EasyChair Preprint

№ 765

Efficient Cipher-Only Attack of a Stream Cipher in RDHEI Based on Pixel Smoothness Estimation

Yuyu Chen, Zenghui Li, Beibei Liu, Jiacheng Zhang, Bangxu Yin and Hongjie He

February 2, 2019

Efficient Cipher-Only Attack of a Stream Cipher in RDHEI Based on Pixel Smoothness Estimation*

Yuyu Chen, Zenghui Li
Mao Yisheng Honors College
Southwest Jiaotong University
Chengdu Sichuan China
yuyu98210@qq.com

Beibei Liu, Jiacheng Zhang
Mao Yisheng Honors College
Southwest Jiaotong University
Chengdu Sichuan China
1098102679@qq.com

Bangxu Yin, Hongjie He †
the school of IST
Southwest Jiaotong University
Chengdu Sichuan China
hjhe@swjtu.edu.cn

ABSTRACT

Reversible data hiding in encrypted images (RDHEI) has recently emerged as an effective approach to protect the confidentiality of image content through encryption while assisting in the management of encrypted images by lossless hiding some additional data in encrypted images. In 2018, Khelifi proposed a cipher-only attack (COA) on the RDHEI methods where a bit-wise XOR encryption (also called as stream cipher) method was applied. In this work, we propose an efficiency COA method where the number of encrypted images can be effectively reduced for estimating the key stream with the same error rate. According to the given encrypted images, this work first estimates the smoothness probability of all pixel in the corresponding original images. And then, the weight coefficient of each pixel in the COA attack is assigned based on their estimated smoothness. The rationality of the proposed pixel smoothness estimation algorithm is discussed and analyzed from both theoretical and experimental aspects. Experimental results show that the error rate of the key stream estimated by the proposed COA method is less than 1/14 of that by the literature COA algorithm [10].

KEYWORDS

Image encryption; Reversible data hiding; Cipher-only attack; Pixel-smoothness

1.Introduction

Today, over two billion photos (images) are shared through the cloud-based sharing services every day. However, advancements of photo sharing have also raised concerns for privacy since photos potentially reveal great amount of sensitive information about people [1]. Image encryption is a privacy protection technique that converts an original image into a noise-like encrypted vision. To achieve effective management of encrypted images including copyright protection, integrity authentication and retrieval, some additional data need to be reversibly embedded in the encrypted image without knowing the original content of images [2, 3]. That is, the combination of image encryption and reversible data hiding (RDH) technique, which can embed additional data into a cover image and later enable the intended user to losslessly recover both the embedded data and the cover image [3,4], is expected to solve some new security problems in cloud computing applications. Recently, RDHEI technology has attracted great attention of many researchers.

In 2011, Zhang [2] proposed a joint RDHEI method. According to the encryption key, an original image was encrypted by the bitwise exclusive-or (XOR) operation, also known as the stream cipher. In encryption phase, the original image is represented as 8 binary images of bit-plane significant level. A content owner encrypts every binary image by an encryption key using a standard stream cipher. Then, the bitwise XOR results of the original bits and pseudo-random bits are calculated in order to encrypt every bit-plane significant level. Compared with other image encryption techniques, the stream cipher is faster and simple. What's more, the bit-planes of encrypted image generated by the bitwise XOR encryption method are independent, which provides more flexibility for the data hider to embed additional data. In Zhang's RDHEI method [2], the additional data was hidden by flipping the 3 least significant bits of part of encrypted pixels, and the fluctuation function was designed to infer the secret data and recover the original image. Due to the above advantages of the bit-wise XOR encryption method, most existing RDHEI methods that have been reported in the literature such as [5-8] apply a bit-wise encryption method to generate the encrypted images. After nearly a decade of development,, the performance of RDHEI technology including reversibility, embedding capacity and the quality of marked images after decryption have been significantly improved. For example, the embedding capacity is increased from the early less than 0.1 bit per pixel (bpp) [2,4,5,6] to 0.3 bpp[7], and further increased to nearly 1 bpp [8].

