Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/MBE

MBE, 18(5): 5236–5251.
DOI: 10.3934/mbe.2021266
Received: 12 March 2021
Accepted: 04 June 2021
Published: 11 June 2021

Research article

AMBTC-based visual secret sharing with different meaningful shadows

Shudong Wang[1,2], **Yuliang Lu**[1,2,*], **Xuehu Yan**[1,2], **Longlong Li**[1,2] **and Yongqiang Yu**[1,2]

[1] National University of Defense Technology, Hefei 230037, China

[2] Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

* **Correspondence:** Email: publicLuYL@126.com.

Abstract: Secret sharing based on Absolute Moment Block Truncation Coding (AMBTC) has been widely studied. However, the management of stego images is inconvenient as they seem indistinguishable. Moreover, there exists a problem of pixel expansion, which requires more storage space and higher transmission bandwidth. To conveniently manage the stego images, we use multiple cover images to make the stego images seem to be visually different from with each other. Futhermore, the stego images are different, which will not cause the attacker's suspicion and increase the security of the scheme. And traditional Visual Secret Sharing (VSS) is fused to eliminate pixel expansion. After images are compressed by AMBTC algorithm, the quantization levels and the bitmap corresponding to each block are obtained. At the same time, when the threshold is (k, k), bitmaps can be recovered losslessly, and the slight degradation of image quality is only caused by the compression itself. When the threshold is another value, the recovered image and the cover images can be recovered with satisfactory image quality. The experimental results and analyses show the effectiveness and advantages of our scheme.

Keywords: absolute moment block truncation coding; visual secret sharing; image compression; no pixel expansion; meaningful shadows

1. Introduction

At present, compared with massive multimedia information, the computer storage resources and network bandwidth provided by hardware technology are limited after all, which makes the storage and transmission of information a thorny problem. It is unrealistic to solve this problem by simply increasing memory capacity, channel bandwidth and processing speed of computer. Effective image compression is the basis of all kinds of dynamic image compression and transmission. Image compression can reduce the amount of data by lowering the redundancy and irrelevance of formatted image

data.

Most of the images in the network are stored and transmitted in the form of compression. Compression is the process of representing data in a compact form rather than in its original or incompact form [1]. Lossy compression is much more easy to achieve, and because of the limitations of human vision it can get better compression ratios compared with loseless compression. Compressed images have the advantages of simple calculation and low distortion rate. The most common methods of compression transforms include AMBTC [2], Discrete Cosine Transform (DCT) [3] and Discrete Wavelet Transform (DWT) [4].

AMBTC is an improvement of Block Truncation Coding (BTC) technology. Compared with BTC, the compression process of AMBTC is faster [5]. And the image quality after AMBTC compression is relatively better. Compared with other compression techniques, AMBTC has the advantages of fast coding speed, low computational cost and real-time implementation. Furthermore, it is insensitive to channel error and can obtain satisfactory image quality, so it is widely used. The comparison of bitmap (BMP) image and compression methods based on AMBTC, DCT, and DWT are shown in the Table 1, where Compression Method (CM), Evaluating Indicator (EI), Compression Ratio (CR), Compression Speed (CS), Storage Bandwidth (RSB), and Image Quality (IQ) are included in the table.

Table 1. The performance comparison of different compression methods.

CM / EI	BMP	AMBTC	DCT	DWT
CR	1	4	10–40	4–40
CS	Fastest	Fast	Slower	Slowest
RSB	Wide	Narrow	Narrower	Narrowest
IQ	Best	Good	Quite Good	Better

AMBTC is a lossy data compression algorithm for gray images. Because of its simple physical implementation and quick encoding and decoding ability, AMBTC was once widely used in broadcasting and television. It has been introduced into color image compression, namely color unit compression. Although the latest research using Progressive and Iterative Approximation for Least Square (LSPIA) fitting has been able to achieve lossless video compression [6], video compression based on AMBTC is still of great significance. In the military industry field, especially in the field of aviation and aerospace, many factors need to be considered, such as CR, CS, RSB and IQ. In order to reduce energy consumption and improve processing speed, spacecraft should choose compression algorithm with narrow bandwidth, fast computational speed and satisfactory image quality. In addition, binary images require narrow bandwidth, but the image quality is not desirable. On the contrary, color images have the satisfactory quality but require wide bandwidth. Due to the excellent characteristics of image compression based on AMBTC, it can quickly pass back important images. The research on the key technologies of AMBTC image secret sharing is expected to promote the development of fast secret image transmission in the fields of edge computing, aerospace and Unmanned Aerial Vehicle (UAV).

As the visual basis of human perception of the world, image is an important means to obtain, express and transfer information. Through the analysis of images, automated carp species identification [7], palmprint identification [8], energy management [9], prediction of rainfall time series [10] and so on can be realized. With the wide application and rapid development of network and multimedia

technology, digital images become easy to obtain, transmit and modify. The security of digital images has attracted more and more attention of scientists and engineers [11]. Images can be transmitted by computers, mobile phones or other communication devices. Therefore, in the process of storage and transmission, they may be stolen. Consequently, image encryption is particularly important [12]. Nonlinear technology of multiple images encryption scheme has become a hot topic, and the encryption scheme based on Latin squares can reduce the time complexity and improve the performance of image encryption [13].

In 1979, Shamir [14] and Blakley [15] proposed the concept of secret sharing for the first time. The (k, n) threshold secret sharing sheme means that a secret is divided into n pieces, when collecting any k or more shares can recover the secret. However, we cannot decrypt when less than k stego images are obtained, and no information about the secret will be revealed.

