

NOTICE: This is the author's version of a work that was accepted to *Communications in Nonlinear Science and Numerical Simulations* in 2010. Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes may have been made to this work since it was submitted for publication. A definitive version has been published in *Communications in Nonlinear Science and Numerical Simulations*, vol. 16, no. 2, pp. 837-843, 2011, Elsevier. DOI: 10.1016/j.cnsns.2010.05.008.

Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps

Chengqing Li^{a,*}, Shujun Li^{b,*}, Kwok-Tung Lo^a

^a*Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China*

^b*Fachbereich Informatik und Informationswissenschaft, Universität Konstanz, Fach M697, Universitätsstraße 10, 78457 Konstanz, Germany*

Abstract

Recently, an image encryption scheme based on chaotic standard and logistic maps was proposed by Patidar et al. It was later reported by Rhouma et al. that an equivalent secret key can be reconstructed with only one known/chosen-plaintext and the corresponding ciphertext. Patidar et al. soon modified the original scheme and claimed that the modified scheme is secure against Rhouma et al.'s attack. In this paper, we point out that the modified scheme is still insecure against the same known/chosen-plaintext attack. In addition, some other security defects existing in both the original and the modified schemes are also reported.

Keywords: cryptanalysis, known-plaintext attack, chosen-plaintext attack, encryption, image, chaos

1. Introduction

With the rapid development of information technology, multimedia data are transmitted over all kinds of wired/wireless networks more and more frequently. Consequently, security of multimedia data becomes a serious concern in many applications. However, traditional text encryption schemes cannot be used in a naive way to protect multimedia data efficiently in some applications, mainly due to some special requirements of the whole multimedia system. This challenge stirs the design of special multimedia encryption schemes to become a hot research topic in the past two decades. Because of the subtle similarity between chaos and cryptography, a great number of multimedia

*Corresponding authors.

Email address: zjulcq@gmail.com (Chengqing Li)

URL: www.hooklee.com (Shujun Li)

encryption schemes based on chaos have been presented [1–4]. Unfortunately, many of them have been found to have security problems from the cryptographical point of view [5–9]. Some general rules about evaluating security of chaos-based encryption schemes can be found in [10, 11].

Since 2003, Pareek et al. have proposed a number of different encryption schemes based on one or more chaotic maps [12–15]. Recent cryptanalytic results [16–18] have shown that all the three schemes proposed in [12–14] have security defects. In [15], a new image encryption scheme based on the logistic and standard maps was proposed, where the two maps are used to generate a pseudo-random number sequence (PRNS) controlling two kinds of encryption operations. In [19], Rhouma et al. reported that the scheme is not secure in the sense that an equivalent key can be obtained from only one known/chosen plain-image and the corresponding cipher-image. To resist Rhouma et al.’s attack, a modified version of the original scheme was proposed in [20]. The present paper reports the following findings: 1) the modified image encryption scheme can still be broken by the same known/chosen-plaintext attack under the same condition; 2) there are some other security defects existing in both the modified and the original schemes.

The rest of this paper is organized as follows. Section 2 briefly introduces the image encryption schemes under study and the known/chosen-plaintext attack reported in [19]. Our cryptanalytic results are presented in Sec. 3 in detail. The last section concludes the paper.

2. The image encryption schemes under study and Rhouma et al.’s attack

For both schemes, we make the following assumptions to ease our description¹. The plaintext is a RGB true-color image of size $H \times W$ (height \times width), which can be denoted by an $H \times W$ matrix of 3-tuple pixel values $\mathbf{I} = \{I(i, j)\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}} = \{(R(i, j), G(i, j), B(i, j))\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$. Similarly, the ciphertext corresponding to \mathbf{I} is denoted by $\mathbf{I}' = \{I'(i, j)\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}} = \{(R'(i, j), G'(i, j), B'(i, j))\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$. To further facilitate our discussion, we adopt the terms in [20]: the original image encryption scheme is called PPS09 and the modified one mPPS09.

