Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **3**, May **2015**

Color PNG Image Authentication Scheme Based on Rehashing and Secret Sharing Method

Wan-Li Lyu[1,2] and Chin-Chen Chang[2]

[1]Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education
School of Computer Science and Technology
Anhui University
Hefei 230039, China

[2]Department of Information Engineering and Computer Science
Feng Chia University
100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC
wanly_lv@163.com, alan3c@gmail.com

Feng Wang

Department of Mathematics and Physics
Fujian University of Technology
Fuzhou, Fujian, 350108, China
w.h.feng@163.com

Received June, 2014; revised February, 2015

Abstract. *An authentication scheme that uses rehashing and secret sharing methods to verify the reality of a color image's content is proposed in this paper. First, the proposed scheme uses Shamir's secret sharing method to share image features. Second, the proposed scheme innovatively utilizes the rehashing method to overcome easy collisions of the random numbers to enhance the effectiveness against attacks. Third, the proposed method utilizes Portable Network Graphics images to hide authentication messages. Using the rehashing method, the collisions take up little in address space, making the process suitable for processing authentication messages. The experimental results indicated that the proposed scheme had very low false acceptance and rejection ratios and verified that the rehashing method can be used in image authentication applications.*
Keywords: Image authentication, Perfect hash, Rehashing, Secret sharing, Portable Network Graphics (PNG) image

1. **Introduction.** It is very easy to manipulate digital images that are used extensively on the Internet The use of image authentication technology with some additional message added can verify whether someone has tampered with an image. There are essentially three steps are required to authenticate the integrity of an image.

The first step is to extract the content of the image as authentication messages. Several of the image hash methods [1-6] that have been proposed in many papers can be used for this aim The hash value of the image is organized with a tag and then appended to the original image I. The tag is computed by a hash function $h(K, I)$ The hash value that is applied to an image must have the properties that similar images should have the same hash values, and visually distinct images should produce different hash values. The image hash method has the advantage that considered the original image features as a whole while short of details arrangement. Some digital watermarking authentication methods

[7] use a binary random sequence that serves as the authentication code, while the binary random sequence cannot denote the features of original image and led to a relatively poor authentication result. Some digital watermarking authentication methods [8-11] extract the features of the original image as watermarks, which are embedded into the original image, creating a watermarked image that is transmitted to the receiver.

The second step is to process the authentication messages. Block-based watermarking authentication methods [11] can verify whether tampering has occurred and where it is located in the potential modified image. Some block-based watermarking authentication techniques confuse the watermark in the second step against a copy-paste attack [7,12] which utilizes some pixels of authentication image itself to tamper other pixels. This leads to another weakness in that the feature value of the paste region has changed, and this can either locate the correct tamper position or the watermark value of the paste region could also change, which would locate the wrong tamper position. Other block-based watermarking authentication techniques add a watermark unit with a random number [13], which also is sent to the receiver with the aim of protecting against the copy-paste attack, and only the original copy region has the correct random values, allowing the paste region to be located. Because the embedding capacity of watermarking algorithms is limited, the random numbers should be very short to avoid many collisions in which different watermark units have the same random numbers, making it impossible to locate many of the tamper units. The design of the random number is important to avoid unsuccessful authentication results. Hashing is a key-to-address transformation technique in which the key space can be mapped into the address space.

The third step is to combine the image's digest and the image itself. Many data hiding methods can be used for this purpose with the help of embedding authentication messages in the spatial [12, 14] or frequency domains [7, 15]. However, these data hiding methods modify the original images' content to a slightly greater extent. The proposed method utilizes Portable Network Graphics (PNG) images to hide the authentication messages. PNG is the most commonly used lossless image compression format on the Internet, and PNG gives a much wider range of transparency options with alpha channel transparency.

The paper proposed a color PNG image authentication scheme. In the first step, the proposed scheme uses Shamir's secret sharing method to share the images' features as a watermark. In the second step, the proposed scheme aims to locate the position of the copy-paste tamper, and innovatively utilizes the rehashing method to overcome easy collisions of the random numbers in order to enhance the ability to resist attacks. In the third step, the proposed method embeds the values of the image's features in the alpha channel, avoids modifying the RGB channel, and effectively protects the original image.

The rest of the paper is organized as follows. Section 2 briefly introduces and discusses Du et al' rehashing method[16] and Shamir' secret sharing method [17, 18]. In Section 3, our PNG image authentication scheme based on rehashing and secret sharing method is described in detail. The experimental results are reported in Section 4. Finally, conclusions appear in Section 5.

2. **Related Work.**

2.1. **Du et al.'s Rehashing Method[16].**

Hashing is a key-to-address transformation technique, and is considered to be an effective means of organizing and retrieving data in practical applications, such as database management, compiler construction, and many other applications.

