Breaking a novel colour image encryption algorithm based on chaos

Chengqing Li · Leo Yu Zhang · Rong Ou · Kwok-Wo Wong · Shi Shu

Received: 20 April 2012 / Accepted: 21 September 2012 / Published online: 11 October 2012 © Springer Science+Business Media Dordrecht 2012

Abstract Recently, a colour image encryption algorithm based on chaos was proposed by cascading two position permutation operations and one substitution operation, which are all determined by some pseudo-random number sequences generated by iterating the logistic map. This paper evaluates the security level of this encryption algorithm and finds that the position permutation-only part and the substitution part can be separately broken with only \(\lceil \log_2(3MN) / 8 \rceil\) and 2 chosen plain-images, respectively, where \(MN\) is the size of the plain-image. The effectiveness of the proposed chosen-plaintext attack is supported by concise theoretical analyses, and is verified by experimental results.

Keywords Image encryption · Chaos · Cryptanalysis · Chosen-plaintext attack

1 Introduction

The security of multimedia data (audio/speech, image, video) has become more and more important as these data are transmitted over all kinds of wired/wireless networks more and more frequently. Both the design and the security analysis of multimedia encryption algorithms have attracted much research attention in the past decade [2, 8, 14, 17, 22]. In particular, chaos is considered as an effective means in the design of secure and efficient encryption algorithms [5, 6, 18, 20]. This is because the dynamical properties of chaos, such as sensitivity to the initial condition and control parameters exhibit certain similarities with the basic confusion and diffusion properties of cryptography. As digital image is a typical form of multimedia data and it can show the performance of a proposed encryption algorithm effectively, most chaos-based encryption algorithms adopt images as the encryption object.

According to the record of Web of Science, more than four hundred papers on the design of chaos-based image encryption schemes were published between 1997 and 2011. Meanwhile, no more than one hundred and fifty papers on the security analysis of chaos-based image encryption schemes can be found. Short of scrutiny on the security analysis makes many chaos-based image cryptosystems insecure against conventional attacks such as known/chosen-plaintext attack.
and chosen-ciphertext attack [3, 9, 10, 16, 21]. Some representative chaos-based encryption algorithms and a general framework evaluating the security of this class of encryption algorithms were analyzed in [1]. In many chaos-based image encryption algorithms, a chaotic system, composed of one or more chaotic maps, is used to generate a pseudo-random number sequence (PRNS) to determine and control the combination of some basic encryption functions [11, 15]. In the discrete domain, finite precision computation and quantization lead to the degeneration of certain dynamical properties of the chaotic system in some form. This may eventually cause a potential threat to the security of the chaos-based encryption algorithms [4].

The present paper analyzes the security of the image encryption algorithms proposed in [19]. It is found that the three basic encryption operations of the algorithm are all key-invertible, i.e. the unknown information controlling an encryption operation can be derived directly from the input and the output. Furthermore, the three encryption functions are performed independently, and so the position permutation part and the substitution part of the encryption algorithm under study can be broken separately with a few chosen plain-images. Both theoretical analyses and experimental results are presented to show the effectiveness of the chosen-plaintext attack.

The rest of this paper is organized as follows. The next section briefly introduces the image encryption algorithm under study. Section 3 presents an efficient chosen-plaintext attack on the encryption algorithm, followed by some simulation results. The last section concludes our work.

2 The colour image encryption algorithm under study

The plain-image of the encryption algorithm under study is a RGB colour image of size $M \times N$ (height $\times$ width), which can be represented as a $M \times N \times 3$ matrix of pixel values $I = \{I(i, j, k)\}_{i=0, j=0, k=0}^{M-1, N-1}$, $\{R(i, j), G(i, j), B(i, j)\}_{i=0, j=0}^{M-1, N-1}$. Similarly, the corresponding cipher-image is denoted by $I' = \{I'(i, j, k)\}_{i=0, j=0, k=0}^{M-1, N-1, 2} = \{(R'(i, j), G'(i, j), B'(i, j))\}_{i=0, j=0}^{M-1, N-1}$. Then the colour image encryption algorithm under study can be described as follows.\(^1\)

- The secret key is composed of two positive integers $m_1, m_2$, and two sets of initial condition and control parameter of the logistic map
  \[f(x) = \mu \cdot x \cdot (1 - x),\]
  \[(x_0, \mu_0), (x_0^*, \mu_0^*), \text{ where } x_0, x_0^* \in (0, 1) \text{, and } \mu_0, \mu_0^* \in (3.5699456, 4).\]