2.1. The original image encryption scheme PPS09 [15]

- *Secret key*: three floating-point numbers x_0, y_0, K , and one integer N , where $x_0, y_0 \in (0, 2\pi)$, $K > 18$, $100 < N < 1100$.
- *Initialization*: prepare data for encryption/decryption by performing the following steps.
 - Generate four XORing keys as follows: $Xkey(1) = \lfloor 256x_0/(2\pi) \rfloor$, $Xkey(2) = \lfloor 256y_0/(2\pi) \rfloor$, $Xkey(3) = \lfloor K \bmod 256 \rfloor$, $Xkey(4) = (N \bmod 256)$. Then, generate a pseudo-image $\mathbf{I}_{Xkey} = \{(R_{Xkey}(i, j), G_{Xkey}(i, j), B_{Xkey}(i, j))\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$ by filling an $H \times W$ matrix with the four XORing keys repeatedly: $R_{Xkey}(i, j) = Xkey((3k \bmod 4) + 1)$, $G_{Xkey}(i, j) = Xkey(((3k + 1) \bmod 4) + 1)$, $B_{Xkey}(i, j) = Xkey(((3k + 2) \bmod 4) + 1)$, where $k = iW + j$.
 - Iterate the standard map Eq. (1) from the initial conditions (x_0, y_0) for N times to obtain a new chaotic state (x'_0, y'_0) . Then, further iterate it for HW more times to get HW chaotic states $\{(x_i, y_i)\}_{i=1}^{HW}$.

¹To make the presentation more concise and more consistent, some notations in the original papers [15, 20] are also modified.

$$\begin{cases} x = (x + K \sin(y)) \bmod (2\pi), \\ y = (y + x + K \sin(y)) \bmod (2\pi), \end{cases} \quad (1)$$

- Iterate the logistic map Eq. (2) from the initial condition $z_0 = ((x'_0 + y'_0) \bmod 1)$ for N times to get a new initial condition z'_0 . Then, further iterate it for HW times to get HW chaotic states $\{z_i\}_{i=1}^{HW}$.

$$z = 4z(1 - z). \quad (2)$$

- Generate a pseudo-image $\mathbf{I}_{CKS} = \{(R_{CKS}(i, j), G_{CKS}(i, j), B_{CKS}(i, j))\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$ by filling its R, G and B channels with the three chaotic key streams (CKS) $\{x_k\}_{k=1}^{HW}$, $\{y_k\}_{k=1}^{HW}$ and $\{z_k\}_{k=1}^{HW}$: $R_{CKS}(i, j) = \lfloor 256x_k/(2\pi) \rfloor$, $G_{CKS}(i, j) = \lfloor 256y_k/(2\pi) \rfloor$, $B_{CKS}(i, j) = \lfloor 256z_k \rfloor$, where $k = iW + j + 1$.

- *Encryption procedure*: a simple concatenation of the following four encryption operations.

- *Confusion I*: Mask the plain-image \mathbf{I} by \mathbf{I}_{Xkey} to obtain \mathbf{I}^* , i.e., $\mathbf{I}^* = \mathbf{I} \oplus \mathbf{I}_{Xkey}$.
- *Horizontal Diffusion (HD)*: Scan $\mathbf{I}^* = \{I^*(i, j)\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$ rowwise from the upper-left pixel to the bottom-right one, and mask each pixel value (except for the first one) by its predecessor in the scan. Denoting the output of this step by $\mathbf{I}^* = \{I^*(i, j)\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$, the HD procedure is described as follows: 1) $I^*(0, 0) = I^*(0, 0)$; 2) for $k = 1, \dots, HW - 1$,

$$I^*(i, j) = I^*(i, j) \oplus I^*(i', j'), \quad (3)$$

where $i = \lfloor k/W \rfloor$, $j = (k \bmod W)$, $i' = \lfloor (k-1)/W \rfloor$, $j' = ((k-1) \bmod W)$.