If a hash function has the feature that from the set of keys in the key space to the address space is one-to-one; this makes the hash function much easier to use because the

key collision problem can be avoided. Sprugnoli [19] called the one-to-one hash function the 'perfect hashing function'. Du [16] proposed an approach to design a perfect hash function with an indicator table called the "hash indicator table" (HIT). With the help of the HIT, several random hash functions can be organized to construct the desired perfect hash function.

Assume that the key space has n distinct keys $K_1, K_2, \cdots, K_n$, and assume that the address space has m entries. The use of a single hash function h_i, which is selected randomly from the $F_{n\times m}$, where $F_{n\times m}$ is the set of the map from the key space to the address space, would result in many collisions in the address space. Let $P_i(m,n)$ denote the probability that the hash function has $i(0 \le i \le \min(m,n))$ entries in the address space with only one key hashed to them. The $P_i(m,n)$ can be computed as shown in Equation (1):

$$P_i(m,n) = \frac{e_i(m,n)}{m^n}, \text{where } e_i(m,n) = n! \binom{m}{i} \sum_{r=0}^{n-i} (-1)^r \binom{m-i}{r} \frac{(m-r-i)^{n-r-i}}{(n-r-i)!} \quad (1)$$

The expected values of i for $P_i(m,n)$ are 3.8742, 7.5471, and 11.2240, and the probabilities are 1.67%, 0.020501% and 0.00030913% when $i \ge 0.8n$ and $m = n = 10, 20, 30$, respectively. The expectation of i for $P_i(m,n)$ approaches $\frac{n}{e}$ is very large when $m = n$.

However, the use of a number of functions $h_1, h_2, \cdots, h_s$, which are called the "rehashing model", is much better. The relationship between the keys and the selected hash functions is stored in the HIT.

Let $P_i^s(m,n)$ denote the probability that Algorithm 1 has $i(0 \le i \le \min(m,n))$ entries in the address space with only one key hashed to them. The $P_i^s(m,n)$ can be computed with Equation (2):

$$\begin{aligned} P_i^s(m,n) &= \sum_{r=0}^{i} P_r^{s-1}(m,n) \cdot Q_{i-r}(m,n,r), \text{where} \\ Q_i(m,n,j) &= \left(\frac{j}{m}\right)^{n-j} \sum_{r=0}^{n-j} \binom{n-j}{r} \frac{e_i(r,m-j)}{j^r}, \text{and } P_i^1(m,n) = P_i(m,n) \end{aligned} \quad (2)$$

The expected values of i for $P_i^7(m,n)$ are 8.8000, 17.4644, and 26.0698, and the probabilities are 96.41%, 97.17% and 97.84% when $i \ge 0.8n$ and $m = n = 10, 20, 30$, respectively. Compared with using a single hashing function, in our proposed scheme, the collisions of using rehashing functions are few and suitable for calculating the address. They also can be used for processing the authentication messages.

2.2. **Shamir's Method [17] for Secret Sharing.** Shamir proposed a (k,n)-threshold secret sharing method, with which a secret integer S is transformed into n shares and distributed to n participants. And at least k of the n shares are collected to recover the secret integer, where $k \le n$. Shamir's method has the advantage that the participants can reconstruct the original message, so the proposed scheme uses Shamir's method to share an image's features.

3. Proposed Scheme for PNG Image Authentication.

The PNG image is created from an RGB color image I and an alpha channel plane. An illustration of this process of PNG image creation is shown in Fig. 1.

The proposed scheme embeds the authentication bits into the alpha channel plane, while the input color image is not modified in contrast with traditional authentication methods.

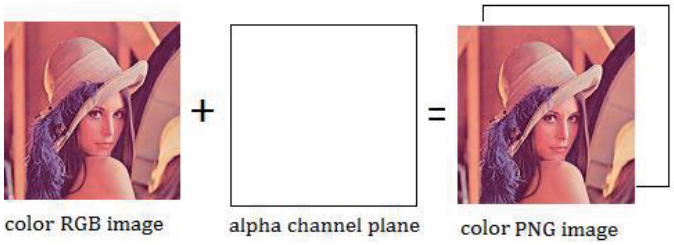

FIGURE 1. Illustration of using a color RGB image and an alpha channel plane to create a color PNG image

Based on the rehashing functions described previously, the basic idea of the proposed scheme for getting a PNG image for use in image authentication is described as Fig. 2 shows.