On the other hand, there is relatively little research on the security of encrypted images produced by the existing RDHEI methods. In fact, the security of RDHEI is critical because the primary purpose of encryption is to protect image content from information disclosure. Our research [9] found that the bitwise XOR encryption used in RDHEI technology has security risks. This is due to the fact that the position of original pixels had not changed though values of encrypted pixels randomly distributed in the range of [0, 255]. Recently, based on the spatial redundancy that characterizes natural images, Khelifi [10] proposed a cipher-only attack (COA) to further highlight the weakness of a bit-wise XOR encryption. Using the COA attack [10], 480 encrypted images generated by the same key are sufficient to accurately estimate the

key stream used to encrypt 5 most significant bit (MSB) planes. Obtaining many encrypted images generated with the same key is the key to the success of the COA attack. Obviously, the more the number of encrypted images required, the higher the attack cost.

To further reduce the cost of COA attacks, this work designs an efficient COA attack method for the bitwise XOR encryption adopted in RDHEI technology. The proposed algorithm can estimate the key stream with the same error rate with fewer encrypted images. From another viewpoint, the key stream estimated by the proposed COA algorithm has a lower error rate under the condition of the same number of encrypted images. This work has two contributions: (i) A pixel smoothness estimation method is designed based on encrypted images. (ii) The weight coefficient is adaptively determined based on the estimated pixel smoothness. The experimental results verify the effectiveness of the proposed COA algorithm.

The rest of this paper is organized as follows. In Section 2, the existing COA proposed in [10] is analyzed. The proposed COA method and experimental results are in Section 3 and Section 4, respectively. Finally, Section 6 summarizes the contributions and concludes the paper.

2. Analysis of COA proposed by Khelifi [10]

Let X denotes the original image set X={X^l|l=1,2,.., L}, where L is the number of gray images with size of m×n pixels. Using the same key stream Ψ, the encrypted image set $\widetilde{\mathrm{X}} = \{\widetilde{\mathrm{X}}^l|\mathrm{l}=1,2,..,\ \mathrm{L}\}$ were generated. The main purpose of COA is to get the estimated key stream (EKS) Φ based on the encrypted image set $\widetilde{\mathrm{X}}$, so that Φ is gradually equal Ψ, which is recorded as $\Phi \simeq \Psi$.

The main idea of the COA proposed in [10] is to use the inter-pixel redundancy that exists in natural images to obtain the EKS Φ. According to the encrypted image set $\widetilde{\mathrm{X}}$, the COA first calculates the q[th] (q=1,2,…,8) bit-plane $\widetilde{\mathrm{X}}_q^l = \{\tilde{x}_q^l(i,j)\}$ which is a binary image.

$$\tilde{x}_q^l(i,j) = \left\lfloor \frac{\tilde{x}^l(i,j)}{2^{(q-1)}} \right\rfloor mod\ 2 \tag{1}$$

where $\widetilde{\mathrm{X}}_8^l$ is the most significant bit-plane (MSB) and $\widetilde{\mathrm{X}}_1^l$ is the least significant bit-plane (LSB) of an encrypted image $\widetilde{\mathrm{X}}^l$. Next, calculate the probability of a pixel $\tilde{x}_q^l(i,j)$ in L binary images is the same as its horizontal estimation $\tilde{x}_q^l(i,j-1)$ and the vertical estimation $\tilde{x}_q^l(i-1,j)$.

Horizontal estimation:

$$p_q^h(i,j) = \frac{1}{L}\sum_{l=1}^{L}\left(1 - \left|\tilde{x}_q^l(i,j) - \tilde{x}_q^l(i,j-1)\right|\right) \tag{2}$$

Vertical estimation:

$$p_q^v(i,j) = \frac{1}{L}\sum_{l=1}^{L}\left(1 - \left|\tilde{x}_q^l(i,j) - \tilde{x}_q^l(i-1,j)\right|\right) \tag{3}$$

And then, according to $p_q^{\mathrm{h}}(i,j)$ or $p_q^v(i,j)$, the horizontal and vertical estimation formulas of the stream cipher key are obtained.

$$\varphi_q^h(i,j) = \begin{cases} \varphi_q(i,j-1), & if\ p_q^h(i,j) > 0.5 \\ 1 - \varphi_q(i,j-1), & otherwise \end{cases} \tag{4}$$

$$\varphi_q^v(i,j) = \begin{cases} \varphi_q(i-1,j), & if\ p_q^v(i,j) > 0.5 \\ 1 - \varphi_q(i-1,j), & otherwise \end{cases} \tag{5}$$

Based on the above four formula, the COA proposed in [10] can be summarized as follows. It is easy known from the Khelifi's COA [10] that the key stream is independently estimated for each bit-plane in a binary image from the recursive estimation formulas of the stream cipher key (4) and (5). The value of ESK mainly depends on the ratio calculated by (2) and (3).