- The initialization process:
  1. Iterate the logistic map (1) $m_1$ times from the initial condition $x_0$ to obtain a new initial condition under a fixed control parameter $\mu_0$. Then further iterate it $3M$ times to get a sequence of chaotic states $\{X_i\}_{i=0}^{3M-1}$. Finally, a permutation sequence $\{T^*_i\}_{i=0}^{3M-1}$ is derived by comparing $\{X_i\}_{i=0}^{3M-1}$ and its sorted version, where $X$ is the $r$th largest element in the sequence $\{X_i\}_{i=0}^{3M-1}$.
  2. Iterate the logistic map (1) $m_2$ times from the initial condition $x_0^*$ to obtain a new initial condition under a fixed control parameter $\mu_0^*$. Then further iterate it $3MN$ times to get a sequence of chaotic states $\{X^{*}_{i}\}_{i=0}^{3MN-1}$. For $i = 0 \sim M - 1$, obtain another permutation sequence $\{T^*_{i}\}_{i=0}^{3N-1}$ by comparing $\{X^{*}_{3iN+t}\}_{i=0}^{3N-1}$ and its sorted version, where $X^{*}_{3iN+t}$ is the $r$th largest element in the sequence $\{X^{*}_{3iN+t}\}_{i=0}^{3N-1}$.
  3. Generate a PRNS $\{Y_i\}_{i=0}^{3MN-1}$ from the sequence $\{X_{i}\}_{i=0}^{3MN-1}$ using $Y_i = \lfloor X_i \cdot 10^{14} \rfloor \bmod 3$, where $(a \mod b) = a - b \cdot \lfloor a/b \rfloor$ and $b \neq 0$.
  4. To make the numbers of the three different elements in $\{Y_i\}_{i=0}^{3MN-1}$ all equal to $MN$, update the last $3MN - 1$ elements as follows: for $l = 1 \sim 3MN - 1$, set

\[
Y_l = \begin{cases}
1, & \text{if } Y_l = 0, n_0 \geq MN \text{ and } n_1 < MN, \\
2, & \text{if } Y_l = 0, n_0 \geq MN \text{ and } n_1 \geq MN, \\
2, & \text{if } Y_l = 1, n_1 \geq MN \text{ and } n_2 < MN, \\
0, & \text{if } Y_l = 1, n_1 \geq MN \text{ and } n_2 \geq MN, \\
0, & \text{if } Y_l = 2, n_2 \geq MN \text{ and } n_0 < MN, \\
1, & \text{if } Y_l = 2, n_2 \geq MN \text{ and } n_0 \geq MN,
\end{cases}
\]

\(^1\)To make the presentation more concise and complete, some notations in the original paper [19] are modified under the condition that the essential form of the encryption algorithm remains unchanged.
where \( n_0, n_1, n_2 \) represent the number of 0, 1, 2 in \( \{Y_l\}_{l=0}^{i-1} \), respectively.

(5) Generate another PRNS \( \{Z_l\}_{l=0}^{3MN-1} \) from the sequence \( \{X_l\}_{l=0}^{3MN-1} \) by
\[
Z_l = [X_l \cdot 10^{15}] \mod 256.
\]

The encryption procedures are a simple concatenation of the following three encryption operations.

1. **Row permutation**: for \( i = 0 \sim M - 1, \ j = 0 \sim N - 1, \ k = 0 \sim 2, \) set
\[
I^*(i, j, k) = I(i^*, j, k^*),
\]
where \( i^* = T_{kM+i} \mod M, \ k^* = [T_{kM+i}/M] \).

2. **Column permutation**: for \( i = 0 \sim M - 1, \ j = 0 \sim N - 1, \ k = 0 \sim 2, \) set
\[
I^{**}(i, j, k) = I^*(i, j^{**}, k^{**}),
\]
where
\[
j^{**} = T_{i,kN+j} \mod N, \ k^{**} = [T_{i,kN+j}/N].
\]

3. **Substitution**: First, let
\[
I'(0, 0, Y_0) = (I^{**}(0, 0, Y_0) + Z_0) \mod 256.
\]