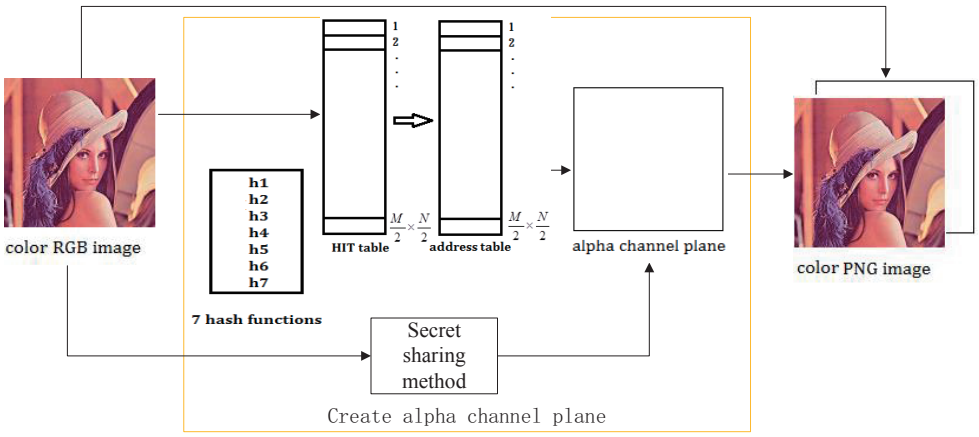

FIGURE 2. Illustration of using rehashing and the secret sharing scheme to create a color PNG image used for image authentication

First, as Fig. 2 shows, the proposed scheme constructs seven random hash functions. Using the rehashing method, design the HIT and hash address table (HAT) of image I, and the size of image I is $M \times N$. For a color image, many pixels have the same value and are not suitable for use as hashing keys. However, the locations of all of the pixels are distinctive, so the proposed method uses the positions of the pixels as hashing keys.

Second, the proposed scheme computes the feature value of image I and uses the secret sharing method to share the feature The size of image I is $M \times N$. Segment image I into nonoverlapped blocks $B_1, B_2, \cdots, B_{\frac{M}{2}\times\frac{N}{2}}$ the size of each block is 2×2. The proposed method uses the RGB channel of block $B_k, (1 \leq k \leq \frac{M}{2} \times \frac{N}{2})$ and uses Shamir's secret sharing method to compute sharing messages of each block B_k

Third, the proposed scheme embeds the sharing messages into the alpha channel and constructs the color PNG image I'. In the color PNG image I', a block of alpha plane $Balpha_k, (1 \leq k \leq \frac{M}{2} \times \frac{N}{2})$ also consists of four elements, i.e.,$b(1,1)$, $b(1,2)$ $b(2,1)$ and $b(2,2)$, as shown in Fig. 3.

The proposed scheme constructs an alpha channel of RGB image I for a pixel $p(i,j)(1 \leq i \leq M, 1 \leq j \leq N)$, of RGB image I also belongs to block $B_{\lfloor\frac{i}{2}\rfloor\times\frac{N}{2}+\lfloor\frac{j}{2}\rfloor+1}$, HIT$(\lfloor\frac{i}{2}\rfloor \times \frac{N}{2} + \lfloor\frac{j}{2}\rfloor + 1)$ is hidden in position $b(1,1)$ of the alpha channel block $Balpha_{\lfloor\frac{i}{2}\rfloor\times\frac{N}{2}+\lfloor\frac{j}{2}\rfloor+1}$ and the feature of block $B_{\lfloor\frac{i}{2}\rfloor\times\frac{N}{2}+\lfloor\frac{j}{2}\rfloor+1}$ is hidden in positions $b(1,2), b(2,1)$and $b(2,2)$ of block $Balpha_{\text{HAT}(B_{\lfloor\frac{i}{2}\rfloor\times\frac{N}{2}+\lfloor\frac{j}{2}\rfloor+1})}$. The alpha channel block $Balpha_{\lfloor\frac{i}{2}\rfloor\times\frac{N}{2}+\lfloor\frac{j}{2}\rfloor+1}$includes

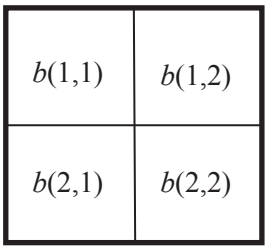

FIGURE 3. Arrangement of the four elements in a block $Balpha_k$

position information of current block, and it includes feature information of the other block. This method can distinguish the original block from the paste block which can resist copy-paste attacks effectively. When all blocks of the alpha channel have been computed, the alpha channel of image I is obtained. With the original RGB image I and the alpha channel of image I, the PNG image I' is obtained and can be used for image authentication.

3.1. **Construct seven random hash functions and design the hash location table (HLT).** The size of image I is $M \times N$. Use S as the seed for a random number generator to get seven random numbers $S_1, S_2, \cdots, S_7$, and then use the seven random numbers $S_1, S_2, \cdots, S_7$ as the random number generators to construct seven hash functions $h_1, h_2, \cdots, h_7$, each of which has the size of $\frac{M}{2} \times \frac{N}{2}$, and the range of the values of the hash functions $h_1, h_2, \cdots, h_7$ is $(1 \leq h_i(S_j) \leq \frac{M}{2} \times \frac{N}{2})$ where $1 \leq i \leq 7$ and $1 \leq j \leq \frac{M}{2} \times \frac{N}{2}$.