Table 1: Summarizing of Khelifi's COA method

Input: $\{\widetilde{\mathrm{X}}^l$ |l=1,2,…,L}, where $\tilde{X}^l = \{\tilde{x}^l(i,j)|i = 1,2,\dots,m; j = 1,2,\dots,n\}$;

Output: the estimated value of the stream cipher key $\Phi = \{\Phi_q|\mathrm{q} = 1,2,\dots,8\}$

COA:

Step 1: $\forall q \in [1,8]$, estimate the stream cipher key of q[th] bit plane significance level $\Phi_q = \{\varphi_q(i,j)\}$;

Step 1.1： Calculates the q[th] bit-plane $\widetilde{\mathrm{X}}_q^l = \{\tilde{x}_q^l(i,j)\}$, which is a binary image, according to (1) .

Step 1.2: Horizontal estimation

Initialize $\varphi_q(1,1) = 0$,

calculate $\{\varphi_q^h(1,j)|j \in [2,\mathrm{n}]\}$ according to (2)

Step 1.3: Vertical estimation

$\forall \mathrm{j} \in [1,\mathrm{n}]$, calculate $\{\varphi_q^v(i,j)|\mathrm{i} \in [2,\mathrm{m}]$

from $\varphi_q(1,j)$ according to (3)

Step 2: Using $\{\Phi_q|\mathrm{q} \in [1,8]\}$ obtained in the previous step, an estimated decrypted image of an encrypted image $\widetilde{\mathrm{X}}^l$can be obtained.

$$\ddot{\mathrm{X}}^l = \sum_{q=1}^{8}\left(\Phi_q \oplus \widetilde{\mathrm{X}}_q^l\right) \times 2^{(q-1)}$$

According to the correlation coefficient of $\ddot{\mathrm{X}}^l$, estimate and update $\{\varphi_q(1,1)|q \in [1,8]\}$ in order to get the Φ_q.

In fact, the substance of the formula (2) and (3) is the same, all of which are used to count the same proportion of pixel values between (i,j) and ⟨(i,j)⟩, where $\langle(i,j)\rangle$ represents the adjacent pixels in the horizontal and vertical directions, Consequently, formula (2) and (3) can be simplified as follows:

$$p(i,j) = \frac{1}{L}\sum_{l=1}^{L}(1 - |(i,j) - \langle(i,j)\rangle|) \tag{6}$$

For smooth areas, the inter-pixel redundancy is larger than that in the texture areas. Correspondingly, the probability of the same pixels in adjacent pixels is bigger in smooth areas.

In COA, it regards the smoothness probability of all pixels in each original image corresponding to the encrypted images as the same. Therefore, for the texture images, or the texture areas, the

error probability of estimating stream cipher key is bigger than that in smoothness. Furthermore, once a bit in a stream cipher key estimated incorrectly, it would make others wrong in this stream cipher key.

In this work, we propose an estimation method based on the smoothness of pixels called PSE (Pixel Smoothness Estimation) in the corresponding original image of the encrypted image. Its aim is to estimate the stream cipher key more accurately with fewer encrypted images.

3. Proposed COA Based on PSE

In this section, we propose a new COA based on PSE. For the encrypted images set $\tilde{X}$, we firstly estimate the pixel smoothness of each encrypted image corresponding to the original image. Then design the weighted COA determined adaptively based on PSE. We can get a better effect, which use fewer encrypted images based on the same accuracy of the stream cipher key estimation, compared the proposed with the original COA.

3.1 Theoretical Basis of PSE

It's important to note that on account of the fact that the object processed is each bit plane of the encrypted image in COA independently, the following section of PSE analyzed is also based on the binary image.