In 1994, Naor and Shamir [16] proposed the VSS scheme, the key advantage of which is stacking-to-see. According to the basic principle of implementation, VSS can be roughly divided into codebook-based VSS [17] and Random Grid (RG)-based VSS (RGVSS) [18, 19]. The encryption of binary secret image based on RG was first proposed by Kafri and Keren [20]. Subsequently, compared with codebook-based VSS, RGVSS has attracted much more attention owing to its superiority in no pixel expansion, easy to implement and no codebook design. However, VSS generally cannot achieve the lossless recovery of secret image, so the follow-up research is devoted to improving the recovery quality of secret image [21, 22, 24, 25]. And even the threshold was extended later [23]. The latest research [26] has been able to achieve satisfactory quality and imperceptibility.

The VSS has the following advantages:

- It has the characteristic of loss tolerance. Even if some shadow images are lost, the secret image can be recovered successfully.
- Prevent the abuse of power caused by excessive concentration.
- The attacker must obtain enough shadow images to recover the secret image, which ensures the security and integrity.
- Without increasing the risk, the reliability of the system is increased.

At present, there are less research on secret sharing of compressed images, although most of the images transmitted on the network are compressed. Yang and Wu considered secret sharing of AMBTC images [5, 27–29], which plays an important role in the compressed domain for secret sharing applications. Their schemes extend Ou and Sun's scheme [30] from $(2, n)$ threshold to (k, n) threshold. Furthermore, the scheme proposed by Yang and Wu realizes authentication and reversibility, in which reversibility means that the cover images can also be recovered. Reversible cover images play an important role in law enforcement and medical diagnosis [31]. Nevertheless, the schemes they proposed exist the problems of pixel expansion and stego images looking the same to the naked eye, which is not convenient to manage.

In general, the major challenges are as follows:

- At present, a large number of images need to be transmitted. Especially in the scene which requires high-speed of image transmission, it is particularly important to compress the image before transmission.
- Images can be transmitted by computers, mobile phones or other communication devices. Therefore, in the process of storage and transmission, images may be easily stolen.

- The current secret sharing scheme of AMBTC compressed image has the problems of pixel expansion and the stego images are the same visually, which is inconvenient to manage them.

The main contributions of the AMBTC-based RGVSS scheme with meaningful shadows proposed in this paper are as follows:

- AMBTC compression is used before secret image sharing to reduce the amount of information to be transmitted and shared.
- Even if the attacker get several stego images, he doesn't know any information about the secret image. Thus the security of the secret image is guaranteed.
- The quality of both the recovered secret image and the recovered cover images is satisfactory. The stego images are meaningful and there is no pixel expansion, which is convenient for the management of stego images and is conducive to saving storage space.

The rest of the paper is organized as follows. Section 2 briefly introduces the basic concept of AMBTC, and presents the compression and decompression process of it. Meanwhile, section 2 also simply introduces the VSS. In section 3, our scheme is given in more details, and the theoretical analysis of the proposed scheme is provided. The experimental results and the analysis of the experimental data are demonstrated in section 4. Finally, concluding remarks are given in section 5.

2. Preliminaries

2.1. AMBTC

AMBTC is a lossy data compression algorithm for gray image. Because of its simple physical implementation and fast processing, it was once widely used in broadcasting and television [33]. It has been introduced into color image compression, namely color unit compression [32]. In the field of military industry, especially in the field of aviation and aerospace, many factors need to be considered, such as bandwidth, computing time, complexity and image quality. In order to reduce energy consumption and improve processing speed, we should choose a compression algorithm with narrow bandwidth, low computational complexity and high image quality applying to the field of aviation and aerospace. Compared with DCT and DWT, the image quality of AMBTC is relatively poor, but the computational complexity is much lower. Weighing multiple indicators, the performance of AMBTC compression algorithm is better than other compression algorithms. In 1997, the United States used it for image compression of Mars Pathfinder.

AMBTC is a fast image compression algorithm that processes pictures in units of blocks. In each block, the original mean value and standard deviation are kept while the gray levels are reduced to achieve the purpose of compression. If the 4×4 block is used as the basic unit and 8-bit integers are used for transmission or storage, this algorithm can achieve a 4:1 compression ratio. If larger blocks are used, higher compression ratio can be obtained, but the image quality will be reduced accordingly. And after AMBTC compression, the image storage format is BMP.

In this paper, AMBTC compression is used to reduce the information need to be hidden in the process of secret sharing of gray image. Traditional VSS scheme needs to share gray image, while the scheme in this paper only needs to share binary image of the same size.

2.1.1. Compression phase

BTC is a block based lossy compression technology for gray image in most cases, which uses quantization levels to reduce the number of gray pixels to be stored in each block. When the AMBTC technology is used to compress the image, each image is divided into non overlapping blocks with $t \times t$ pixels, the value of t is usually taken as 4. In the i-th block of the image, the average pixel value of this block is calculated as

$$V_i = \frac{\sum_{j=1}^{t\times t} x_{i,j}}{t \times t} \tag{2.1}$$

The generation standard of bitmap is as follows: if $x_{i,j} \leq V_i$, the corresponding position in bitmap is marked as "0" ; otherwise, the corresponding position in bitmap is marked as "1" . Note that q is the number of "1" in the bitmap, and the formulas for calculating the two quantization levels are shown in Eq (2.3) and Eq (2.2) respectively.

$$H_i = \frac{\sum_{x_{i,j}\geq V_i} x_{i,j}}{q} \tag{2.2}$$

$$L_i = \frac{\sum_{x_{i,j}\leq V_i} x_{i,j}}{t \times t - q} \tag{2.3}$$

Then the i-th block is compressed into two quantization levels and the bitmap.