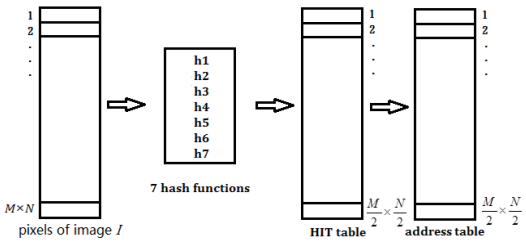

FIGURE 4. Using seven hash functions to compute values of the HIT table and the address table

For a color image, many pixels have the same value. Having the same pixel values can lead to having the same hashing values, so the pixels cannot be distuinguised from each other and are not suitable for use as hash keys However, the locations of all of the pixels in an image are distinctive, so the proposed scheme uses the locations of pixels as keys of hash functions. The procedure of constructing the HIT table and the address table of RGB image I is described as Algorithm 1.

Algorithm 1: Construct HIT and HAT of RGB image I

Input: RGB image I, which has the size of $M \times N$, and a random number seed S

Output: HIT and HAT of image$I$

Step 1. Use S as the seed for a random number generator to get seven random numbers $S_1, S_2, \cdots, S_7$; then use $S_1, S_2, \cdots, S_7$ as the random number generators to construct seven hash functions $h_1, h_2, \cdots, h_7$, each of which has the size of $\frac{M}{2} \times \frac{N}{2}$.

Step 2. Initialize HIT, HAT and a flag table (FT), each of which has the size of $\frac{M}{2} \times \frac{N}{2}$ and zero contents.

Step 3. Set variables $i = 1$, $x = 1$, $y = 1$, $m = 1$ and $n = 1$.

Step 4. If $i <= 7$, goto Step 5; otherwise, set $i = 1$, $m = m + 1$, and goto Step 5.

Step 5. If $m <= \frac{M}{2}$, goto Step 6; otherwise, set $x = 1$, $y = 1$, $m = 1$, and $n = 1$and goto Step 8.

Step 6. If $n <= \frac{N}{2}$ goto Step 7; otherwise $m = m + 1$; goto Step 5.

Step 7. If $FT(m, n) = 0$, set $FT(h_i(m, n)) = 1$, $HIT(m, n) = i$, $HAT(m, n) = h_i(m, n)$ and $n = n+1$, and goto Step 6; otherwise, set $i = i+1$, $m = 1$, and $n = 1$, and goto Step 4.

Step 8. Scan the HIT and FT tables, if $HIT(x, y) = 0$ and $FT(m, n) = 0$, set $HAT(x, y) = (m, n)$ and $FT(m, n) = 1$, until $x = \frac{M}{2}$,$y = \frac{N}{2}$,$m = \frac{M}{2}$, and $n = \frac{N}{2}$.

Algorithm 1 uses a flag table (FT) to indicate whether the address table unit is occupied to speed up the execution time.

3.2. **Using Shamir's Method to Compute Shared Image Features and Construct the Alpha Channel.** The proposed scheme uses Shamir's method to compute shared image features and construct the alpha channel, which are described as Algorithm 2.

Algorithm 2: Compute shared feature message bits and construct alpha channel of RGB image I

Input: The RGB image I, which has the size of $M \times N$

Output: The alpha channel I_{alpha} of image I, which has the size of $M \times N$

Step 1. Segment the image I into 2×2 blocks $B_1, B_2, \cdots, B_{\frac{M}{2} \times \frac{N}{2}}$

Step 2. Set $k = 1$, and goto Step 3.

Step 3. If $k <= \frac{M}{2} \times \frac{N}{2}$ goto Step 4; otherwise, output the alpha channel I_{alpha}.

Step 4. For a block B_k , compute the mean value of the R channel Br_k, G channel Bg_k, and B channel Bb_k, respectively. $r = \text{mean}(Br_k)g = \text{mean}(Bg_k)$,, $b = \text{mean}(Bb_k)$ Then use Equation (3) to compute the shared feature message bits.

$$\begin{cases} F(x_1) = (r + gx_1 + bx_1^2) \bmod p, \\ F(x_2) = (r + gx_2 + bx_2^2) \bmod p, \\ F(x_3) = (r + gx_3 + bx_3^2) \bmod p. \end{cases} \tag{3}$$

p in Equation (3) be a prime number greater than eight which controls the length of feature message bits. If p is too small, many blocks would have the same feature value. If p is too large, the modified image would have a recognizable distortion when compared with the original image.

Step 5. Compute element $b_k(1, 1)$ in the alpha channel $Balpha_k$ of block B_k with Equation (4).

$$b_k(1, 1) = 248 + \text{HIT}\left(\left\lfloor \frac{k-1}{N} \right\rfloor + 1, (k-1) \bmod N + 1\right) \tag{4}$$

In Equation (4), the HIT has already been computed with Algorithm 1.