- *Vertical Diffusion (VD)*: Scan \mathbf{I}^* columnwise from the bottom-right pixel to the upper-left one, and mask each pixel value (except for the first one) by its predecessor in the scan. Denoting the output of this step by $\mathbf{I}^{**} = \{R^{**}(i, j), G^{**}(i, j), B^{**}(i, j)\}_{\substack{0 \leq i \leq H-1 \\ 0 \leq j \leq W-1}}$, the VD procedure can be described as follows: 1) $I^{**}(H-1, W-1) = I^*(H-1, W-1)$; 2) for $k = HW - 2, \dots, 0$,

$$I^{**}(i, j) = I^*(i, j) \oplus \overline{I^{**}(i', j')}, \quad (4)$$

where $i = (k \bmod H)$, $j = \lfloor k/H \rfloor$, $i' = ((k+1) \bmod H)$, $j' = \lfloor (k+1)/H \rfloor$, and

$$\overline{I^{**}(i', j')} = (G^{**}(i', j') \oplus B^{**}(i', j'), R^{**}(i', j') \oplus B^{**}(i', j'), R^{**}(i', j') \oplus G^{**}(i', j')).$$

- *Confusion II*: Mask the pixel values in \mathbf{I}^{**} with \mathbf{I}_{CKS} to get the ciphertext \mathbf{I}' , i.e., $\mathbf{I}' = \mathbf{I}^{**} \oplus \mathbf{I}_{CKS}$.

- *Decryption procedure*: the simple reversion of the above encryption procedure.

2.2. Rhouma et al.'s attack [19]

Denoting the horizontal and vertical diffusion processes by HD and VD, respectively, the encryption procedure of PPS09 can be represented as follows:

$$\mathbf{I}' = \text{VD}(\text{HD}(\mathbf{I} \oplus \mathbf{I}_{Xkey})) \oplus \mathbf{I}_{CKS}. \quad (5)$$

In [19], Rhouma et al. showed that the HD and VD processes are commutative with XOR operations:

$$\begin{aligned} \text{HD}(\mathbf{X} \oplus \mathbf{Y}) &= \text{HD}(\mathbf{X}) \oplus \text{HD}(\mathbf{Y}), \\ \text{VD}(\mathbf{X} \oplus \mathbf{Y}) &= \text{VD}(\mathbf{X}) \oplus \text{VD}(\mathbf{Y}). \end{aligned}$$

Therefore, Eq. (5) is equivalent to the following one:

$$\mathbf{I}' = \text{VD}(\text{HD}(\mathbf{I})) \oplus \text{VD}(\text{HD}(\mathbf{I}_{Xkey})) \oplus \mathbf{I}_{CKS}. \quad (6)$$

Assuming $\mathbf{I}_{key} = \text{VD}(\text{HD}(\mathbf{I}_{Xkey})) \oplus \mathbf{I}_{CKS}$, we can observe the following two important facts:

1. neither HD nor VD depends on the key;
2. \mathbf{I}_{key} does not depend on the plaintext \mathbf{I} or the ciphertext \mathbf{I}' .

The above facts immediately lead to a conclusion: \mathbf{I}_{key} can be used as an equivalent key to encrypt any plaintext of the same size $H \times W$ and decrypt any ciphertext of size $H \times W$. A known/chosen-plaintext attack can be easily mounted to derive \mathbf{I}_{key} from a known/chosen plaintext \mathbf{I} and its corresponding ciphertext \mathbf{I}' :

$$\mathbf{I}_{key} = \text{VD}(\text{HD}(\mathbf{I})) \oplus \mathbf{I}'. \quad (7)$$

2.3. The modified image encryption scheme mPPS09 [20]

To enhance the security of PPS09 against Rhouma et al.'s attack, in [20] Patidar et al. proposed a modified edition of PPS09 by making both HD and VD dependent on the secret key.

The modified key-dependent HD and VD processes are denoted by mHD and mVD in [20]. Both mHD and mVD are based on 16 diffusion keys derived from the secret key (x_0, y_0, K, N) :

- for $i = 1, \dots, 5$, $Dkey(i) = \sum_{j=0}^2 a_{3 \cdot (i-1) + j} \cdot 10^{2-j} \bmod 256$, where $x_0 = a_1.a_2 \dots a_{15} \dots$ and a_i are decimal digits representing x_0 ;
- for $i = 6, \dots, 10$, $Dkey(i) = \sum_{j=0}^2 b_{3 \cdot (i-6) + j} \cdot 10^{2-j} \bmod 256$, where $y_0 = b_1.b_2 \dots b_{15} \dots$ and b_i are decimal digits representing y_0 ;
- for $i = 11, \dots, 15$, $Dkey(i) = \sum_{j=0}^2 c_{3 \cdot (i-11) + j} \cdot 10^{2-j} \bmod 256$, where $K = \dots c_1.c_2 \dots c_{15} \dots$ and c_i are decimal digits representing K ;
- $Dkey(16) = (N \bmod 256)$.