Then one pixel is selected iteratively from the other un-encrypted pixels of the intermediate image \( I^{**} = \{I^{**}(i, j, k)\}_{i=0}^{M-1, j=0}^{N-1, k=0}^{2} \) according to a PRNS \( \{Y_l\}_{l=1}^{3MN-1} \), determining which channel’s pixel is chosen. The chosen pixels are encrypted by the previous selected pixel, the corresponding cipher-pixel, and a pseudo-random number by
\[
I'(i, j, k) = (I^**(i, j, k) + I^{**}(i', j', k')) + I'(i', j', k') \mod 256
\]
for \( l = 1 \sim 3MN - 1, \) where
\[
i = [n_k/N], \ j = n_k \mod N, \ k = Y_l, \ i' = [n_{k'}/N], \ j' = n_{k'} \mod N, \ k' = Y_{l-1}.
\]
\( n_k \) and \( n_{k'} \) represent the number of \( k \) and \( k' \) in \( \{Y_l\}_{l=0}^{i-1} \) and \( \{Y_l\}_{l=0}^{i-2} \), respectively.

The decryption procedures are similar to the encryption one except the following points: (1) the above-mentioned encryption operations are performed in a reverse order; (2) the permutation sequences are replaced by their invertible versions; (3) Eqs. (2) and (3) are replaced by
\[
I^{**}(0, 0, Y_0) = (I'(0, 0, Y_0) - Z_0) \mod 256
\]
and
\[
I^{**}(i, j, k) = (I'(i, j, k) - I^{**}(i', j', k')) - I'(i', j', k') \mod 256,
\]
respectively.

### 3 Chosen-plaintext attack

In [19, Sect. 3.2.6], it is claimed that the image encryption algorithm under study is robust against chosen-plaintext attack based on the following two points: (a) all the PRNSs employed are sensitive to a change in the secret key; (b) the substitution function (3) possesses a feedback mechanism. However, we will show that their claim is incorrect. As the image encryption algorithm under study is composed of three independent encryption operations, the position permutation part and the substitution part can be compromised separately using the Divide and Conquer strategy.

For a plain-image formed by identical pixels, both the Row permutation and the Column permutation have no effect and only the Substitution can have a change on the image. Assume two chosen plain-images having fixed pixel values \( I_1 = \{I_1(i, j, k) = d_1\}, I_2 = \{I_2(i, j, k) = d_2\} \) are available. From Eq. (2), one has
\[
I_1'(0, 0, Y_0) = (I_1(0, 0, Y_0) + Z_0) \mod 256
\]
and
\[
I_2'(0, 0, Y_0) = (I_2(0, 0, Y_0) + Z_0) \mod 256.
\]
Subtract Eq. (5) from Eq. (4), one obtains
\[
(I_1'(0, 0, Y_0) - I_2'(0, 0, Y_0)) \in \{D, D - 256, D + 256\},
\]
where \( D = d_1 - d_2 \). Referring to Eq. (3), one gets
\[
I_1'(i, j, k) = (I_1(i, j, k) + I_1(i', j', k')) + I_1'(i', j', k') \mod 256,
\]
\[
I_2'(i, j, k) = (I_2(i, j, k) + I_2(i', j', k')) + I_2'(i', j', k') \mod 256
\]
for \( l = 1 \sim 3MN - 1 \), where \((i, j, k)\) and \((i', j', k')\) are determined by \( \{Y_l\}_{l=0}^{l=1} \) and \( \{Y_l\}_{l=0}^{l=1} \), respectively, as mentioned in the above section. Subtract Eq. (8) from Eq. (7), one has

\[
(I'_1 - I'_2)(i, j, k) = (2D + (I'_1 - I'_2)(i', j', k')) \pmod {256}
\]

where \( (I'_1 - I'_2)(i, j, k) = I'_1(i, j, k) - I'_2(i, j, k) \), and \( (I'_1 - I'_2)(i', j', k') = I'_1(i', j', k') - I'_2(i', j', k') \), the same hereinafter.

Then a property of \( (I'_1 - I'_2) \) can be presented as follows.

**Property 1** The difference between the cipher-images \( I_1 \) and \( I_2 \) satisfies

\[
(I'_1 - I'_2)(i, j, Y_l) = ((2l + 1)D) \pmod {256}
\]

for \( l = 0 \sim 3MN - 1 \), where \((i, j) = (0, 0)\) when \( l = 0 \), \((i, j) = ((nY_l/N), nY_l \mod N)\) otherwise, and \( nY_l \) denotes the number of the elements in \( \{Y_l\}_{l=0}^{l=1} \) whose values are equal to \( Y_l \).