Step 6. Scan the HAT table computed with Algorithm 1, and find $\text{HAT}(m, n) = \left(\lfloor \frac{k-1}{N} \rfloor + 1, (k-1) \bmod N + 1\right)$. Compute element in alpha channel $Balpha_{(m-1)\times \frac{M}{2}+n}$ of block $B_{(m-1)\times \frac{M}{2}+n}$ with Equation (5).

$$\begin{cases} b_{(m-1)\times \frac{M}{2}+n}(1, 2) = 256 - p + F(x_1), \\ b_{(m-1)\times \frac{M}{2}+n}(2, 1) = 256 - p + F(x_2), \\ b_{(m-1)\times \frac{M}{2}+n}(2, 2) = 256 - p + F(x_3). \end{cases} \tag{5}$$

Step 7. Set $k = k + 1$, and goto Step 3.

With the original RGB image I and the alpha channel I_{alpha}, the PNG image I' is acquired and can be used for image authentication.

3.3. **Procedure for PNG image authentication.** The receiver reveived the PNG image I', which was generated with Algorithm 1 and the random number S, then he or she can verify whether tampers have occurred in the image content

The PNG image authentication procedure can be described as Fig. 5 shows.

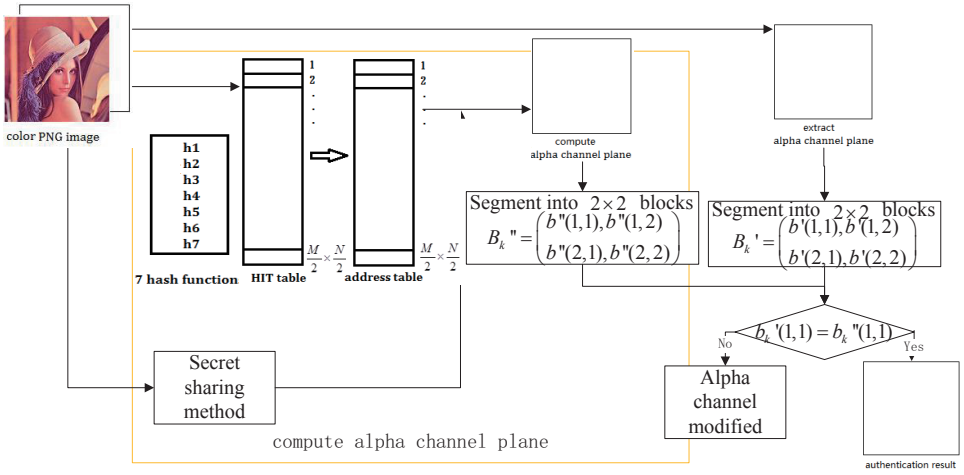

FIGURE 5. Illustration of using rehashing and a secret sharing scheme to authenticate a color PNG image

Algorithm 3: Verify the reality of PNG image I', which was generated by Algorithm 2

Input: The potential tampered PNG image I' which had the size of $M \times N$, and the random number S, which was used in Algorithm 1

Output: Verify the results and locate the tamper position

Step 1. Separate the received PNG image I' from the RGB plane I'_{RGB} and the alpha plane I'_{alpha} Then, segment I'_{alpha} into 2×2 blocks $B'_k = \begin{pmatrix} b'(1,1), b'(1,2) \\ b'(2,1), b'(2,2) \end{pmatrix}, k = 1, 2, \cdots, \frac{M}{2} \times \frac{N}{2}$.

Step 2. Use Algorithm 4 to construct the HIT table and address table of I'_{RGB}.

Step 3. Use Algorithm 5 to construct another alpha channel of I'_{RGB}, named I''_{alpha} Then segment I''_{alpha} into 2×2 blocks $B''_k = \begin{pmatrix} b''(1,1), b''(1,2) \\ b''(2,1), b''(2,2) \end{pmatrix}, k = 1, 2, \cdots, \frac{M}{2} \times \frac{N}{2}$.

Step 4. Initialize a tamper location map (TLM), which has the size of $M \times N$ and element values are ones. Initialize an alpha channel modify map (ACMM), which has the size of $\frac{M}{2} \times \frac{N}{2}$ and element values are ones.

Step 5. Set $k = 1$, and goto Step 6.

Step 6. If $k <= \frac{M}{2} \times \frac{N}{2}$, goto Step 7; otherwise, goto Step 9.

Step 7. If $b'_k(1,1) = b''_k(1,1)$ goto Step 8; otherwise, set $k = k+1$, $ACMM(k) = 0$, and goto Step 6.

Step 8. If $b'_k(1,2) = b''_k(1,2)$, $b'_k(2,1) = b''_k(2,1)$, and $b'_k(2,2) = b''_k(2,2)$, $\mathrm{TLM}(2k, 2k+1, 2k+2, 2k+3) = 1$; otherwise set $\mathrm{TLM}(2k, 2k+1, 2k+2, 2k+3) = 0$. Set $k = k+1$ and goto Step 6.

Step 9. If the proportion of the numbers of zero in ACMM is more than a threshold τ the alpha channel has been altered. Otherwise, if the proportion of the numbers of zero in TLM is more than another threshold γ, the image has been tampered, output TLM.

