectively.

3.2 Take in order three elements from S, denoted as S_1, S_2, and S_3, to perform the following operations to obtain three bits r, g, and b, respectively:

$(V_R + S_1) \bmod 2 = r$;

$(V_G + S_2) \bmod 2 = g$;

$(V_B + S_3) \bmod 2 = b$:

3.3 Concatenate r, g, and b as a 3-bit string rgb, for p_i.

Generate 6 bit authentication signal $s=a_1a_2$ where

$a_1 = p_1 \oplus p_2 \oplus p_3$ and

$a_2 = p_4 \oplus p_5 \oplus p_6$ where $\oplus$ denotes the exclusive-OR operation.

Transform a_1 and a_2 into two decimal numbers m_1 and m_2 respectively.

Step 4. (*Partial share generation*) Set p=11 (smallest prime number larger than 7), $d = m_1$ and $c_1 = m_2$ and $x_1=1$, $x_2=2$… $x_6=6$. Perform (2,6) threshold secret sharing scheme to generate six partial shares q_1 through q_6 using the following equation

$q_i = F(x_i)=(d+c_1x_i) \bmod p$ where i=1,2,…,6.

Step 5. (*Mapping the partial shares*) Add 244 to each of q_1 through q_6 resulting in the new values q_1' through q_6' which falls in the nearly total transparency range of 244 through 254 in the alpha channel plane.

Step 6. (*Authentication signal embedding into three pixels*) Take each block in the alpha plane and embed any two authentication signals between q_1' and q_6' into first two pixels of the block in I.

Step 7. (*End of looping*) If there exists any unprocessed pixel in I, then go to Step2; otherwise, take the final I as the desired stego-image I'.

Algorithm 2: Authentication signal verification

- **Input:** A protected stego-image I' created by Algorithm 5, and a key K used there.
- **Output:** Image I' with altered pixels, if found, marked as tampered.

Steps:

Step 1. (*Initialization and beginning of looping*) Take in a raster-scan order 2X3 block B with six pixels p_1, p_2, p_3, p_4, p_5 and p_6 from I', let their alpha-channel values be denoted as q_1', q_2', q_3', q_4', q_5' and q_6' respectively; and use K as the seed for a random number generator to generate a random number sequence $S=S_1$, S_2 and S_3.

Step 2. (*Extraction of authentication signals embedded in alpha channels*) Extract only the first two alpha-channel values q_1' and q_2' and subtract 244 from each alpha-channel value to get the partial shares q_1 and q_2. Using Shamir's reverse secret sharing scheme take q_1 and q_2 as input to retrieve the secret and the coefficient, m_1' and m_2' respectively, as output.

Step 3. (*Computation of authentication signals from pixels' color values*) For each of p_1, p_2, p_3, p_4, p_5 and p_6, denoted as p_i, perform the following steps.

3.1. Take the R, G, and B values of pi, denoted as V_R, V_G, and V_B, respectively.
3.2. Take in order three elements from S, denoted as S_1, S_2, and S_3, to perform the following operations to obtain three bits r, g, and b, respectively:
$(V_R + S_1) \bmod 2 = r$;
$(V_G + S_2) \bmod 2 = g$;
$(V_B + S_3) \bmod 2 = b$.
3.3. Concatenate r, g, and b as a 3-bitstring rgb, for p_i.
Generate 6 bit authentication signal $s=a_1a_2$ where

$a_1 = p_1 \oplus p_2 \oplus p_3$ and

$a_2 = p_4 \oplus p_5 \oplus p_6$ where $\oplus$ denotes the exclusive-OR operation.
Transform a_1 and a_2 into two decimal numbers m_1 and m_2 respectively.
Step 4. (*Matching of extracted and computed authentication signals*) Match m_1 and m_2 with m_1' and m_2', respectively, and if there exists any mismatched pair, then mark the corresponding block as being tampered within the input image I'.
Step 5. (*End of looping*) If there exists any unprocessed pixel in I', then goto Step1; otherwise, take the final image I', possibly marked as tampered, as output.