The mHD process is modified from HD by replacing Eq. (3) with the following equation:

$$I^*(i, j) = I^*(i, j) \oplus I^*(i', j') \oplus Dkey^*(k-1), \quad (8)$$

where

$$Dkey^*(k) = (Dkey((k \bmod 16) + 1), Dkey((k \bmod 16) + 1), Dkey((k \bmod 16) + 1)).$$

The mVD process is modified from VD by replacing Eq. (4) with the following equation:

$$I^{**}(i, j) = I^*(i, j) \oplus \overline{I^{**}(i', j')} \oplus Dkey^{**}(k'), \quad (9)$$

where $k' = HW - 2 - k$ and

$$Dkey^{**}(k') = (Dkey(3k' \bmod 16) + 1), Dkey(((3k' + 1) \bmod 16) + 1), Dkey(((3k' + 2) \bmod 16) + 1)).$$

3. Cryptanalysis

In this section, we first show that the key-dependent horizontal and vertical diffusion steps mHD and mVD do not increase the security of mPPS09 against Rhouma et al.'s attack. Then we point out some common security weaknesses in both PPS09 and mPPS09.

3.1. Insecurity of mPPS09 against Rhouma et al.'s attack

Although both mHD and mVD are dependent on the secret key, we noticed that they can be represented in an equivalent form which renders the key-dependence useless. Assuming \mathbf{X} is the input matrix and Θ is a zero matrix of the same size as \mathbf{X} , we have the following two lemmas.

Lemma 1. $mHD(\mathbf{X}) = HD(\mathbf{X}) \oplus mHD(\Theta)$.

Proof. This lemma can be easily proved with mathematical induction on k .

For $k = 0$, i.e., $i = j = 0$, we have $mHD(X(0, 0)) = X(0, 0)$ and $HD(X(0, 0)) \oplus mHD(\Theta(0, 0)) = X(0, 0) \oplus (0, 0, 0) = X(0, 0)$. This lemma holds. Then, assume the lemma is true for $k \geq 0$, let us prove the case of $k + 1$.

For $k + 1$, i.e., $i = \lfloor (k + 1)/W \rfloor$, $j = ((k + 1) \bmod W)$, $i' = \lfloor k/W \rfloor$ and $j' = (k \bmod W)$, $mHD(X(i, j)) = X(i, j) \oplus mHD(X(i', j')) \oplus Dkey^*(k)$. According to the assumption on k , we have $mHD(X(i', j')) = HD(X(i', j')) \oplus mHD(\Theta(i', j'))$. Thus, $mHD(X(i, j)) = X(i, j) \oplus HD(X(i', j')) \oplus mHD(\Theta(i', j')) \oplus Dkey^*(k)$. Noting that $HD(X(i, j)) = X(i, j) \oplus HD(X(i', j'))$, we get $mHD(X(i, j)) = HD(X(i, j)) \oplus mHD(\Theta(i', j')) \oplus Dkey^*(k)$. Further note that $mHD(\Theta(i, j)) = \Theta(i, j) \oplus mHD(\Theta(i', j')) \oplus Dkey^*(k) = mHD(\Theta(i', j')) \oplus Dkey^*(k)$. This immediately leads to $mHD(X(i, j)) = HD(X(i, j)) \oplus mHD(\Theta(i, j))$. \square

Lemma 2. $mVD(\mathbf{X}) = VD(\mathbf{X}) \oplus mVD(\Theta)$.

Proof. This lemma can be proved in a similar way to Lemma 1, but the mathematical induction should be made in descending order on k (starting from $k = HW - 1$ and ending at $k = 0$). \square

The above two lemmas lead to the following proposition.

Proposition 1. *The encryption procedure of mPPS09 is equivalent to the following equation:*

$$\mathbf{I}' = VD(HD(\mathbf{I})) \oplus \tilde{\mathbf{I}}_{key}, \quad (10)$$

where $\tilde{\mathbf{I}}_{key} = VD(HD(\mathbf{I}_{Xkey})) \oplus VD(mHD(\Theta)) \oplus mVD(\Theta) \oplus \mathbf{I}_{CKS}$.

