Adaptive Secret Sharing for Color Images

Jia-Hong Li[1], Wei-Bin Lee[1], Dengpan Ye[2], Tzong-Jye Liu[1] and Chuan Qin[1, 3]

[1]*Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan*
[2]*Computer School of Wuhan University, Wuhan 430072, China*
[3]*School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China*
E-mail: P9317874@fcu.edu.tw, wblee@fcu.edu.tw, yedp2001@163.com, tjliu@fcu.edu.tw, qin@usst.edu.cn

Abstract

A secret sharing model can secure a secret over multiple noise-like shadows and remain recoverable despite multiple shadow failures. Even if some of the shadows are compromised, the secret will not be revealed as long as the number of the compromised shadows is smaller than a pre-determined threshold. Moreover, there are some necessary details of concerns: the malicious tampering on shadows must be detectable; the shadows must be concealed in a camouflage image with adequate quality to reduce suspicion and possible attack; color image properties must be considered. In addition to these concerns, in this paper, an adaptable mechanism is further designed to balance the hiding quantity and the quality of camouflage image depending on different applications. This is an important and interesting aspect that has never been discussed in previous research.

Keywords: Authentication; bayer pattern; color filter array; secret sharing; steganography

1. Introduction

Generally, a secret key is used to control the access to protected files. When such a key is lost or unavailable, the problems will arise. A basic solution to avoid the situation that one's important files may depend on a single key is to divide the secret key into several pieces. These pieces are then distributed to different people such that a certain subset of these people can pool together to recover the original key. This kind of the key management motivated the discovery of the secret sharing schemes by Shamir [9].

Afterward, several researches [1-2, 5-8, 10-11] based on the above (r, n) threshold scheme were proposed to split a secret image into n noise-like shadow images. The secret image can be reconstructed if and only if any r or more shadow images are available. On the contrary, the secret cannot be revealed if less than the threshold number of shadows are lost incidentally or modified intentionally. However, these schemes tend to attract the attention of attackers due to the nature of the meaningless shadow. Recently, in order to make these images less conspicuous, researches [3-4, 15-16] focused on embedding the shadows within a meaningful medium, such as an image or a video, to conceal the existence of the shadows. This transparency property undeniably lowers the attention of the attackers and as a result increases the security of the scheme.

However, as color images are generally preferred over grayscale one, we will focus on the model based on (r, n) threshold scheme for color image. In 2003, Chang and Lin [4] proposed a scheme only for indexed color images, such as GIF (graphics interchange format). In 2008, Chang *et al.* [2] proposed another (r, n) threshold based image secret sharing scheme for color images but it lacks the transparency property. No matter what ideas are discussed, the research results could treat as a method which is directly applied to the grayscale domain. Accordingly, the proportion of the hiding capacity is exactly the same, and the size of the secret image can be significantly increased if the property of color image could be skillfully considered.

Moreover, in order to avoid the malicious participants modifying the stego-images and causing the

Published by Atlantis Press

failure of the reconstructed secret image, the authentication procedure should be involved in the secret image sharing scheme to protect the integrity of the stego-images. In 2007, Yang *et al*. [16] introduced the authentication mechanism based on a one way hash function to detect and locate the tampered area. Later, Chang *et al*. [3] proposed a similar scheme but used a different method, the Chinese Remainder Theorem (CRT), to implement the authentication component.

Both [16] and [3] are based on (r, n) threshold scheme for color images with the transparency property. However, the predetermined threshold r is used as a secure parameter directly applied from the grayscale image into the color image so that the proportion of hiding capacity is exactly the same, then the image quality cannot be significantly increased. Of course, not only the quality of the camouflage image but also the extracted secret image must be good enough to be identifiable, recognizable and unambiguous.

Almost all of previous researches only focused on how to obtain the maximum hiding capacity and the desirable image quality simultaneously. However, in real applications, there is a trade-off between them. For instance, hiding enormous secrets into an image will cause noticeable artifact. On the other hand, in order to improve the imperceptibility, the capacity of the hiding secret must be reduced. Therefore, according to different applications, the adaptable capability is the most important issue because people can choose the appropriate trade-off between the hiding capacity and the image quality as they wish.

More than that, in the (r, n) threshold scheme, there is an interesting issue in each polynomial, namely, how to absolutely utilize the whole space in a polynomial so as to mine the maximum accommodated size. In other words, the threshold r, i.e., the degree of the polynomial, will affect the space used to accommodate the secret image and the distortion on the camouflage image. Therefore, the maximum size of secret image that can be embedded is tunable with the threshold r and, of course, the side-effect is the quality of the camouflage image.