4. Experimental Results

In this section, we show some experimental results of applying the proposed image authentication algorithms –
Algorithm 1 and Algorithm 2 to verify stego-images attacked by two common image editing operations i.e., superimposing and painting.
Table 1 displays the statistics of the performance of proposed method shown by the above experimental results in terms of three parameters: detection ratio, false acceptance ratio and false rejection ratio which are defined by the following:

- Detection ratio = (number of detected pixels) / (number of tampered pixels).
- False acceptance ratio = (numbered of tampered pixels marked as untampered)/ (total number of tampered pixels).
- False rejection ratio = (number of untampered pixels marked as tampered)/ (total number of untampered pixels).

It was found that if the superimposing operation is used in the attack, the alpha channel values will be replaced with the new value 255 at the attacked part. Since the largest alpha channel value generated by the proposed method is 254 (see Step 5 in Algorithm 1), attacked pixels can be easily detected and marked by checking the existence of the specific value 255 in the alpha channel. As an example, Fig. 1(a) shows a source image of an airport runway in BMP format and Fig. 1(c) is the stego-image of airport runway. In Fig. 1(d), the stego-image was attacked by superimposing a fake airplane on the runway. Fig. 10(e) shows the authentication result in which all altered blocks of pixels were detected and marked in black. Both the false acceptance ratio and false rejection ratio are 0% for the reason that, as mentioned previously, alpha channel values 255 only occur at attacked pixels.
Another kind of attack used to alter the content of stego-image is Painting attack. In this attack painting operation is used to alter the stego-image by using the color of the background. As an example, Fig. 2(a) and (c) are respectively an input source image ''eagle with fish'' and a generated stego-image. In Fig. 2(d), the fish is removed from the eagle's claws by painting color similar to the background sky. The authentication result generated from Algorithm 2 is shown in Fig. 2(e) in which tampered regions were successfully detected and marked in black. However, as can be seen, some tampered pixels were not detected and appeared as noise in the marked region. This phenomenon results from the case that the authentication signals extracted from the alpha channel incidentally match the authentication signals computed from the tampered pixels. Since the authentication signal of each pixel is com- posed of three bits, there is a probability of 1/8 for an erroneous authentication, leading to a false acceptance ratio of around 12.5%.

Figure 3: Results of Superimposing Attack. (a) Source image in BMP format, (b) Source image transformed to PNG format, (c) Stego-image with authentication signals embedded inside it, (d) Stego-image is tampered by superimposing an airplane, (e) Verification of stego-image by detecting and localizing the tampered area

Figure 4: Results of Painting Attack. (a) Source image in BMP format, (b) Source image transformed to PNG format, (c) Stego-image with authentication signals embedded inside it, (d) Stego-image is tempered by removing the fish by painting operation, (e) Verification of stego-image by detecting and localizing the tampered area

5. Conclusion

A new lossless color image verification technique based on data hiding and information sharing has been proposed. The authentication signals are generated from the source BMP image and converted into partial shares by using Shamir's secret sharing scheme. The generated partial shares values are then mapped skillfully so that they lie close to the maximum transparency value of 255 to create a consistent opaque effect and reduce white noise. Data hiding is achieved by embedding the generated share values into the alpha channel plane of the PNG image. In image verification process, the block is marked as tampered if the computed authentication signals doesn't match with the extracted authentication signals. Experimental results prove the effectiveness of the proposed method in the aspect of tampering detection ratio, false acceptance ratio and false rejection ratio. The proposed method is first of its kind to verify the integrity of lossless image in BMP format.

6. References

1. C.S. Lu, H.Y.M. Liao, Multipurpose watermarking for image authentication and protection, IEEE Transactions on Image Processing 10 (10) (2001) 1579–1592.
2. C.W. Lee, W.H. Tsai, A secret-sharing-based method for authentication of grayscale document images via the use of the png image with a data repair capability, IEEE Transactions on Image Processing 21 (1) (2012) 207–218.
3. A. Shamir, How to share a secret, Communication of the ACM 22 (11) (1979) 612–613.
4. G.J. Yu, C.S. Lu, H.Y.M. Liao, Mean quantization-based fragile water- marking for image authentication, Optical Engineering 40 (7) (2001) 1396–1408.
5. C.W. Lee, W.H. Tsai, Optimal pixel-level self-repairing authentication method for grayscale images under a minimax criterion of distortion reduction, Optical Engineering 51 (5) (2012). 057006-1- 057006-10.
6. X. Gao, X. Li, D. Tao, C. Deng, J. Li, Robust reversible watermarking via clustering and enhanced pixel-wise masking, IEEE Transactions on Image Processing 21 (8) (2012) 3598–3611