2.1.2. Decompression phase

In the decompression phase, if the quantization levels and bitmaps are obtained at the same time, the corresponding blocks can be restored by replacing "0" in the bitmap with low quantization levels L_i and "1" with high quantization levels H_i.

2.2. Visual secret sharing

VSS [34] can be recovered without any relevant cryptographic knowledge, and the recovery process is simple. According to the basic principle of implementation, VSS can be roughly divided into codebook-based VSS and RG-based VSS. The scheme based on RG has the advantages of simple implementation and no pixel expansion, so the current research is mostly based on the implementation of it [35]. However, VSS generally cannot achieve the lossless recovery of secret images, so the follow-up research is devoted to improving the recovery quality of secret image [21, 22, 24, 25]. The original visual secret sharing was proposed by Naor and Shamir in 1994 [16]. In threshold VSS, binary secret image is encrypted into random shadow images. When decrypting, more than k shadow images are superimposed, and the secret can be seen through vision. Its core idea is to decrypt through Human Vision System (HVS), without any encryption and decryption knowledge and computing equipment.

At present, VSS is mainly applied to binary image. Considering that the bitmap of AMBTC image can be regarded as a binary image, the bitmap information of the secret image can be hidden through the bitmap of different cover images to realize secret sharing.

3. The proposed scheme

3.1. Motivation

Due to the excellent characteristics of AMBTC images, important images can be quickly passed back. Research on the key technology of AMBTC secret image sharing is expected to promote the development of important secret image fast transmission in the fields of edge computing, aerospace and drones.

However, all the schemes proposed in [5, 27–29] with the pixel expansion, which will cause great pressure on storage and transmission. At the same time, the stego images of the four schemes are similar to the naked eye, and it is inconvenient to manage shadow images. In addition, the quality of the stego images varies when distributed to the participants, which may arouse the suspicion of attackers.

The goal of the proposed scheme is to solve the problems of pixel expansion and inconvenient shadow images management. First of all, the proposed scheme adopts VSS scheme based on RG, which does not produce pixel expansion at all. Secondly, for the (k, n) threshold sharing scheme, n cover images are used to generate n visually different stego images.

3.2. Framework of the proposed scheme

The proposed scheme includes three phases: (1) compression phase, (2) sharing phase, (3) recovery phase. Figure 1 demonstrates the framework of the proposed scheme. In addition, the notations used in this paper are introduced in Table 2.

Table 2. The notations used in the paper.

Notations	Decriptions
k	The minimum number of shadow images (bitmaps) need to be obtained in recovery phase.
t	The number of stego shadow images actually obtained by the dealer in recovery phase.
n	The number of cover images used in sharing phase and the total number of shadow images.
$t \times t$	The block size used in AMBTC compression.
i	The i-th block of the image.
SC_i	Substitute the shadow images with L and H.
$M \times N$	The size of the bmp image.
V_i	The average pixel value of the current block.
H_i	In the current block, the high quantization level, in other words, the pixels higher than the average pixel value are averaged.
L_i	In the current block, the low quantization level, in other words, the pixel lower than the average pixel value are averaged.
H	The set of H_i, and we save it with images.
L	The set of L_i, and we save it with images..
$BM_{i,j}$	The value of the bitmap in the position of i, j.
BM	The entire bitmap of the image.

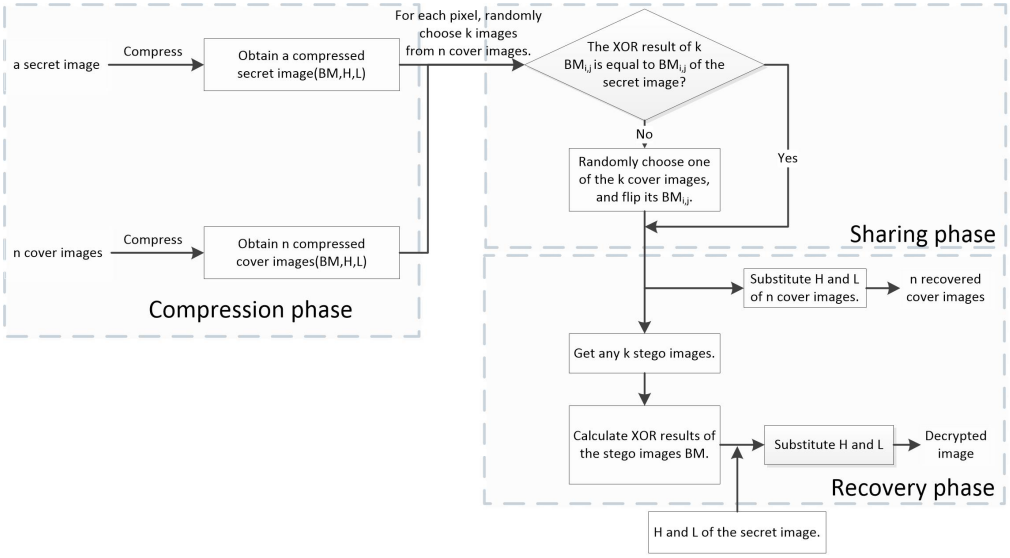


Figure 1. Framework of the proposed scheme.