4. **Experimental Results.** The purpose of our scheme is to locate tamper regions more accurately To accomplish this purpose, the proposed scheme uses the rehashing method and the secret sharing method to authenticate the integrity of a PNG image's content.

For a PNG image, the element value of the alpha channel is from 0 to 255 to control the transparency of the corresponding pixels. Fig. 6 shows the alpha channel of the PNG image Lena modified with different values.

FIGURE 6. PNG image Lena with alpha channel values of (a) 255, (b) 254, (c) 252, (d) 248, (e) 240, (f) 224, (g) 192, and (h) 128.

The first five images in Fig. 6 are very similar. When the value of the alpha channel in PNG image Lena is less than 224 as Figs 6(f) to 6(h) show, the distinction can be perceived by the naked eye. Taking into account the feature value and visual impact, in the proposed method, we chose to use $p = 11$ in Algorithm 2.

To prove the performance of the proposed scheme, four 256×256 color RGB images as shown in Fig. 7, were used as original images for a later comparison of tamper location Because we don't modify the RGB channals data, the PSNRs [20] of RGB channals in Fig. 7 are ∞.

Fig. 8 shows the tamper images and the authentication results. Because of the proposed method's basic process units are 2×2 pixels, the tampered zeros have expanded a little, and there appears to be a trapezoid shape at the edge of the tampered zero.

TABLE 1. Statistics of experimental results

Image size 256×256	No. of tampered blocks	No. of detected blocks (detection ratio)	False acceptance ratio (%)	False rejection ratio (%)
Fig. 8(a)	128	128 (100%)	0	0
Fig. 8(b)	688	672 (97.67%)	2.33	0
Fig. 8(c)	2372	2336 (98.48%)	1.52	0
Fig. 8(d)	268	260 (97.01%)	2.99	0
Fig. 8(e)	800	793(99.09%)	0.91	0
Fig. 8(f)	152	151(99.34%)	0.66	0
Fig. 8(g)	898	887(98.78%)	1.22	0
Fig. 8(h)	0	0	0	0

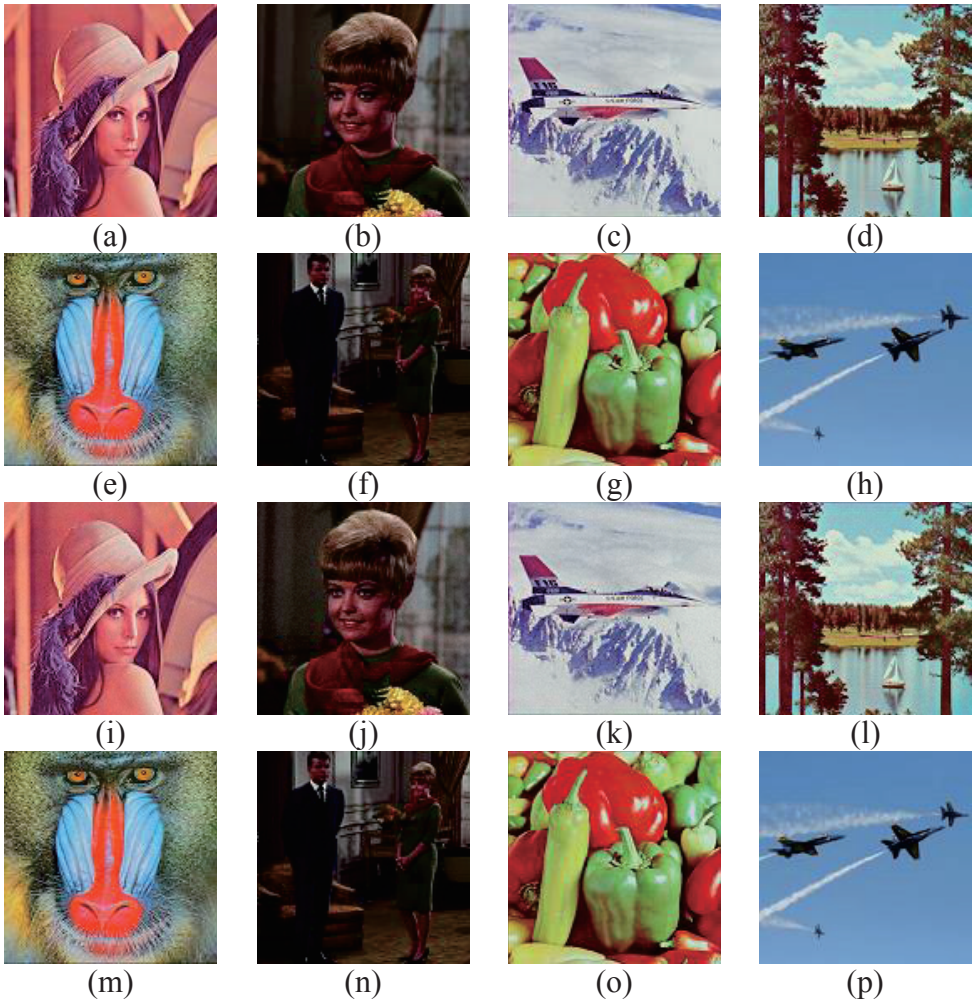

FIGURE 7. Original test color RGB images (a) Lena, (b) Girl, (c) Jet, (d) Boat, (e) Baboon, (f) Couple, (g) Peppers and (h) fighters and their PNG images with embedded authentication messages in the alpha channel.