In this paper, we proposed an adaptable mechanism that makes possible the balance of the hiding capacity and the image quality through adjusting the threshold r, the degree of the polynomial, rather than enlarging the size of the camouflage images directly. This is a very interesting aspect which has never been discussed in previous research, and can be widely applied in the military image transmission [12] or other secure image applications [13].

In the rest of this paper, the concept of color filter array (CFA) and the (r, n) threshold scheme are reviewed in Section 2. Section 3 depicts the proposed color secret image sharing scheme utilizing the concept of CFA and the (r, n) threshold scheme. The experiments and discussions are presented to show the feasibility and the superiority of the proposed scheme in Section 4. Finally, some conclusions are stated in the last section.

2. Preliminaries

This section will briefly review two related techniques: (1) color filter array and (2) the (r, n) threshold scheme. These two techniques will be used by the proposed scheme.

2.1. *Fundamental of Bayer CFA*

The most important perspective which differs our work from previous research is taking the property of the color image into account. The CFA image is composed of a mosaic-like grayscale image, whose effect comes from a Bayer filter mosaic, shown in Fig. 1.

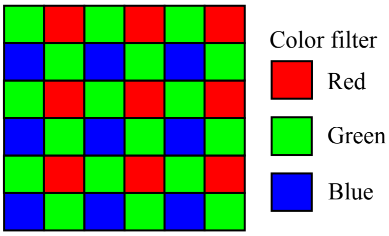


Fig. 1. Sample of Bayer Color Filter Array.

In this way, each pixel is filtered to record one of three colors; two-thirds of the color data is dropped. Fig. 2(b) shows the result filtered by CFA from Fig. 2(a).

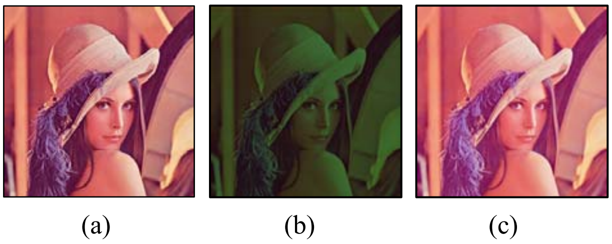

(a) (b) (c)

Fig. 2. Bayer CFA image: (a) from raw sensor, (b) arranged as a color domain, (c) recovered by interpolation from (b).

To obtain a full-color image, various demosaicking methods such as [14] can be used to interpolate a set of complete red, green, and blue values for each point. Different methods require different computing power which results in varying-quality final images. Fig. 2(c) shows one of the possible results recovered from Fig. 2(b) by the color demosaicking scheme in [14].

With the help of CFA, the size of an image can be reduced to one-third of the original so that the consumption of bandwidth is saved during the transmission via Internet. Furthermore, the quality of the recovered image still stands good.

2.2. *Review of the (r, n) threshold scheme*

The concept of (r, n) threshold secret sharing method proposed by Shamir [9] is used to distribute a secret among a group of participants. Accordingly, any r or more participants can pool together to recover the secret. To setup a (r, n) threshold scheme, first, a r-1 degree polynomial must be chosen. The shadow held by each participant is analogous to a point over the polynomial. Therefore, any r or more participants can reconstruct the polynomial to obtain the secret.

3. Proposed Color Secret Image Sharing Scheme

In this section, the proposed color secret image sharing scheme is explained in two phases: the first phase for hiding the color secret image, and the other for extracting and reveailing the color secret image. The details are described respectively as below.

3.1. *Phase for color secret image sharing*

This phase contains three procedures: color filtering, the r-pixel polynomials generation, and embedding and sharing procedures. Assume that secret image $S = \{(r_{i,j}, g_{i,j}, b_{i,j}) \mid 1 \le i \le m, 1 \le j \le n$, and $r_{i,j}, g_{i,j}, b_{i,j} \in [0,255]\}$ is a 24-bit RGB-color image with size of $m \times n$.

Procedure 1. Color filtering

Generate a grayscale CFA image $A = \{a_{i,j} \mid 1 \le i \le m, 1 \le j \le n$, and $a_{i,j} \in [0,255]\}$, where

$$a_{i,j} = \begin{cases} r_{i,j} & \text{if } i \text{ is odd and } j \text{ is even,} \\ b_{i,j} & \text{if } i \text{ is even and } j \text{ is odd,} \\ g_{i,j} & \text{otherwise.} \end{cases}$$

Procedure 2. Adaptable r choice and polynomials generation

In this procedure, the element $a_{i,j}$'s in A are processed by row scanning and are grouped into ($m \times n/r$) sections. That is, each section t has r pixels, $Z_{t,0}$, $Z_{t,1}, \ldots, Z_{t,r\text{-}1}$, where $1 \le t \le m \times n \,/\, r$. For section t, the constructed polynomial is $q_t(x) = (z_{t,0} + z_{t,1}x + z_{t,2}x^2 + \ldots + z_{t,r\text{-}1}x^{r\text{-}1}) \bmod p$.