Let a binary image B with size of m×n pixels, all pixels in the binary image B are firstly classified into smooth pixels and non-smooth ones. We use a binary matrix $S^{\{B\}} = \{s^{\{B\}}(i,j)|i = 1,2,\dots,m, j = 1,2,\dots,n\}$, called it as the smoothness-mark of B, to represent the type of corresponding pixel in the original image. In other words, if $s^{\{B\}}(i,j)$=0, the corresponding pixel b(i,j) in the binary image B is smooth pixel; otherwise, the pixel b(i,j) is non-smooth one.

Definition 1: For each non-boundary pixel b(i,j) in an binary image B, if the sum of all pixels in the 3×3 neighborhood centered on this pixels b(i,j) is 0 or 9, we consider the pixel b(i,j) as smooth; otherwise it is considered as non-smooth. That is,

$$s^{\{B\}}(i,j) = \begin{cases} 0, & if \ \sum[\![(b(i,j))]\!]_8 = 0 \ or \ 9 \\ 1, & otherwise \end{cases} \quad (7)$$

Where, $[\![.]\!]_8$ represent a 3×3 neighborhood centered on the pixel b(i,j) in the original image. $\sum[\![(b(i,j))]\!]_8 = 0 \ or \ 9$ means that all pixel in the 3×3 neighborhood centered on the pixel b(i,j) are either 0 or 1. The smoothness of binary image B can be measured by the ratio of 0 in the corresponding type-mark matrix.

$$\zeta^B = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(1 - s^{\{B\}}(i,j)\right) \quad (8)$$

According to the formula (12), ζ^B falling into [0,1]. The larger the value is, the smoother the binary image B is.

Definition 2: When B^p and B^q are two binary images with the same size, the common smoothness-mark (CSM) can be represented as $S^{\{B^p \cap B^q\}} = \{s^{\{B^p \cap B^q\}}(i,j)\}$ and obtained by

$$s^{\{B^p \cap B^q\}}(i,j) = \begin{cases} 0, \text{if } s^{\{B^p\}}(i,j) = s^{\{B^p\}}(i,j) \\ 1, \text{otherwise} \end{cases} \quad (9)$$

The **Definition 1** and **Definition 2** show the smoothness of binary image B and the CSM respectively. However, for the COA attackers, what they can get is just some encrypted images encrypted by the common stream cipher key XOR. The focus of this section is to get the PSE of the encrypted images corresponding to the original images by using the images that attackers have gotten. For the sake of this discussion, we firstly estimate the CSM of the original images on the basis of the 2 known encrypted images.

Proposition 1: Let B^p and B^q are two binary images with the same size, the encrypted images generated using the same stream cipher key are denoted as $\tilde{B}^p$ and $\tilde{B}^q$. The CSM of two encrypted images $\tilde{B}^p$ and $\tilde{B}^q$, denoted as $S^{\{\tilde{B}^p \cap \tilde{B}^q\}} = \{s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j)\}$, can be computed by,

$$s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = \begin{cases} 0, & if \ [\![(\tilde{b}^p(i,j))]\!]_8 = [\![(\tilde{b}^q(i,j))]\!]_8 \\ 0, & if \ [\![(\tilde{b}^p(i,j))]\!]_8 = -[\![(\tilde{b}^q(i,j))]\!]_8 \\ 1, & otherwise \end{cases} \quad (10)$$

In the following, we proof that the $S^{\{\tilde{B}^p \cap \tilde{B}^q\}}$is approximately equal to the $S^{\{B^p \cap B^q\}}$ in terms of the SM of corresponding to original image B^p and B^q.