Proof. From the properties of HD & VD and Lemmas 1 & 2, we can make the following deduction:

$$\begin{aligned}
\mathbf{I}' &= \text{mVD}(\text{mHD}(\mathbf{I} \oplus \mathbf{I}_{X_{key}})) \oplus \mathbf{I}_{CKS}, \\
&= \text{mVD}(\text{HD}(\mathbf{I} \oplus \mathbf{I}_{X_{key}}) \oplus \text{mHD}(\Theta)) \oplus \mathbf{I}_{CKS}, \\
&= \text{VD}(\text{HD}(\mathbf{I} \oplus \mathbf{I}_{X_{key}}) \oplus \text{mHD}(\Theta)) \oplus \text{mVD}(\Theta) \oplus \mathbf{I}_{CKS}, \\
&= \text{VD}(\text{HD}(\mathbf{I} \oplus \mathbf{I}_{X_{key}})) \oplus \text{VD}(\text{mHD}(\Theta)) \oplus \text{mVD}(\Theta) \oplus \mathbf{I}_{CKS}, \\
&= \text{VD}(\text{HD}(\mathbf{I})) \oplus \text{VD}(\text{HD}(\mathbf{I}_{X_{key}})) \oplus \text{VD}(\text{mHD}(\Theta)) \oplus \text{mVD}(\Theta) \oplus \mathbf{I}_{CKS}, \\
&= \text{VD}(\text{HD}(\mathbf{I})) \oplus \tilde{\mathbf{I}}_{key}.
\end{aligned}$$

This proves the proposition. \square

Since $\text{mHD}(\Theta)$ and $\text{mVD}(\Theta)$ are both independent of the plaintext and the ciphertext, they are uniquely determined by the key (x_0, y_0, K, N) . This means that $\tilde{\mathbf{I}}_{key}$ is also uniquely determined by the key (x_0, y_0, K, N) . Therefore, $\tilde{\mathbf{I}}_{key}$ can be used as an equivalent key of mPPS09 exactly in the same way as \mathbf{I}_{key} in PPS09. In fact, even the determination process of the equivalent key is also the same:

$$\tilde{\mathbf{I}}_{key} = \text{VD}(\text{HD}(\mathbf{I})) \oplus \mathbf{I}'.$$

This means that the same known/chosen-plaintext attack can be applied to mPPS09 without any change to the program. In other words, the security of mPPS09 against Rhouma et al.'s attack remains the same as that of the original scheme PPS09.

We have performed some experiments to verify the correctness of the conclusion. With the secret key $(x_0, y_0, K, N) = (3.98235562892545, 1.34536356538912, 108.54365761256745, 110)$, the equivalent key $\tilde{\mathbf{I}}_{key}$ was constructed from a known plain-image ‘‘Lenna’’ and the corresponding cipher-image, which are shown in Figs. 1a) and b), respectively. Then, $\tilde{\mathbf{I}}_{key}$ was used to recover a cipher-image shown in Fig. 1c, and the plain-image ‘‘Peppers’’ (Fig. 1d) was successfully recovered.

3.2. Other security weaknesses of PPS09 and mPPS09

3.2.1. Insufficient randomness of the PRNS $\{B_{CKS}(i, j)\}$

As illustrated in [21], the randomness of pseudo-random bit sequences derived from chaotic orbits of the logistic map is very weak. To further verify the randomness of the PRNS $\{B_{CKS}(i, j)\}$ generated via the logistic map with control parameter 4.0, we tested 100 PRNSs of length $512 \times 512 = 262144$ (the number of bytes used for encryption of a 512×512 plain color image) by using the NIST statistical test suite [22]. The 100 sequences were generated with randomly selected secret keys, and transformed to 1-D bit sequences by concatenating the bits of all the elements. For each test, the default significance level 0.01 was used. The results are shown in Table 1, from which one can see that the PRNS $\{B_{CKS}(i, j)\}$ is not random enough.