After all sections are processed, a set of polynomials $Q = \{q_t(x) \mid 1 \le t \le m \times n \,/\, r\}$ will be obtained. Furthermore, since the gray value of a pixel is belongs to [0, 255], p could be the Galois Field GF(2^8). The interested readers may refer to [16] for the details.

Procedure 3. Embedding and sharing procedure

In this procedure, each polynomial must contribute a point for each camouflage image, so that n camouflage images will possess n points for each polynomial. In other words, any r or more camouflage images can reconstruct the polynomial together.

Assume each camouflage image C is a 24-bit RGB-color image of size $M \times N$ pixels. For simplicity, the red channel C^R is taken. The 8-bit pixels in the red channel are divided into a L-pixel based image $C^R = \{C_{t,l}^R \mid 1 \le t \le M \times N \,/\, L, 1 \le l \le L$, and $C_{t,l}^R \in [0,255]\}$, shown in Fig. 3, where $1 \le t \le (m \times n \,/\, r) \le (M \times N \,/\, L)$ is confirmed to guarantee the enough hiding capacity.

The following shows how each grouped block $C_{t,l}^R$ in C^R with identity ID is used to hide a point of the polynomial $q_t(x)$.

Step 1. Compute $q_t(x_t) \bmod p = \{q_{t1}, q_{t2}, \ldots, q_{t8}\}$, where x_t is the first six most significant bits (MSBs) of $C_{t,1}^R$ and $\{q_{t1}, q_{t2}, \ldots, q_{t8}\}$ is the 8-bit binary representation of the result.

Step 2. Hide $\{q_{t1}, q_{t2}\}$, $\{q_{t3}, q_{t4}\}$, $\{q_{t5}, q_{t6}\}$, and $\{q_{t7}, q_{t8}\}$ into the last (8/L) LSBs in $C_{t,l}^R$ to generate $\hat{C}_{t,l}^R$, respectively. The result is shown in Fig. 4.

Step 3. Calculate the authenticator:

$$f_t = f\left(\left(\hat{C}_{t,l}^R \setminus p_t\right) \| \, t \, \| \, ID \, \| \, K\right),$$

where $f(\cdot)$ denotes a one-way hash function, $\setminus p_t$ denotes minus (without) p_t, $\|$ denotes concatenation, and K is the secret key shared by the related participants.

Step 4. Obtain the authentication bit p_t by folding f_t. For instance, the authenticator $f_t = (1101)_2$ is worked out to be 1_2 since $1 \oplus 1 \oplus 0 \oplus 1 = 1$.

Step 5. Hide p_t into the $\lceil 8/L \rceil$-th LSBs in the predetermined $C_{t,l}^R$.

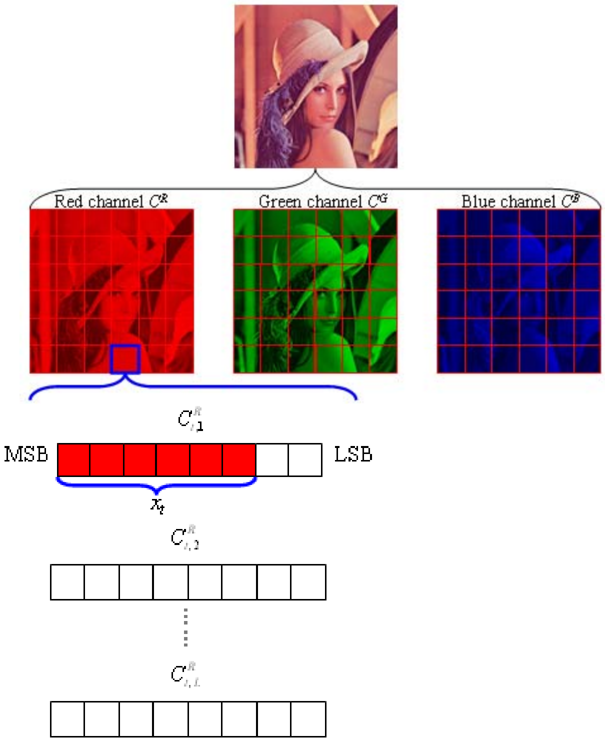


Fig. 3. Block of camouflage image.