Proof: according to the smoothness of $s^{\{B^p\}}(i,j)$ and $s^{\{B^q\}}(i,j)$, there are three cases:

Case 1: $s^{\{B^p\}}(i,j)$=$s^{\{B^q\}}(i,j) = 0$

One hand, $s^{\{B^p \cap B^q\}}(i,j) = 0$ according to Definition 2;

On the other hand, after using the same stream cipher key to encrypt images, there will be $[\![(\tilde{b}^p(i,j))]\!]_8 = \pm[\![(\tilde{b}^q(i,j))]\!]_8$. That is, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = 0$. As a result, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = s^{\{B^p \cap B^q\}}(i,j)$ in the conditional of Case 1;

Case2: $s^{\{B^p\}}(i,j) = 0, s^{\{B^q\}}(i,j) = 1$

One hand, $s^{\{B^p \cap B^q\}}(i,j) = 1$ according to Definition 2;

On the other hand, after using the same stream cipher key to encrypt images, there will be$[\![(\tilde{b}^p(i,j))]\!]_8 \neq \pm[\![(\tilde{b}^q(i,j))]\!]_8$. That is, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = 1$. As a result, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = s^{\{B^p \cap B^q\}}(i,j)$ in the conditional of Case 2;

Case3: $s^{\{B^p\}}(i,j)$=$s^{\{B^q\}}(i,j) = 1$

One hand, $s^{\{B^p \cap B^q\}}(i,j) = 1$ according to Definition 2

On the other hand, after using the same stream cipher key to encrypt images, there will be 2 different cases showed as follows.

(1)$[\![(b^p(i,j))]\!]_8 \neq \pm[\![(b^q(i,j))]\!]_8$.That is, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = 1$

(2)$[\![(b^p(i,j))]\!]_8 = \pm[\![(b^q(i,j))]\!]_8$.That is, $s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j) = 0$

In all these three cases, only in the condition of 3.2, $s^{\{B^p \cap B^q\}}(i,j) \neq s^{\{\tilde{B}^p \cap \tilde{B}^q\}}(i,j)$

Then discuss the special case in the condition of (2) in case 3 in detail. Assume two binary images B^p and B^q are independent, then the probability that the condition (3.2) is true is:

$$\frac{(2^9-2)\times 2}{(2^9-2)\times(2^9-2)} = \frac{2}{510} = 0.39\% \quad (11)$$

That is to say, about 0.39% of pixels in $\left(S^{\{B^p B^q\}}\right)$and $\tilde{S}^{\{\tilde{B}^p \cap \tilde{B}^q\}}$ are different. So, $\tilde{S}^{\{\tilde{B}^p \cap \tilde{B}^q\}} \approx \left(S^{\{B^p B^q\}}\right)$.

According to Proposition 1, using $\tilde{B}^p$ and $\tilde{B}^q$ to estimate the mutual type-mark of corresponding original images, about 0.39% of pixels are judged wrongly as non-smooth pixels.

Given the encrypted image set $\{\tilde{B}^l | l = 1,2,\dots,L\}$ which contains L images, it can be used to estimate the mutual type-mark $s^{\{\tilde{B}^p \cap \tilde{B}^l\}}(l \neq p)$ in order to approximate the type-mark $S^{\{B^p\}} = \left\{s^{\{B^p\}}(i,j) | i = 1,2,\dots,m, j = 1,2,\dots,n\right\}$

$$s^{\{B^p\}}(i,j) \approx \left(\sum_{l=1}^{L} s^{\{\tilde{B}^p \cap \tilde{B}^l\}}(i,j)\right) \geq (L - Th), (l \neq p) \quad (12)$$

3.2 Proposed Weighted COA

Similar to the COA, extracting the q[th] bit plane significant level of all images from the encrypted images set $\{\tilde{X}^l | l = 1,2,\dots,L\}$ step by step. Every q[th] bit plane significance level constitutes an encrypted binary image set $\{\tilde{X}_q^l | l = 1,2,\dots,L\}$. In this work, we can gain the estimated stream cipher key of the q[th] bit plane significance level by performing the algorithm as follows.

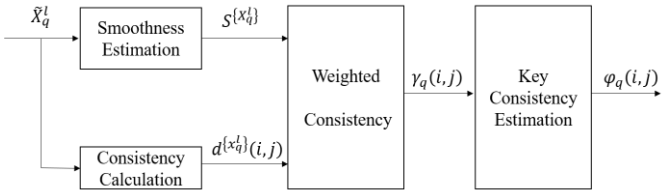

Figure 1*: *Weighted ciphertext-only attack

Step1: Smoothness Estimation Find each smooth binary matrix $S^{\{X_q^l\}}=\{s^{\{x_q^l\}}(i,j)\}$ of corresponding pixels in the original image according to the formula (16) from the encrypted images set $\{\tilde{X}_q^l | l = 1,2,\dots,L\}$;