3.3. Compression phase

In compression phase, the secret image and the cover images are compressed by AMBTC algorithm to generate high and low quantization levels and bitmaps, as stated in 2.1.1. We will give a detailed description of the compression process in Algorithm 1.

Algorithm 1: The compression algorithm of secret image and cover images.

Input: An original BMP image of size $M \times N$.
Output:BM, H and L.
Step 1: Divide the picture into 4×4 blocks.
Step 2: For each block $(i, j) \in \{(i, j)|1 \leq i \leq \frac{M}{4}, 1 \leq j \leq \frac{N}{4}\}$, repeat Steps 3–4 (the commonly used image size is an integral multiple of four).
Step 3: Calculate V_i of each block, take the average value of the pixel value less than V_i and the average value of the pixel value greater than V_i as L and H respectively.
Step 4: The position of the pixel value less than V_i is recorded as "0" , and greater than V_i is recorded as "1" in the bitmap.
Step 5: Output BM, H and L.

In this paper, shadow images refer to the binary images generated by embedding the information of secret image bitmap into the bitmaps of cover images, while stego images refer to the images generated by substituting the quantization levels of the cover image into the shadow images, denoted by SC_i.

In compression phase, a secret image and n cover images are compressed into the bitmaps and quantization levels through the same compression process.

In sharing phase, for each pixel of the secret image bitmap, randomly choose k images from n cover images, and judge whether the XOR result of k images' $BM_{i,j}$ is equal to that of secret image $BM_{i,j}$. If equal, change nothing. Otherwise, randomly choose one of the k cover images, and flip $BM_{i,j}$ of this image.

In recovery phase, as long as any k $(0 < k \leq n)$ or more participants share their stego images, the

bitmap of the recovered image is obtained when XOR decryption is applied. By replacing "0" and "1" in the bitmap with H_i and L_i, we can get the decrypted image.

3.4. Sharing phase

In sharing phase, the (k, n) threshold is realized by using n cover images, and any k of them embeded secret information can decrypt the secret image. The proposed scheme mainly realizes the sharing of bitmaps. For the sharing of each pixel value, randomly select k cover images. If the XOR result of their $BM_{i,j}$ is equal to the value of $BM_{i,j}$ of the secret image, no operation is performed; otherwise, one of the k images is randomly selected, and the $BM_{i,j}$ of it is reversed. Finally, H and L of each cover image generated in the compression process is substituted into the shadow images. Therefore, n stego images are generated, as described in Algorithm 2.

Algorithm 2: Bitmaps sharing algorithm.

Input: BM of the secret image and BMs of n cover images.
Output: SC_i $(i = 1, 2, \cdots, n)$.
Step 1: For each pixel of the secret image bitmap, repeat Steps 2–4.
Step 2: Randomly select k of n cover images, and calculate the XOR result of their $BM_{i,j}$.
Step 3: If the result is equal to the $BM_{i,j}$ of the secret image, return to step 1. Otherwise, go to step 4.
Step 4: Randomly select one of the k images in step 2, and flip its $BM_{i,j}$.
Step 5: Substitute H and L of each cover image generated in the compression process into the shadow images obtained in Step 4.
Step 6: Output SC_i $(i = 1, 2, \cdots, n)$.

3.5. Recovery phase

In recovery phase, the dealer obtains at least k stego images and takes the XOR result of the stego images' BM as the bitmap of the recovered image. Taking the shadow images as the bitmaps of the cover images and substituting H and L generated in the compression phase into them, the cover images can be recovered. The decrypted image can be obtained by replacing "0" with the low quantization level of the secret image obtained in the compression phase and "1" with the high quantization level, which is detailed in Algorithm 3.

Algorithm 3: Recovery algorithm of the secret image and cover images.

Input: t $(k \leq t \leq n)$ stego images, H and L of secret image and cover images.
Output: The recovered image and n recovered cover images.
Step 1: Take the XOR result of the t stego images' BM as the bitmap of the recovered image.
Step 2: Take t shadow images as the bitmaps of the recovered cover images.
Step 3: For $t + 1$ bitmaps, replace the bitmaps with the corresponding H and L generated in the compression phase.
Step 4: The gray srcret image and t cover images are recovered.

3.6. Theoretical analysis

Herein, analysis on the performance of the proposed scheme from visual quality and security is given as below. The contrast used in this paper refers to the evaluation of the similarity between the recovered image and the secret image and the clarity of human eye recognition, rather than the contrast of the image in traditional image processing.

Definition 1. *(Contrast) The visual quality of the recovered image is evaluated by contrast, which determines the degree of recognition of the recovered image by human eyes. Compared with the secret image, the contrast α is defined as*

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S'[AS\,0] = 0) - P(S'[AS\,1] = 0)}{1 + P(S'[AS\,1] = 0)}. \tag{3.1}$$

Where P_1 (P_0) denotes the probability that the black (white) area corresponding to the secret image be white in the recovered image. P_0 is the probability that the white area decode correctly, and P_1 is the probability that the black area decode incorrectly. The bigger α, the higher visual quality.

Theorem 1. *(Correctness and security) The proposed scheme is an effective construction of VSS, and it meets the requirements of correctness and security.*

Proof. The security of the proposed scheme is guaranteed by (k, n) threshold VSS scheme based on RG. Less than k secret images disclose no information of secret image bitmap. At the same time, bitmaps can be recovered losslessly when threshold is (k, k), and the slight degradation of image quality is only related to the compression itself. Therefore, the correctness of the scheme is realized.