Table 1 shows that, when the detection ratio is closer to 100%, the false acceptance ratio and false rejection ratio are very small, and the algorithm's ability to detect tamper is more accurate.

TABLE 2. Comparision of existing color image authentication method

	Average false acceptance ratio (%)	Average false rejection ratio (%)
Method of [11]	11.15	0
Method of [21]	50	0
Method of [13]	12.5	0
Proposed scheme	1.2	0

Table 2 shows that Lee and Tsai's method [13] ordinarily adds a random number, which led to collisions that occurred frequently after processing, and the average false acceptance ratio was 12.5%. Tang et al's method [11] only uses local color features to generate image hash for image content authentication, and the average false acceptance ratio was 12.5%. Using the rehashing method, our proposed scheme had the lowest false acceptance ratio of 1.20%, which is a significant advantage.

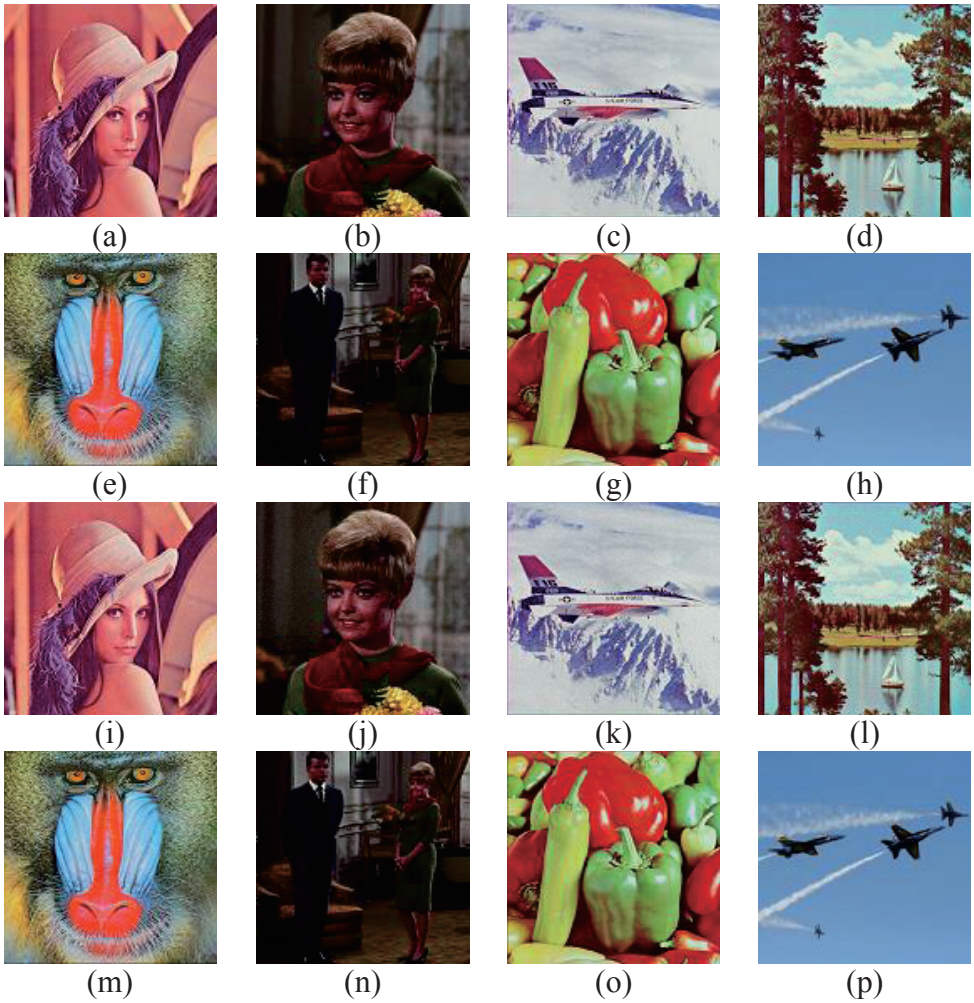

FIGURE 8. Tampered images: (a) Lena with 'abc' painting, (b) Girl with tampered flowers, (c) Jet with copy clouds, (d) Boat with copy boat, (i) Baboon with black eyes, (j) Couple with tampered flowers, (k) Pepper with a black hole and (l) Original Fighters. Tamper location maps (TLMs): (e) Lena TLM, (f) Girl TLM, (g) Jet TLM, (h) Boat TLM, (m) Baboon TLM, (n) Couple TLM, (o) Pepper TLM and (p) Fighters TLM.