Step2: Consistency calculation Estimate the consistency $d^{\{x_q^l\}}(i,j)$ between the pixel and the pre-pixel in each encrypted image $\tilde{X}_q^l$.

$$d^{\{x_q^l\}}(i,j) = \begin{cases} 1, if \left|\tilde{x}_q^l(i,j) - \langle \tilde{x}_q^l(i,j)\rangle\right| = 0 \\ -1, otherwise \end{cases} \quad (13)$$

Step3: Weighted consistency Hypothesis the weight $\alpha \in [0.5,1]$, then we can get the weighted consistency as follows:

$$\mu_q^l(i,j) = \begin{cases} \alpha, if\ s^{\{x_q^l\}}(i,j) = 0 \\ 1-\alpha, otherwise \end{cases} \quad (14)$$

Step 4: Key consistency estimation Hypothesis the given weight $\alpha \in [0.5,1]$, then the horizontal and vertical estimations of the stream cipher key are obtained.

$$\varphi_q(i,j) = \begin{cases} \langle \varphi_q(i,j)\rangle, \ if\ \gamma_q(i,j) > 0 \\ 1 - \langle \varphi_q(i,j)\rangle, \ otherwise \end{cases} \quad (15)$$

4. Experimental result

The proposed algorithm is implemented in Matlab. The six gray-scale images of size 512×512×8 bits with different textured images were selected as test images, as shown in Figure 2. In the following experiments, the correctness of the proposed PSM method is verified by experiments, then the performance of Khelifi's COA [10] and proposed one are compared.

Figure 2*: *Test images

4.1 Accuracy of proposed PSE method

According to the same secret key, the 6 original images shown in Figure 2 were encrypted by the bitwise XOR operation to obtain the encrypted image-set $\widetilde{X} = \{\widetilde{X}^l | l=1,2,..,6\}$. For each encrypted image, the 8 bit-plane $\left\{\tilde{X}_q^l(i,j) | q = 1,2,\dots,8\right\}$ are computed according to formula (1). The q[th] CMS can be computed by formula (10) in the Proposition 2 using the q[th] bit-plane of each two encrypted images. Taking the encrypted Man image $\widetilde{X}^6$, shown as in Figure 2(e), as an example, Figure 3 and Figure 4 are the 8th and 7th CMSs, respectively, where white is non-smooth pixels and black is smooth pixels. In Figure 3 and 4, (a)~(e) are the CMSs of the corresponding bit plane of Man and the other five images, which are in order Lena, Baboon, Crowd, Photographer and Village. Figure 3(f) and Figure 4(f) are the sum of the corresponding the five 8th CMSs and the five 7th CMSs, respectively. Each pixel in

Figure 3(f) and Figure 4(f) is a non-negative integer not greater than 5 since the CMS is binary image.

As can be seen from (a)~(e) in Figure 3 and Figure 4, the white part outlines the edge of the original image well and the black area happens to be the common smoothness area of the two images. The comparison shows that the white area in Figure 4 is much more than that in Figure 3, mainly due to the different smoothness of the different bit planes significance level of the image. The larger the q is, the smoother pixels are in the corresponding bit planes significance level. The smoothness of Man's 8th and 7th bit plane is 0.79 and 0.64.

All 5 CMS cumulated is Figure4(f), where the brightest areas show the edge information in the Figure4. Consequently, the brightest part is nearly maximized the value 5, which implies the fact that the pixels are non-smoothness in the Man image. Next, we can estimate the smoothness-mark of the Man image according to the threshold.