The bitmaps of n cover images are uncorrelated, that is, pixels in the same position can be regarded as random values. Therefore, the contrast of the recovered image can refer to [35].

As proved in Chen and Tsao's scheme [35], the contrast of XOR results of w collected stego images is $\alpha = \left(2 \times \binom{w}{k}\right) / \left((2^w + 1) \times \binom{n}{k} - \binom{w}{k}\right)$.

When $0 \le w < k$, $\alpha = 0$. Consequently, no secret image information will be divulged.

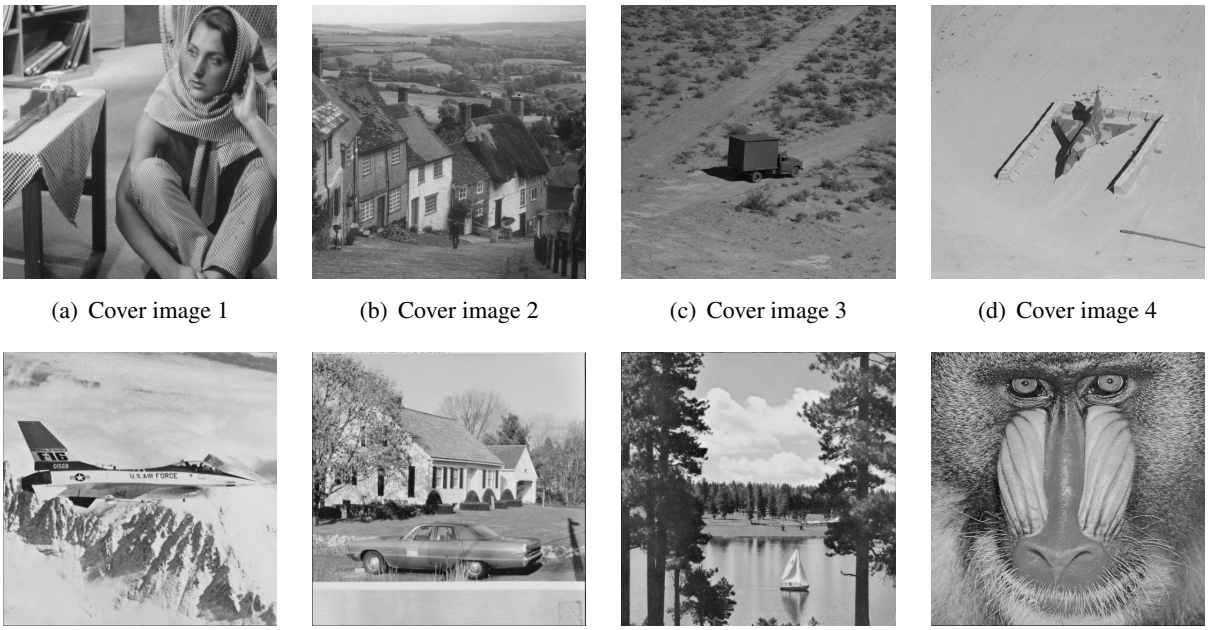
When $k \le w \le n$, $\alpha \ge 0$. The numerator $2 \times \binom{w}{k}$ is always greater than zero. Given $n \ge w$, we have $(2^w + 1) \times \binom{n}{k} = (2^w + 1) \times (n(n-1)\cdots(n-k+1)) / (1 \times 2 \times \cdots \times k) \ge \binom{w}{k} = (w(w-1)\cdots(w-k+1)) / (1 \times 2 \times \cdots \times k)$. Therefore, the denominator $(2^w + 1) \times \binom{n}{k} - \binom{w}{k}$ is greater than zero, so is the contrast α, implying the secret information on the recovered result is recognizable. □

4. Experimental results and analyses

We will present the experimental results and analyses to show the effectiveness and advantages of our scheme in this section. The secret image and the cover images used in this scheme are all uncompressed grayscale images with 512×512 pixels. In order to compare with the scheme proposed by Wu et al. [29] conveniently, we use the same cover images as their scheme, which are demonstrated

in Figure 2(a)–2(h). And all the images used in our scheme are downloaded from USC-SIPI and CVG-UGR image databases.

An example of a $(2, 5)$ threshold is shown in Figure 3. Among them, Figure 3(a) shows the secret image, Figure 3(b)–3(f) show the five stego images, and Figure 3(g)–3(h) show the reconstructed images using 2 stego image with XOR recovery. Figure 3(b)–3(f) are generated by embedding the bitmap of secret image into the bitmaps of Figure 2(a)–2(e) using the VSS scheme. Simultaneously, we use the same evaluation indexes as the compared scheme to assess the quality of the stego images in Figure 3, which are illustrated in Table 4. The Peak Signal to Noise Ratio (PSNR) of original uncompressed cover images compared with AMBTC cover images is represented by PSNR_{A-O}, the PSNR of original uncompressed images compared with AMBTC stego image is represented by PSNR_{S-O}, and the PSNR of AMBTC cover image compared with AMBTC stego image is represented by PSNR_{S-A}. In Wu et al. [29], PSNR_{A-O} is approximately 29.4 dB and PSNR_{S-O} is approximately 24.6 dB. The value of PSNR decreases by 4.8 dB because of the sharing process, while in our scheme only decreases by about 1.1 dB on average. Therefore, the visual quality of the stego images is much better in our scheme.