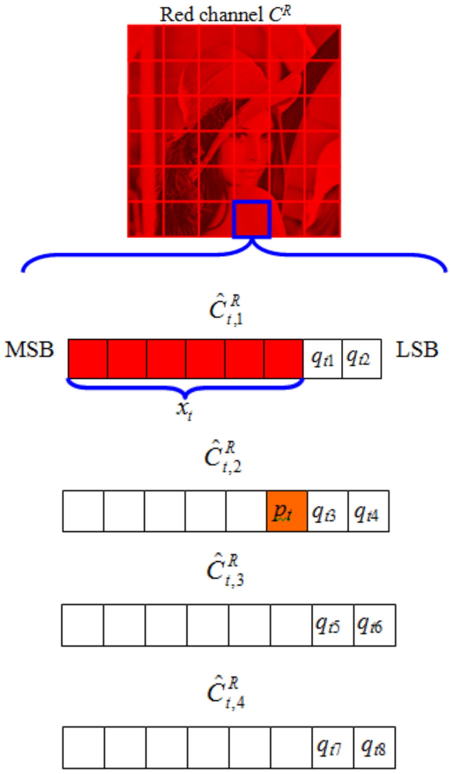


Fig. 4. Block of stego-image which assume L = 4.

The above steps help to embed a point in the polynomial into a block of C^R. The green channel C^G and blue channel C^B are processed in the same way. Therefore, a polynomial is completely hidden if the steps are repeated for each color channel of the camouflage image. After all polynomials in Q are hidden, the whole embedding and sharing process is completed.

The entire proposed color secret image sharing procedure can be illustrated in Fig. 5. The color filtering transforms the secret image into a CFA image. The r-pixel polynomials generation produces the r-1 degree polynomial using the pixels of the secret image. Finally, the embedding and sharing procedure performs the specified LSB substitution and secret sharing to achieve the objective of steganography.

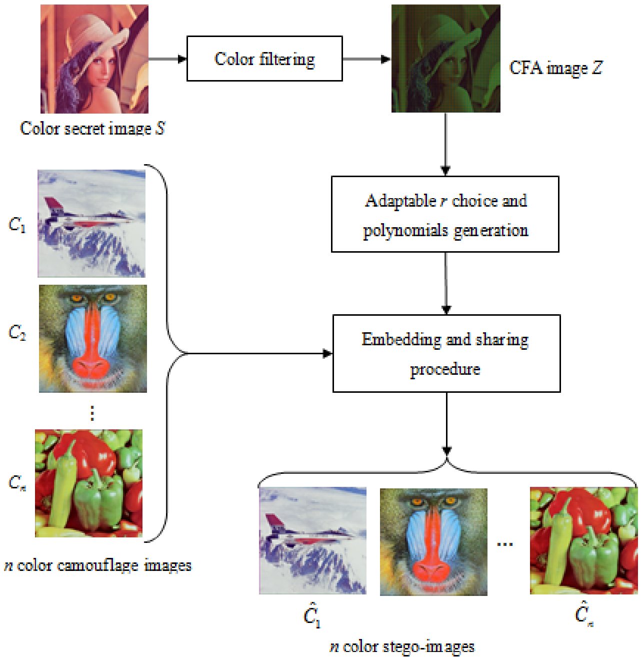


Fig. 5. Block diagram of the proposed CFA color secret image sharing procedure.

3.2. *Phase for color secret image revealing*

In this section three procedures — the authentication check, the r-pixel polynomials reconstruction, and the color demosaicking procedures — are involved in the color secret image revealing phase.

Procedure 1. Authentication check

The authentication check procedure verifies the red channel C^R of the stego-image $\hat{C}$ as follows.

Step 1. Divide the red channel $\hat{C}^R$ into t L-pixel blocks, where $\hat{C}^R = \{\hat{C}^R_{t,l} \mid 1 \le t \le M \times N / L, 1 \le l \le L, \text{and } \hat{C}^R_{t,l} \in [0,255]\}$.

Step 2. Calculate the authenticator: $f_t = f\left(\left(\hat{C}^R_{t,l} \setminus p_t\right) \| t \| ID \| K\right)$.

Step 3. Obtain authentication bit $\hat{p}_t$ by folding f_t.

Step 4. Verify whether $\hat{p}_t = p_t$. The block is genuine if the equality holds; otherwise, the block is tampered.

The green channel C^G and the blue channel C^B are processed in the same way. If all authentication bits derived from the blocks in each color channel are verified, the stego-image is considered as the genuine.

Procedure 2. r-pixel polynomials reconstruction

Once the image passes the authentication check, Procedure 2 is performed as follows. In this procedure, at least r camouflage images must be collected and then the r-1 degree polynomial $q_t(x)$ is reconstructed. For simplicity, the following steps show how a point of $q_t(x)$ is recovered.

Step 1. Extract the data bits $\{q_{t1}, q_{t2}\}$, $\{q_{t3}, q_{t4}\}$, $\{q_{t5}, q_{t6}\}$, and $\{q_{t7}, q_{t8}\}$ directly from the last (8/L) LSBs in $\hat{C}^R_{t,l}$, respectively, to obtain $y_t=\{q_{t1}, q_{t2,\ldots,} q_{t8}\}$.