3.2.2. Insufficient sensitivity with respect to change of plaintext

In [15, 20], Patidar et al. recognized that the sensitivity of cipher-image with respect to change of plain-image is very important. However, both PPS09 and mPPS09 are actually very far from the desired property. As well known in cryptography, this property is termed as avalanche effect. Ideally, it requires the change of any single bit of plain-image will make every bit of cipher-image change with a probability of one half.

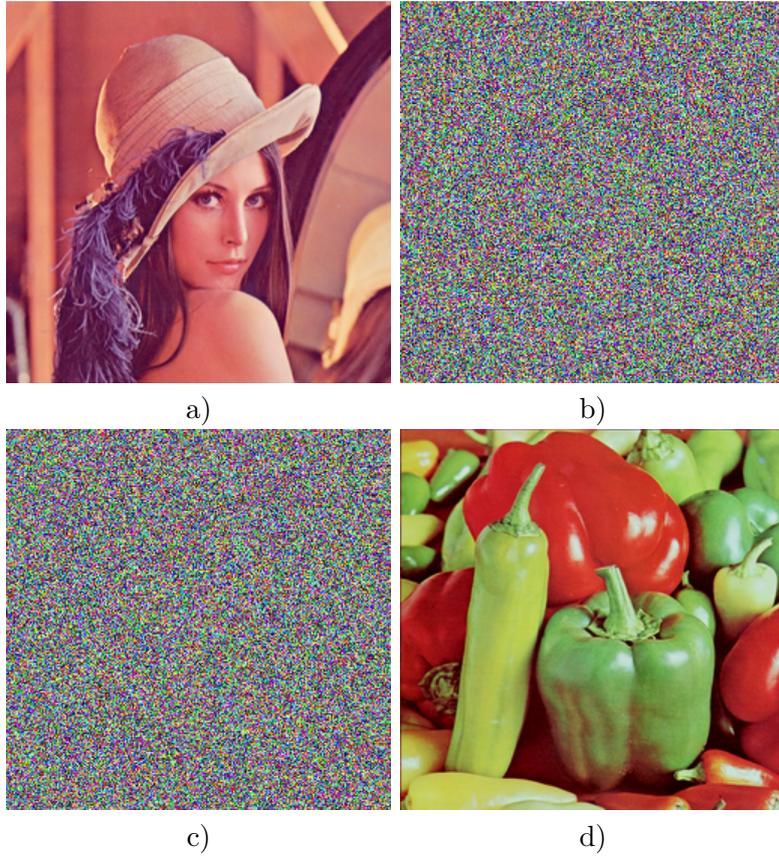


Figure 1: An experimental result of the proposed known-plaintext attack: a) the known plain-image “Lenna”; b) the corresponding cipher-image; c) a cipher-image encrypted with the same key; d) the recovered plain-image “Peppers”.

Table 1: The performed tests with respect to a significance level 0.01 and the number of sequences passing each test in 100 randomly generated sequences.

Name of Test	Number of Passed Sequences
Frequency	95
Block Frequency ($m = 100$)	0
Cumulative Sums-Forward	93
Runs	0
Rank	0
Non-overlapping Template ($m = 9, B = 010000111$)	10
Serial ($m = 16$)	0
Approximate Entropy ($m = 10$)	0
FFT	0

For both PPS09 and mPPS09, the following equation holds for two plain-images \mathbf{I} and $\mathbf{J} =$

$\mathbf{I} \oplus \mathbf{I}_\Delta$:

$$\begin{aligned} \mathbf{I}' \oplus \mathbf{J}' &= (\text{VD}(\text{HD}(\mathbf{I}))) \oplus (\text{VD}(\text{HD}(\mathbf{J}))), \\ &= \text{VD}(\text{HD}(\mathbf{I} \oplus \mathbf{J})), \\ &= \text{VD}(\text{HD}(\mathbf{I}_\Delta)). \end{aligned}$$

The above equation implies the following two facts:

- any change in a single bitplane will not change any other bitplanes in the cipher-image;
- a change in plain-image \mathbf{I}_Δ will cause a change pattern determined by $\text{VD}(\text{HD}(\mathbf{I}_\Delta))$, which is far from a random pattern.