(a) Cover image 1 (b) Cover image 2 (c) Cover image 3 (d) Cover image 4

(e) Cover image 5 (f) Cover image 6 (g) Cover image 7 (h) Cover image 8

Figure 2. Eight uncompressed cover images used in this paper.

4.1. Visual quality of stego images

PSNR is used to evaluate the visual quality of stego images as well. The higher PSNR is, the better the image quality is. The PSNR of the stego images for (2,2) threshold are shown in Table 3. We use Figure 2(a)–2(b), 2(c)–2(d), 2(e)–2(f) and 2(g)–2(h) as the cover images respectively. The PSNR_{S-A} values of all the stego images are greater than 34 dB, which means that the proposed scheme can get better visual quality of stego images.

(a) Secret image (b) Stego image 1 SC_1 (c) Stego image 2 SC_2 (d) Stego image 3 SC_3

(e) Stego image 4 SC_4 (f) Stego image 5 SC_5 (g) Reconstructed image $SC_1 \otimes SC_2$ (h) Reconstructed image $SC_3 \otimes SC_4$

Figure 3. An experimental example of the proposed (2,5) threshold. (a) Secret image, (b)–(f) stego images SC_1, SC_2, SC_3, SC_4, SC_5, (g) reconstructed image $SC_1 \otimes SC_2$, and (h) reconstructed image $SC_3 \otimes SC_4$.

Table 3. PSNR of the stego images for the (2,2) threshold.

Cover images in Figure 2	$PSNR_{S-A}$(dB) of stego image 1	$PSNR_{S-A}$(dB) of stego image 2
(a) (b)	35.0359	34.4229
(c) (d)	34.7117	39.6069
(e) (f)	36.8109	35.4058
(g) (h)	34.8926	33.6556

Table 4. Visual quality of the stego images in Figure 3 (unit dB).

Stego image	$PSNR_{A-O}$		$PSNR_{S-O}$		$PSNR_{S-A}$	
	Our method	Wu et al. [29]	Our method	Wu et al. [29]	Our method	Wu et al. [29]
1	32.8368	29.3867	32.2722	24.6240	39.0208	26.4169
2	34.5202	29.3867	33.4245	24.6231	38.3990	26.4100
3	35.2864	29.3867	34.0183	24.6551	38.6779	26.4324
4	41.1087	29.3867	39.4648	24.6125	43.6731	26.4180
5	35.9097	29.3867	35.0476	24.6051	40.8447	26.4001

4.2. Quality of the recovered secret image

In order to compare with the scheme proposed by Wu et al. [29], we analyze the experiments of (2,2) threshold and $(2, 5)$ threshold in detail above. Herein, we adopt PSNR and SSIM to evaluate the visual quality of the recovered secret image. In our scheme, (k, n) threshold are used to do the test of the proposed scheme, among which k and n both range from 2 to 8.

We have tested the influence of n on the quality of the recovered secret image when k is a constant, and the influence of k on the quality of the recovered secret image when n is a constant, as shown in Figure 4(a)–4(c).

We have tested that when k is constant, the impact of n changes on recovered secret image quality and when n is constant, the impact of k changes on recovered secret image, which is demonstrared in Figure 4(a)–4(c). Among them, Figure 4(a) shows when k is constant, the visual quality of the recovered secret image decreases as n increases. Figure 4(b) shows when n is constant, the visual quality of the recovered secret image increases as k increases. The content shown in Figure 4(c) is consistent with the experimental result of Figure 4(a) and 4(b).

4.3. Comparisons with related schemes

In this subsection, we compare the proposed method with other related schemes, and the content is shown in Table 5. The reason why we choose the listed schemes is that they are all secret sharing schemes of AMBTC compression, and for several of them the key technology is VSS.

The same evaluation index ER(Embedding rate) is adopted to evaluate the embedding ability, which is calculated by Eq (4.1). It is obvious that ER is expected to be as large as possible. Compared with other methods, the proposed scheme has no pixel expansion, and after the sharing process, it can generate different stego images which is convenient for the management of these images. The scheme proposed by Yang and Wu et al. [27] requires the users to manage multiple shadows. With the increase of k and n, it is a more and more annoying disadvantage.

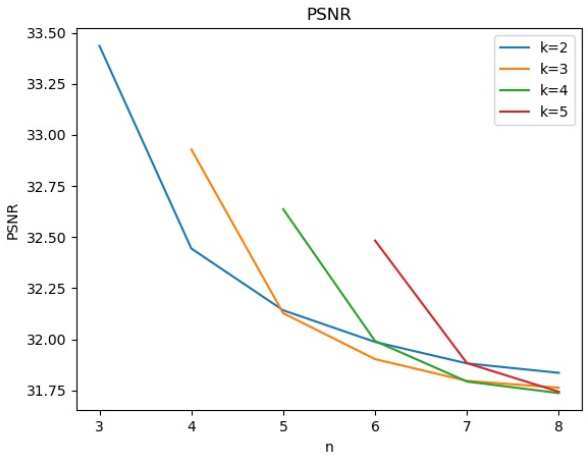
Owing to the fact that we employ the VSS, the pleasant advantage of our scheme is that the algorithm for the whole process is relatively simple and does not require a lot of calculations. Meanwhile, when the threshold is (k, k), the bitmap of secret image can be recovered losslessly, and the slight degradation of image quality is only related to the compression algorithm itself. In other cases, the decrypted image and the cover images can be recovered with satisfactory image quality. Meanwhile, the proposed scheme has no authentication capability, which will be the future work of our scheme.