Step 2. Extract the first six MSBs of $C^R_{t,1}$, denoted as x_t.

At this time, a point (x_t, y_t) is recovered. When r points are reconstructed from the corresponding r stego-images, the polynomial $q_t(x) = (z_{t,0} + z_{t,1}x + z_{t,2}x^2 + \ldots + z_{t,r\text{-}1}x^{r\text{-}1}) \bmod p$ can be rebuilt based on the Lagrange's interpolation. Together with all of the polynomials reconstructed in Q, $A'=\{a_{i,j}' \mid 1\le i \le m, 1\le j \le n, \text{and } a_{i,j}'\in[0,255]\}$ is recovered, and a grayscale CFA image is obtained finally.

Procedure 3. Color demosaicking

In this procedure, the color secret image $S' = \{(r_{i,j}', g_{i,j}', b_{i,j}') \mid 1 \le i \le m, 1 \le j \le n, \text{and } r_{i,j}', g_{i,j}', b_{i,j}' \in[0,255]\}$ can be reconstructed from $A'=\{a_{i,j}' \mid 1\le i \le m, 1\le j \le n, \text{and } a_{i,j}'\in[0, 255]\}$ through color demosaicking that interpolates a complete image from the partial raw data from a CFA. The details for this procedure can be found in related color demosaicking schemes, such as [14].

The entire proposed color secret image revealing procedure can be illustrated in Fig. 6. The authentication check procedure verifies the collected r color stego-images. Once these r images pass the authentication check, the r-pixel polynomials reconstruction recovered a reconstructed CFA image. Finally, the color demosaicking procedure interpolates a color secret image from the reconstructed CFA image.

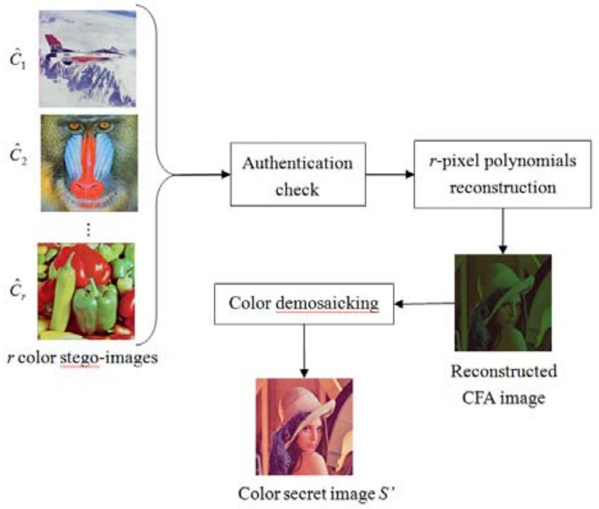


Fig. 6. Block diagram of the proposed CFA color secret image revealing procedure.

4. Discussions

In order to show the feasibility of the proposed scheme, some numerical evaluations, experiments, comparisons, and security analyses are carried out.

The peak-signal-to-noise ratio (PSNR) is employed to measure the image quality, which is defined as:

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{I^2_{\max}}{\text{MSE}}\right) \text{dB}, \tag{1}$$

where $I_{\max}$ is 255 for an 8-bit grayscale images, and the MSE for the color image is defined as

$$\text{MSE} = \frac{1}{3 \times M \times N} \sum_{x,y \in \{r,g,b\}} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2, \tag{2}$$

where x_{ij} denotes a color value of the original image, y_{ij} denotes a color value of the compared stego-image, $M \times N$ is the image size, and r, g, and b represent the 24-bit colors red, green, and blue, respectively.

4.1. *Feasibility of the proposed scheme*

The feasibility and performance are investigated which include the impact of the proposed adaptable scheme, the qualities of stego-images, the maximum hiding capacity, and the quality of revealed secret image.

4.1.1. *The impact of adaptability*

An adaptable mechanism balancing the demand between quality and capacity is designed. The following gives some lemmas to show the relationship between the threshold *r* and the embedding capacity.

Lemma 1. *Given a grayscale camouflage image C of size M × N, the number of polynomials that can be embedded is M × N / L.*

Proof. In the proposed scheme, every *L*-pixel block in *C* is utilized to hide a point of a polynomial. Therefore, the grayscale camouflage image with size *M* × *N* can provide *M* × *N* / *L* blocks, and *M* × *N* / *L* points can be hidden. Because each point is contributed by a polynomial, it implies that each camouflage image is able to accommodate *M* × *N* / *L* polynomials. □

Lemma 2. *With the* (*r*, *n*) *threshold strategy, given a grayscale camouflage image C of size M × N, the total number of pixels that can be embedded is M × N× r / L.*

Proof. With the (*r*, *n*) threshold strategy, because the *r* coefficients of each polynomial are taken from the CFA image *Z*, each polynomial implies *r* secret pixels. Based on the result of Lemma 1, a total of *M* × *N* × *r* / *L* pixels can be embedded. □

The above lemmas are proven in the grayscale domain. This can be extended to the color image scenario which is given as follows.