5. **Conclusions.** An authentication scheme that uses rehashing and secret sharing methods to verify the integrity of a color image's content is proposed in this paper The proposed scheme uses Shamir's secret sharing method to share image features, utilizes the rehashing method to overcome easy collisions of the random numbers, and employs PNG images to hide authentication messages, thereby innovatively enhancing its effectiveness against attacks. PNG is the most commonly used lossless image compression format on the Internet The proposed method embeds image feature values in the alpha channel to protect the original RGB image effectively. Also, the experimental results verified that the proposed method can be used for image authentication applications In fact, our authentication scheme based on the rehashing and secret sharing method is designed for color PNG images. If the Alpha channel data of the authentication image is separated from the RGB channel data, we would not obtain the correct authentication results.

REFERENCES

[1] R. Venkatesan, S. M. Koon, M. H. Jakubowski, and P. Moulin, Robust image hashing, *Proc. of IEEE International Conference on Image Processing*, Vol. 3, pp. 664-666, 2000.

[2] J. Fridrich, and M. Goljan, Robust hash functions for digital watermarking, *Proc. of IEEE International Conference on Information Technology: Coding and Computing*, pp. 178-183, 2000.

[3] M. Tagliasacchi, G. Valenzise, and S. Tubaro, Hash-based identification of sparse image tampering, *IEEE Trans. on Image Processing*, vol. 18, no.11, pp. 2491-2504, 2009.

[4] F. Ahmed, M. Y. Siyal, and V. Uddin Abbas, A secure and robust hash-based scheme for image authentication, *Signal Processing*, vol. 90, no. 5, pp. 1456-1470, 2010.

[5] Y. Lei, Y. Wang, and J. Huang, Robust image hash in radon transform domain for authentication, *Signal Processing:Image Communication*, vol. 26, no. 6, pp. 280-288, 2011.

[6] Y. Zhao, S. Wang, X. Zhang, and H. Yao, Robust hashing for image authentication using Zernike moments and local features, *IEEE Trans. on Information Forensics and Security*, vol. 8, no. 1, pp. 55-63, 2013.

[7] R. O. Preda, Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain, *Measurement*, vol. 46, no. 1, pp. 367-373, 2013.

[8] M. Wu and B. Liu, Watermarking for image authentication, *Proc. of IEEE International Conference on Image Processing, ICIP 98*, vol. 2, pp. 437-441, 1998.

[9] D. Kundur and D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, *Proc. of the IEEE*, vol. 87, no.7, pp. 1167-1180, 1999.

[10] L. Yang, R. Ni, and Y. Zhao, Segmentation-based image authentication and recovery scheme using reference sharing mechanism, *International Conference on Industrial Control and Electronics Engineering,ICICEE 2012*, pp. 863-866, 2012.

[11] Z. Tang, X. Zhang, X. Dai, J. Yang, and T. Wu, Robust image hash function using local color features, *AEU-International Journal of Electronics and Communications*, vol. 67, no. 8, pp. 717-722, 2013.

[12] X. Tong, Y. Liu, M. Zhang, and Y. Chen, A novel chaos-based fragile watermarking for image tampering detection and self-recovery, *Signal Processing*: *Image Communication*, vol. 28, no. 3, pp. 301-308, 2012.

[13] C. W. Lee, and W. H. Tsai, A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, *Signal Processing*, vol. 93, no 7, pp. 2010-2025, 2013.

[14] W. Y. Zhang, and Y. S. Frank, Semi-fragile spatial watermarking based on local binary pattern operators, *Optics Communications*, vol. 284, no. 16, pp. 3904-3912, 2011.

[15] Z. Wei, and K. N. Ngan, Spatio-temporal just noticeable distortion profile for grey scale image/video in DCT domain, *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 19, no. 3, pp. 337-346, 2009.

[16] M. W. Du, T. M. Hsieh, K. F. Jea, and D. W. Shieh, The study of a new perfect hash scheme, *IEEE Trans. on Software Engineering*, vol. SE-9, no. 3, pp. 305-313, 1983.

[17] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22, no.11, pp. 612-613, 1979.

[18] C. Guo and C. C. Chang, A construction for secret sharing scheme with general access structure, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 1-8, 2013.

[19] R. Sprugnoli, Perfect hashing functions: a single probe retrieving method for static sets, *Communications of the ACM*, vol. 20, no. 11, pp. 841-850, 1977.

[20] P. Li, Q. Kong, and Y. P. Ma, Image secret sharing and hiding with authentication based on PSNR estimation, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 3, pp. 353-366, 2014.

[21] S. C. Byun, I. L. Lee, T. H. Shin, and M. H. Ahn, A public-key based watermarking for color image authentication, *Proc. of IEEE International Conference on Multimedia and Expo*, vol. 1, pp. 593-596, 2002.