$$ER = \frac{number\ of\ shared\ bits}{number\ of\ bits\ in\ stego\ image} \tag{4.1}$$

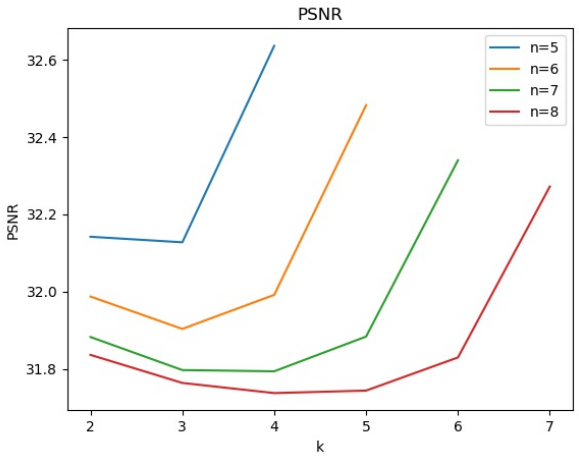
4.4. Discussion

The experimental results show that the quality of the stego images and the recovered secret image are better than the scheme proposed by Wu et al. [29]. And the value of ER is acceptable compared with other secret sharing schemes of AMBTC. Our scheme has total supremacy in the time cost, pixel expansion and meaningful shadows generation.

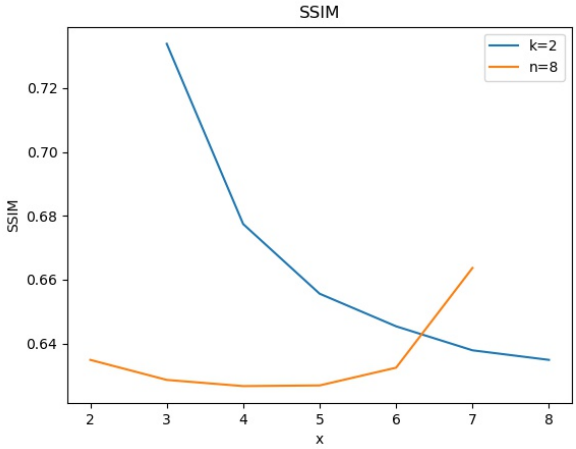
However, our scheme has no authentication capability. Moreover, we only do the secret image sharing of the AMBTC compressed image bitmap, and the quantization levels need to be saved by the



(a) PSNR of k is constant



(b) PSNR of n is constant



(c) SSIM of k=2 and n=8

Figure 4. Visual quality of the recovered secrer image.

Table 5. Comparison of significant properties with related schemes.

Schemes	Key technique	ER	Stego image format	Pixel expansion	Reversible	Functionality
Ref. [27]	VSS,AMBTC	0.5	AMBTC compressed	16 times	Yes	SIS,steganography
Ref. [5]	VSS,AMBTC	–	AMBTC compressed	16 times	Yes,partial.	Stacking-to-see decryption
Ref. [28]	PSIS,HMAC,AMBTC	0.25	AMBTC compressed	2 times	Yes	SIS,authentication,steganography
Ref. [29]	PSIS,HMAC,AMBTC	0.25	AMBTC compressed	8 times	Yes,partial.	SIS,authentication,steganography
Our	VSS,AMBTC	0.5	AMBTC compressed	No	Yes	SIS,steganography

dealer, which may cause security problems. In the future work, we will consider sharing the bitmap and quantization levels at the same time, as well as providing authentication function.

5. Conclusions

In this paper, an AMBTC-based visual secret image sharing scheme with meaningful shadows is proposed. Firstly, the secret image and n cover images are compressed into bitmaps and quantization levels. Then, in the sharing phase, the information of the secret image bitmap is hidden in the bitmaps of cover images. Finally, by obtaining enough shadow images, the secret image bitmap is recovered by XOR operation. There is no pixel expansion and the shadow images are meaningful, which are the biggest advantages of the paper. The experimental results and theoretical analysis prove the effectiveness of the proposed scheme, and the visual quality and security of the scheme are satisfactory.

However, only the bitmap of AMBTC compressed image is shared according to the principle of VSS, and the quantization levels need to be saved by the dealer, which may lead to security problems. Moreover, our scheme has no authentication capability. In the future, we will consider the sharing of the bitmap and quantization levels at the same time. Besides , we plan to provide authentication function in the future.

Acknowledgement

This work is supported by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (Number: 61602491).

Conflict of interest

The authors declared that they have no conflict of interest, nor any commercial or associative interest conflict in relation to the submitted work.

References

1. R. I. Yousif, N. H. Salman, Image compression based on arithmetic coding algorithm, *Iraqi J. Sci.*, **2021** (2021), 329–334.
2. S. Kim, D. Lee, J. S. Kim, H. J. Lee, A block truncation coding algorithm and hardware implementation targeting 1/12 compression for lcd overdrive, *J. Display Technol.*, **12** (2015), 376–389.
3. V. Holub, J. Fridrich, Low-complexity features for jpeg steganalysis using undecimated dct, *IEEE Trans. Infor. Forensics Secur.*, **10** (2015), 219–228.
4. R. Starosolski, Skipping selected steps of dwt computation in lossless jpeg 2000 for improved bitrates, *Plos One*, **11** (2016), e0168704.
5. X. Wu, D. Chen, C. N. Yang, Y. Y. Yang, A (k , n) threshold partial reversible ambtc-based visual cryptography using one reference image, *J. Visual Commun. Image Representation*, **59** (2019), 550–562.
6. M. Ebadi, A. Ebrahimi, Video data compression by progressive iterative approximation, *Int. J. Interact. Multimedia Artif. Intell.*, **6** (2020), 89–195.