Lemma 3. *For color images in the proposed scheme, the total number of pixels that can be embedded is M × N × r × 3 / L.*

Proof. With the help of CFA technique, the color secret image *S* is shrunk into a CFA image *Z* first. Hence, only one of the three channels — red, green, or blue, will be preserved, while still allowing all information to be restructured. That is, the total embedded pixels are three times of that in Lemma 2. Therefore, there are *M* × *N* × *r* × 3 / *L* pixels that can be embedded. □

From Lemma 3, we can deduce that the maximum accommodated capacity of the camouflage image is *M* × *N* × *r* × 3 / *L*. Of course, the threshold *r* must be less than or equal to the number of camouflage images *n*.

On the other hand, with the demand of higher image quality, it is not necessary to utilize all hidden space of the camouflage image. Such as Fig. 7, the simulation adopts the secret image of size 256×256 pixels and the camouflage image of size 512×512 pixels using the proposed scheme with different thresholds. Contrary to Yang *et al.*'s steady PSNR [16], the results show that a better PSNR value is obtained when a larger threshold *r* is adopted. In other words, the user can choose a larger threshold *r* if the image quality is crucially considered.

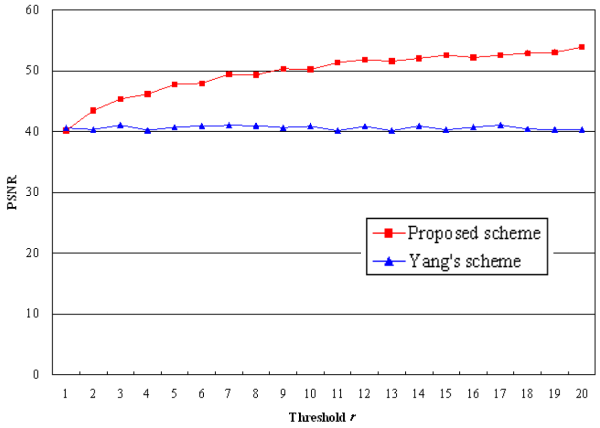


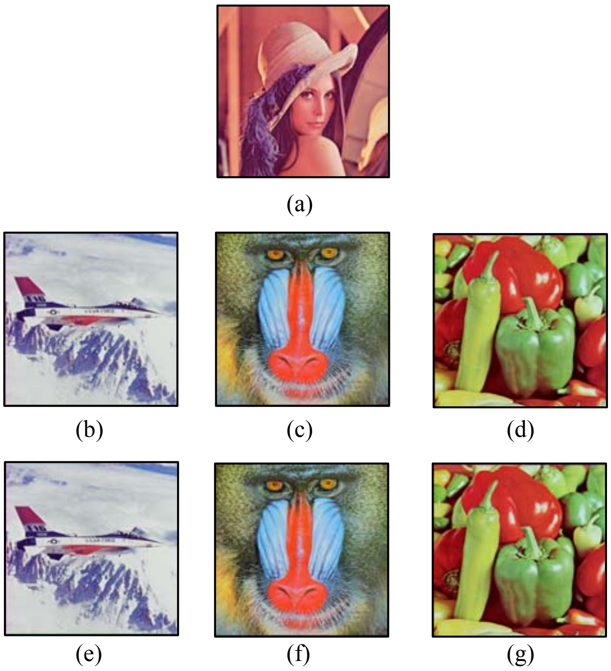
Fig. 7. Stego image quality with different thresholds.

In summary, the accommodated hiding capacity can be increased without greatly sacrificing image quality. Similarly, if the hiding capacity is steady, the image quality will be promoted. Therefore, this adaptive hiding strategy facilitates the proposed scheme applicability.

4.1.2. *The qualities of the stego-images*

To demonstrate the transparency property of the proposed scheme, the qualities of the stego-images are examined in this section. For the ease of understanding, an (2, 3)-threshold case is utilized. The test images shown in Fig. 8(a), (b), (c), and (d) are selected from the USC-SIPI image database. Here, Fig. 8(a) is the secret image, Lena, with the size of 256×256, and other images — Jet, Baboon, and Pepper — are used as camouflage images, with the size of 512×512.

As shown in Fig. 8, the PSNR value of the stego-images Fig. 8(e), Fig. 8(f), and Fig. 8(g) are 44.58 dB, 44.61 dB, and 44.54 dB, respectively.