To show this defect clearly, we made an experiment by changing only one bit of the red channel of a plain-image. It is found that only some bits on the same bitplane in the corresponding cipher-image were changed. The locations of the changed bits can be seen from the differential cipher-image $\text{VD}(\text{HD}(\mathbf{I}_\Delta))$ and its three color channels as shown in Fig. 2. Apparently, the change pattern is far from random and balanced.

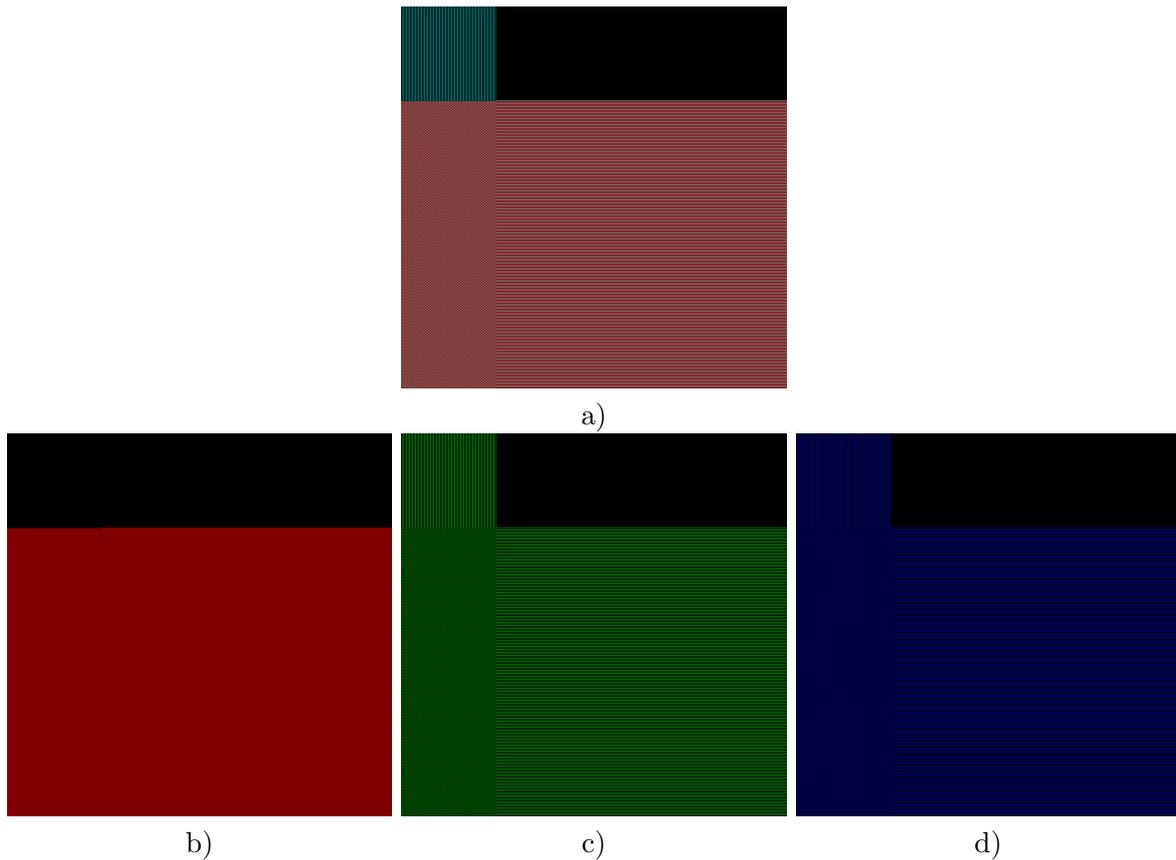


Figure 2: The differential cipher-image and its three color channels, when the MSB (i.e., the 8-th bit) of $R(127, 127)$ in a plain-image was changed: a) the differential cipher-image; b) red channel; c) green channel; d) blue channel.

4. Conclusion

In this paper, the security of the image encryption scheme proposed in [20] (a modified version of the one proposed in [15]) is re-evaluated. It is found that the scheme is still insecure against a known/chosen-plaintext attack which can break the original scheme in [19]. In addition, two more security weaknesses of both the original and the modified image encryption schemes are reported: insufficient randomness of a PRNS involved, and insufficient sensitivity with respect to change of plain-image. Due to such a low level of security, we recommend not to use the image encryption schemes under study unless their security is further enhanced with more complicated countermeasures.