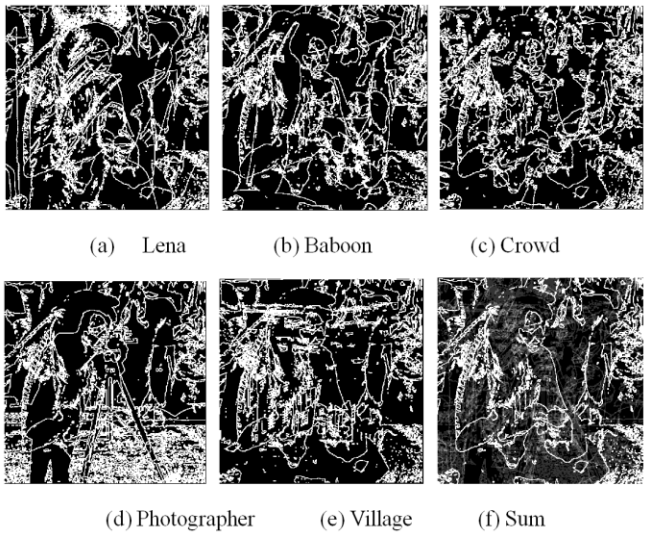

Figure 3*: *The 8th CMS of Man image and their sum

With the threshold fixed 4, the values of the pixels greater than 4 can be seen as 1 in (f) of the Figure3 and Figure4 otherwise as 0. Next, we can get the ESM of the Man image. Figure5(b) are the thresholding ESM of the most significant bit plane (MSB) and the second MSB, respectively. We can easily find it that both of them are largely consistent compared Figure5(a) with Figure5(b). Figure5(c) is the difference between Figure5(a) and Figure5(b), in which the white spots are the error estimation. The error rate of Figure5(a) and Figure5(b) is 0.0032 and 0.0109 respectively. The result shows the fact that PSE is effective.

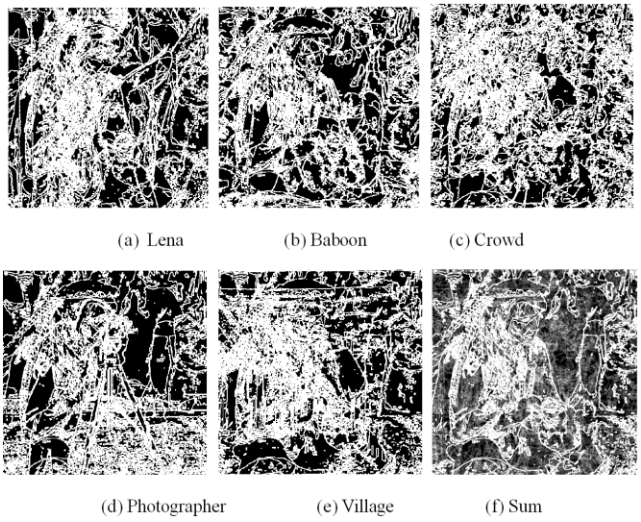

Figure 4: The 7th CMS of Man image and their sum

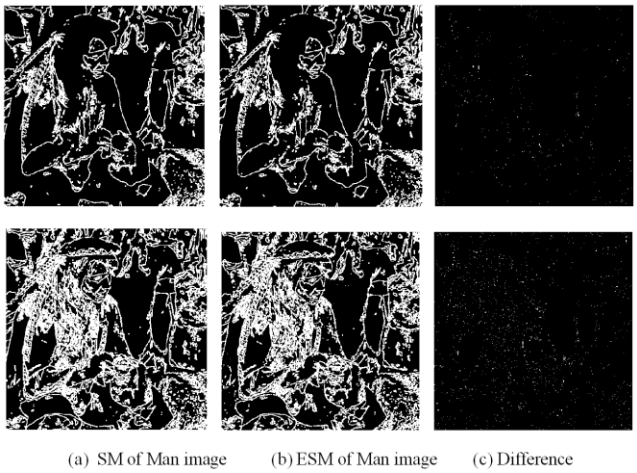

Figure 5: Estimation errors of different bit-planes (Above is the 8th bit-plane and below is the 7th bit-plane)

4.2 Accuracy of Stream Cipher Estimation

We used the encrypted images to get the CSM of each image's 8 bit planes according to the method from 3.1. Then, get the estimation stream cipher key on the basis of the algorithm proposed in our work. To visually show whether the key stream estimation result is correct, the decrypted image is obtained by using PSE, as shown in Figure6. Figure6(a) is the decrypted image estimated by the proposed method, Figure6(b) is the decrypted one estimated by COA. The first line in Figure6 is the decrypted image according to 6 encrypted images and the second line is the image according to 10 encrypted images. It can be seen that, the more encrypted images are, the higher the accuracy is. Given 6 encrypted images, the error rate of the proposed method is 0.54%, and the COA method is

9.02%. The error rate of COA method is 14 times as many as that of the proposed method. Therefore, proposed COA is efficient.