(a)

(b) (c) (d)

(e) (f) (g)

Fig. 8. (2, 3)-threshold color secret image sharing. (a) The secret image S (256×256), (b) Camouflage image Jet, (c) Camouflage image Baboon, (d) Camouflage image Pepper, (e) stego-image PSNR= 44.58 dB, (f) stego-image PSNR=44.61 dB, (g) stego-image PSNR=44.54 dB.

The proposed scheme greatly outperforms Yang *et al.*'s scheme [16] in terms of the quality of the stego-image as compared under the same size of the camouflage image and that of the secret image. Table 1 shows the results where all of the PSNR values are higher than 44 dB on our proposed scheme and are lower than 41 dB on Yang *et al.*'s.

Table 1. PSNRs of stego-image for [16] and proposed scheme.

Scheme	Jet	Baboon	Pepper
[16]	40.15	40.06	40.66
Proposed	44.58	44.61	44.54

4.1.3. *The maximum embedding secret size*

In this section, we compare the embedding capacity of Yang *et al.*'s scheme [16] with our scheme, using a (2, 3)-threshold scheme as an example with three camouflage images of size 512×512 pixels. Table 2 shows that the proposed scheme provides higher hiding capacity at the similar level image quality compared with Yang *et al.*'s scheme. In fact, our proposed scheme also gains better image quality.

Table 2. Comparison about PSNRs of stego-image and the size of secret image.

Scheme	Secret image	Jet	Baboon	Pepper
[16]	256x256	40.15	40.06	40.66
Proposed	626x626	41.60	41.62	41.52

4.1.4. *The quality of the revealed secret image*

In the following, the experiment is done according to the color secret image revealing procedure and is shown in Fig. 9. It is obvious to show that the quality of the revealed secret image S' of size 256×256 pixels, examined by Wu and Zhang's color demosaicking scheme [14], can be accepted by the human visual system with the PSNR value 35.05 dB.

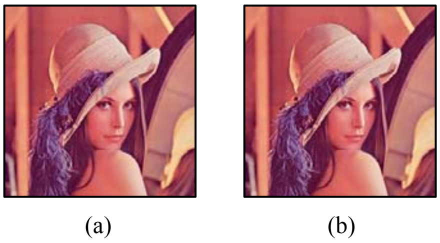

(a) (b)

Fig. 9. Comparison with the secret image and the revealed image of size 256×256 pixels. (a) The secret image S, (b) The revealed image S'

4.2. *Security of the proposed scheme*

This section investigates the authentication property with experiments and discusses that the security characteristics of the (r, n) threshold scheme applied in our scheme.

4.2.1. *Evaluation of the authentication ability*

For each block, an authentication bit pt is generated to verify whether the block has been tampered. Because the bit is computed based on a one-way hash function with the secret key K, an attacker lacking this vital information has no way to control the forged pixels such that the corresponding authentication bit remains valid. The best an attacker can do is to guess the result of the computed authentication bit. The chance of a success as suggested by Yang *et al.*'s analysis [16], for guessing a right bit p_t is (1/2). For a $M \times N$ camouflage image, there are $M \times N / L$ blocks created, therefore, the successful guessing probability will be $(1/2)^{(MN/L)}$. This makes spoofing extremely unlikely. For example, if $M = N = 512$ and $L = 4$, the probability is calculated to be $(1/2)^{65536}$.

In the following, the stego-images embedded with the authentication bit are shown in Fig. 10(a), Fig. 10(d), and Fig. 10(g). Then, some modifications are performed on each of them to simulate a malicious attack as shown in Fig. 10(b), Fig. 10(e), and Fig. 10(h). The results of the tamper localization with the detected blocks marked in white are shown in Fig. 10(c), Fig. 10(f), and Fig. 10(i), respectively. It can be observed that all three tempering attempts have been reliably detected, which demonstrates the aptitude of the authentication capability.

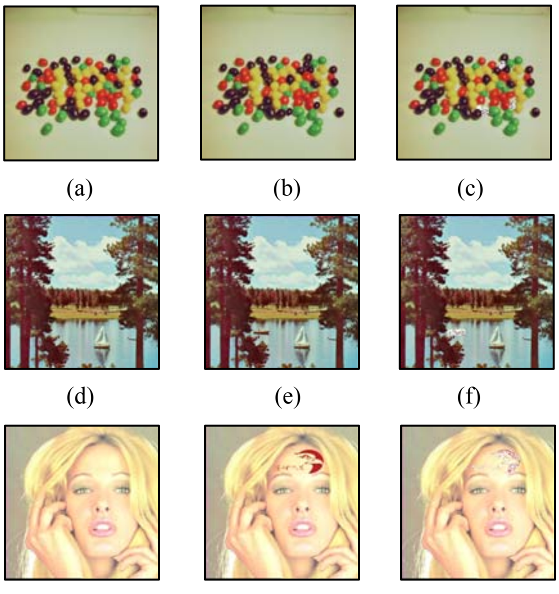


Fig. 10. Results of the tamper localization. (a) stego image Beans, (b) the modified image Beans, (c) detected result Beans, (d) stego-image Sailboat, (e) the modified image Sailboat, (f) detected result Sailboat, (g) stego-image Tiffany, (h) the modified image Tiffany, (i) detected result Tiffany.