Acknowledgement

Chengqing Li was supported by The Hong Kong Polytechnic University's Postdoctoral Fellowships Scheme under grant no. G-YX2L. Shujun Li was supported by a fellowship from the Zukunftskolleg of the Universität Konstanz, Germany, which is part of the "Exzellenzinitiative" Program of the DFG (German Research Foundation).

- [1] H.-C. Chen, J.-C. Yen, A new cryptography system and its VLSI realization, *Journal of Systems Architecture* 49 (7-9) (2003) 355–367.
- [2] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos, Solitons & Fractals* 21 (3) (2004) 749–761.
- [3] N. J. Flores-Carmona, M. Carpio-Valadez, Encryption and decryption of images with chaotic map lattices, *Chaos* 16 (3) (2006) art. no. 033118.
- [4] K.-W. Wong, C.-H. Yuen, Embedding compression in chaos-based cryptography, *IEEE Transactions on Circuits and Systems II: Express Brief* 55 (11) (2008) 1193–1197.
- [5] K. Wang, W. Pei, L. Zou, A. Song, Z. He, On the security of 3D cat map based symmetric image encryption scheme, *Physics Letters A* 343 (6) (2005) 432–439.
- [6] C. Li, G. Chen, On the security of a class of image encryption schemes, in: *Proceedings of 2008 IEEE Int. Symposium on Circuits and Systems*, 2008, pp. 3290–3293.
- [7] S. Li, C. Li, G. Chen, K.-T. Lo, Cryptanalysis of the RCES/RSES image encryption scheme, *Journal of Systems and Software* 81 (7) (2008) 1130–1143.
- [8] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, *Chaos* 18 (3) (2008) art. no. 033112.
- [9] C. Li, S. Li, G. Chen, W. A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, *Image and Vision Computing* 27 (8) (2009) 1035–1039.
- [10] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *International Journal of Bifurcation and Chaos* 16 (8) (2006) 2129–2151.
- [11] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), *Multimedia Security Handbook*, CRC Press, 2004, Ch. 4, pp. 133–167.
- [12] N. Pareek, V. Patidar, K. Sud, Discrete chaotic cryptography using external key, *Physics Letters A* 309 (1-2) (2003) 75–82.
- [13] N. Pareek, V. Patidar, K. Sud, Cryptography using multiple one-dimensional chaotic maps, *Communications in Nonlinear Science and Numerical Simulation* 10 (7) (2005) 715–723.
- [14] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, *Image and Vision Computing* 24 (9) (2006) 926–934.
- [15] V. Patidar, N. Pareek, K. Sud, A new substitution-diffusion based image cipher using chaotic standard and logistic maps, *Communications in Nonlinear Science and Numerical Simulation* 14 (7) (2009) 3056–3075.
- [16] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, *Physics Letters A* 319 (3-4) (2003) 334–339.
- [17] C. Li, S. Li, G. Álvarez, G. Chen, K.-T. Lo, Cryptanalysis of a chaotic block cipher with external key and its improved version, *Chaos, Solitons & Fractals* 37 (1) (2008) 299–307.
- [18] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, *Image and Vision Computing* 27 (9) (2009) 1371–1381.

- [19] R. Rhouma, E. Solak, S. Belghith, Cryptanalysis of a new substitution-diffusion based image cipher, *Communications in Nonlinear Science and Numerical Simulation*, in press, doi:10.1016/j.cnsns.2009.07.007 (2009).
- [20] V. Patidar, N. Pareek, K. Sud, Modified substitution-diffusion image cipher using chaotic standard and logistic maps, *Communications in Nonlinear Science and Numerical Simulation*, in press, doi:10.1016/j.cnsns.2009.11.010 (2009).
- [21] C. Li, S. Li, G. Álvarez, G. Chen, K.-T. Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations, *Physics Letters A* 369 (1-2) (2007) 23–30.
- [22] A. Rukhin, et al., A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22, available online at <http://csrc.nist.gov/rng/rng2.html> (2001).