In order to further compare the performance of the two methods, the stream cipher is estimated separately when L is 6, 10, 15, and 20. Table 2 gives the rate of PSE in the condition of different number of encrypted images. With the number of 20, the error rates of the most and the second most significant bit planes PSE is 0, the third-MSB of which is only 0.61%. It is clear from the above experiment result, and the proposed method reduces the attack cost.

(a) Proposed (b) [10]

Figure 6: Decrypted image obtained from stream cipher key estimation by the MSB

Table 2: the error rates of PSE in the condition of different numbers of encrypted images (%)

q	algorithm	Number L/Th			
		6/4	10/7	15/12	20/16
8	[10]	9.02	1.75	0	0
	Proposed	0.54	0	0	0
7	[10]	46.54	18.16	0.38	0.13
	Proposed	47.31	2.32	0	0
6	[10]	49.12	44.56	19.73	15.94
	Proposed	50.03	28.06	3.4	0.61
5	[10]	50.06	49.71	45.43	45.17
	Proposed	50.03	45.70	38.61	35.44

5. Conclusion and Future Work

This work proposed a new COA based on pixel smoothness estimation. Firstly, define the smooth pixel and the common smoothness-mark (CSM), then propose a method to estimate the CSM corresponding to the original images, which used 2 binary images encrypted by XOR according to the same stream cipher key. Furthermore, we can get the CSM of the encrypted images corresponding to the original images according to the threshold value. Meanwhile, discuss the relationship between the smoothness of the images and pixel smoothness estimation. Theoretical analysis and computation show that the demands on the number of the known encrypted images will decrease with the proposed weighted COA under the condition of the same performance. Besides, theoretical proof and experimental verification of the proposed pixel smoothness estimation algorithm are given. Experiments have validated the effectiveness and feasibility of the proposed scheme, the superiority compared with the original COA. In the future, it will be studied that how to use the discrete optimization to improve the performance of the COA base on PSE.

ACKNOWLEDGMENTS

This work is supported by National Natural Science Foundation of China (NSFC) Under grants (61872303,61461047), Student Research Training Program (201810613040) and Technology Innovation Talent Program of Science & Technology Department of Sichuan Province(2018RZ0143).

REFERENCES

[1] L.Yuan and T.Ebrahimi(2018). Image privacy protection with secure JPEG transmorphing[J]. Iet Signal Processing, 11(9),1031-1038.

[2] X. Zhang(2011). Reversible data hiding in encrypted image. IEEE Signal Process. Lett., vol. 18, no. 4, pp, 255-258.

[3] Y.Shi, X.Li and X.Zhang(2016). Reversible data hiding: Advances in the past two decades. IEEE Access, vol. 4, pp, 3210–3237.

[4] F. Huang, J. Huang and Y. Shi(2016). New framework for reversible data hiding in encrypted domain. IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp, 2777-2789.

[5] J.Zhou, W.Sun, L.Dong and X.Liu. (2016). Secure reversible image data hiding over encrypted domain via key modulation. IEEE Transactions on Circuits & Systems for Video Technology, vol. 26, no. 3, pp, 441–452.

[6] C.Qin, Z.He, X.Luo and J.Dong(2018). Reversible data hiding in encrypted image with separable capability and high embedding capacity. Information Sciences, vol. 465, pp, 285–304.

[7] Z.Qian and X.Zhang(2016). Reversible data hiding in encrypted images with distributed source encoding, IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4, pp, 636–646.

[8] P.Puteaux and W.Puech(2018). An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images[J]. IEEE Transactions on Information Forensics and Security.

[9] Y.Chen, B.Yin, H.He, S.Yan and F.Chen(2018). Reversible data hiding in classification- scrambling encrypted-image based on iterative recovery. Computers, Materials and Continua, vol. 56, no. 2, pp. 299–312.

[10] Fouad.Khelifi (2018). On the security of a stream cipher in reversible data hiding schemes operating in the encrypted domain[J]. Signal Processing.