4.2.2. *Validation of the (r, n) threshold scheme*

According to (r, n) threshold secret sharing method proposed by Shamir [9], a r-1 degree polynomial can only be reconstructed if at least r valid points over the polynomial are known. Subsequently, the secret remains safe as long as less than r points are exposed, and the only way for revealing the secret image is to collect at least r camouflage images.

5. Conclusions

In this paper, a new secret sharing scheme based on steganography is proposed. The color filter array (CFA) is used to reduce a 24-bit color image to an 8-bit gray image, thereby raising the hiding capacity and the quality of stego-image enormously. In addition, an adaptable mechanism is introduced which makes possible the balance of image quantity through adjusting the threshold r, the degree of the polynomial, rather than enlarging the size of the camouflage images directly. This is a very interesting aspect which has never been discussed in previous research. The adjustable threshold value is able to accommodate the quality of camouflage image to a wide range of applications. Moreover, this novel adaptive color image sharing scheme provides a secure means for delivering color image with the guarantee of authentication, high capacity, and excellent quality.

Acknowledgements

This work was supported by the Natural Science Foundation of China (60903197).

References

1. Alvarez, G., Hernández E. A., Hernández E. L. and Martín R. A., A secure scheme to share secret color images, *Computer Physics Communications*, **173**(1), 2005, pp. 9-16.
2. Chang, C. C., Lin, C. C., Lin, C. H. and Chen, Y. H., A novel secret image sharing scheme in color images using small shadow images, *Information Sciences*, **178**(11), 2008, pp. 2433-2447.
3. Chang, C. C., Hsieh, Y. P. and Lin, C. H., Sharing secrets in stego images with authentication, *Pattern Recognition*, **41**(10), 2008, pp. 3130-3137.
4. Chang, C. C. and Lin, I. C., A new (t, n) threshold image hiding scheme for sharing a secret color image, *Proceedings of IEEE International Conference on Communication Technology*, 2003, pp. 196-202.
5. Chen, C. C. and Suen, G. Y., Sharing an image with cheater identification, *International Journal of Innovative Computing, Information and Control*, **6**(2), 2010, pp. 677-685.
6. Lukac, R. and Plataniotis, K. N., A color image secret sharing scheme satisfying the perfect reconstruction property, *Proceedings of IEEE 6th Workshop on Multimedia Signal Processing*, 2004, pp. 351-354.
7. Lukac, R. and Plataniotis, K. N., A cost-effective encryption scheme for color images, *Real-Time Imaging*, **11**(5), 2005, pp. 454-464.
8. Lukac, R. and Plataniotis, K. N., Bit-level based secret sharing for image encryption, *Pattern Recognition*, **38**(5), 2005, pp. 767-772.
9. Shamir, A., How to share a secret, *Communications of*

ACM, **22**(11), 1979, pp. 612-613.

10. Thien, C. C. and Lin, J. C., Secret image sharing, *Computers and Graphics*, **26**(5), 2002, 765-770.
11. Tsai, M. H., Lin, Y. B. and Wang, C. M., Image sharing with steganography and cheater identification, *International Journal of Innovative Computing, Information and Control*, **6**(3), 2010, pp. 1165-1178.
12. Wang, Z., Li, S., Lv, Y. and Yang, K., Remote sensing image enhancement based on orthogonal wavelet transformation analysis and pseudo-color processing, *International Journal of Computational Intelligence Systems*, **3**(6), 2010, pp. 745-753.
13. Witte, V. D., Schulte, S. and Kerre, E. E., New vector ordering in the redgreenblue colour model with application to morphological image magnification, *International Journal of Computational Intelligence Systems*, **1**(2), 2008, pp. 103-115.
14. Wu, X. and Zhang, N., Primary-consistent soft-decision color demosaicking for digital cameras, *IEEE Transactions on Image Processing*, **13**(9), 2004, pp. 1263-1274.
15. Wu, Y. S., Thien, C. C. and Lin, J. C., Sharing and hiding secret images with size constraint, *Pattern Recognition*, **37**(7), 2004, pp. 1377-1385.
16. Yang, C. N., Chen, T. S., Yu, K. H. and Wang, C. C., Improvements of image sharing with steganography and authentication, *Journal of Systems and Software*, **80**(7), 2007, pp. 1070-1076.