7. A. Ab, B. An, C. Tg, Deep learning-based appearance features extraction for automated carp species identification, *Aquacultural Eng.*, **89** (2020), 102053.
8. J. Wei, B. Ling, K. W. Chau, L. Heutte, Palmprint identification using restricted fusion-sciencedirect, *Appl. Math. Comput.*, **205** (2008), 927–9348.
9. S. Shamshirband, T. Rabczuk, K. W. Chau, A survey of deep learning techniques: Application in wind and solar energy resources, *IEEE Access*, **7** (2019), 164650–164666.
10. C. L. Wu, K. W. Chau, Prediction of rainfall time series using modular soft computingmethods, *Eng. Appl. Artif. Intell.*, **26** (2013), 997–1007.
11. Y. Wu, Q. Wu, N. Dey, R. S. Sherratt, Learning models for semantic classification of insufficient plantar pressure images, *Int. J. Interact. Multimedia Artif. Intell.*, **6** (2020), 51–61.
12. G. Ye, K. Jiao, H. Wu, C. Pan, X. Huang, An asymmetric image encryption algorithm based on a fractional-order chaotic system and the rsa public-key cryptosystem, *Int. J. Bifurcations Chaos*, **30** (2020), 2050233.
13. J. Zhou, N. R. Zhou, L. H. Gong, Fast color image encryption scheme based on 3d orthogonal latin squares and matching matrix, *Optics Laser Technol.*, **131** (2020), 106437.
14. A. Shamir, How to share a secret, *Commun. ACM*, **22** (1979), 612–613.
15. G. R. Blakley, Safeguarding cryptographic keys, in *1979 International Workshop on Managing Requirements Knowledge*, IEEE Computer Society, 1979.
16. M. Naor, A. Shamir, Visual cryptography, *Lect. Notes Comput. Sci.*, **1994** (1994), 1–12.
17. H. B. Chen, H. C. Hsu, S. T. Juan, An easy-to-implement construction for (k, n)-threshold progressive visual secret sharing schemes, preprint, arXiv:2002.09125.
18. R. De Prisco, A. De Santis, On the relation of random grid and deterministic visual cryptography, *Inf. Forensics Secur. IEEE Trans.*, **9** (2014), 653–665.
19. C. N. Yang, C. C. Wu, D. S. Wang, A discussion on the relationship between probabilistic visual cryptography and random grid, *Inf. Sci.*, **278** (2017), 141–173.
20. O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, *Optics Lett.*, **12** (1987), 377.
21. X. Yan, X. Liu, C. N. Yang, An enhanced threshold visual secret sharing based on random grids, *J. Real Time Image Proc.*, **14** (2018), 61–73.
22. X. Wu, W. Sun, Improved tagged visual cryptography by random grids, *Signal Proc.*, **97** (2014), 64–82.
23. T. Guo, F. Liu, C. K. Wu, K out of k extended visual cryptography scheme by random grids, *Signal Proc.*, **94** (2014), 90–101.
24. X. Yan, S. Wang, X. Niu, C. N. Yang, Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality, *Digital Signal Proc.*, **38** (2015), 53–65.
25. X. Yan, W. Q. Yan, L. Liu, Y. Lu, Penrose tiling for visual secret sharing, *Multimedia Tools Appl.*, **79** (2020), 32693–32710.

26. G. Ye, C. Pan, Y. Dong, K. Jiao, X. Huang, A novel multi-image visually meaningful encryption algorithm based on compressive sensing and schur decomposition, *Trans. Emerging Telecommun. Technol.*, **32** (2021), e4071.
27. C. N. Yang, X. Wu, Y. C. Chou, Z. Fu, Constructions of general (k, n) reversible ambtc-based visual cryptography with two decryption options, *J. Visual Commun. Image Representation*, **48** (2017), 182–194.
28. X. Wu, C. N. Yang, Invertible secret image sharing with steganography and authentication for ambtc compressed images, *Signal Proce. Image Commun.*, **78** (2019), 437–447.
29. X. Wu, C. N. Yang, Partial reversible ambtc-based secret image sharing with steganography, *Digital Signal Proc.*, **93** (2019), 22–33.
30. D. Ou, W. Sun, Reversible ambtc-based secret sharing scheme with abilities of two decryptions, *J. Visual Commun. Image Representation*, **25** (2014), 1222–1239.
31. X. Yan, Y. Lu, L. Liu, X. Song, Reversible image secret sharing, *IEEE Trans. Inf. Forensics Secur.*, **15** (2020), 3848–3858.
32. D. M. Liou, Y. Huang, N. Reynolds, A new microcomputer based imaging system with technique, in *IEEE Region 10 Conference on Computer and Communication Systems*, 2002.
33. D. Healym O. Mitchell, Digital video bandwidth compression using block truncation coding, *IEEE Trans. Commun.*, **29** (1981), 1809–1817.
34. D. Wang, T. Song, L. Dong, C. Yang, Optimal contrast grayscale visual cryptography schemes with reversing, *IEEE Trans. Inf. Forensics Secur.*, **8** (2013), 2059–2072.
35. T. H. Chen, K. H. Tsao, Threshold visual secret sharing by random grids, *J. Syst. Software*, **84** (2011), 1197–1208.

AIMS Press