**Proof** This property can be proved via mathematical induction on \( l \). When \( l = 0 \), one can get

\[
(I'_1 - I'_2)(0, 0, Y_0) \equiv D \pmod {256}
\]

from Eq. (6), which means Eq. (10) holds for \( l = 0 \). Assume Eq. (10) holds for \( l = l^n \), i.e.,

\[
(I'_1 - I'_2)(i, j, Y_{l^n}) \equiv ((2l^n + 1)D) \pmod {256}
\]

where \( l^n < 3MN - 1 \). Then let us study the case for \( l = (l^n + 1) \). From Eq. (9), one has

\[
(I'_1 - I'_2)(i, j, Y_{l^n+1}) = (2D + (I'_1 - I'_2)(i, j, Y_{l^n})) \pmod {256} = ((2(l^n + 1) + 1)D) \pmod {256}.
\]

This completes the mathematical induction and also the proof of this property. \( \square \)

Making use of Property 1, one can derive an estimate of \( Y_0 \),

\[
\bar{Y}_0 = \begin{cases} 
0 & \text{if } (I'_1 - I'_2)(0, 0, 0) \equiv D \pmod {256}, \\
1 & \text{if } (I'_1 - I'_2)(0, 0, 1) \equiv D \pmod {256}, \\
2 & \text{if } (I'_1 - I'_2)(0, 0, 2) \equiv D \pmod {256}, 
\end{cases}
\]

when \( D \neq 128 \). Obviously, one can assure \( \bar{Y}_0 = Y_0 \) definitely when

\[
\#(\{k | (I'_1 - I'_2)(0, 0, k) \equiv D \pmod {256}\}) = 1.
\]

where \( \#(\cdot) \) denotes the cardinality of a set. Once the value of \( Y_0 \) is determined, the estimates of \( \{Y_l\}_{l=0}^{l=1} \), \( \{\hat{Y}_l\}_{l=0}^{l=1} \), can be obtained in order using a similar method, i.e., set

\[
\hat{Y}_l = k \quad \text{if } (I'_1 - I'_2)(i_k, j_k, k) \equiv ((2l + 1)D) \pmod {256}
\]

for \( l = 1 \sim 3MN - 1 \), where \( i_k = [(n_k + 1)/N], j_k = (n_k + 1) \mod N, \) and \( n_k \) represents the number of \( k \) in \( \{\hat{Y}_l\}_{l=0}^{l=1} \).

Referring to [7, Sect. 5.4], one can find out the period of the sequence \(((2l + 1)D) \pmod {256} \}_{l=0}^{l=1} \),

\[
T = \frac{256}{\gcd(D, 256)} = \frac{128}{\gcd(D, 256)}.
\]

To help estimate the success probability of this attack, we make use of the following property of \( (I'_1 - I'_2) \).

**Property 2** Inequality

\[
\#(\{k | (I'_1 - I'_2)(i_k, j_k, k) \equiv ((2l + 1)D) \pmod {256}\}) > 1
\]

holds if and only if

\[
Y_{l+S} \notin \{Y_l\}_{l=0}^{l=1} \quad (14)
\]

for any \( S \equiv 0 \pmod T \), where \((i_k, j_k) = (0, 0)\) when \( l = 0 \), \((i_k, j_k) = ((n_k/N), n_k \mod N)\) otherwise, and \( n_k \) denotes the number of \( k \) in \( \{Y_l\}_{l=0}^{l=1} \).

**Proof** Let \( \{Y_l\}_{l=0}^{l=1} \), \( \{Y_l\}_{l=1}^{l=1} \) and \( \{Y_l\}_{l=2}^{l=1} \) denote the corresponding segments of \( \{Y_l\}_{l=0}^{l=1} \) determining \( i'(i_0, j_0, 0), i'(i_1, j_1, 1) \) and \( i'(i_2, j_2, 2) \) via Eq. (3), respectively, where \( (I'_1 - I'_2)(i_k, j_k, k) = ((2l + 1)D) \pmod {256} \) for \( k = 0, 1, 2 \). If condition (14) holds, one can assure that at least one element in set

\[
\{l_1 - l_0 \pmod T, l_2 - l_0 \pmod T, l_2 - l_1 \pmod T\}
\]

is equal to zero, which means that inequality (13) exists. Therefore, the “if” part of the property is proved. If condition (14) does not hold, there is an integer \( S = s \cdot T \) satisfying condition (14), where \( (l+s \cdot T) < 3MN \). In this case, one can obtain

\[
0 \notin \{|l_1 - l_0 \pmod T, l_2 - l_0 \pmod T, l_2 - l_1 \pmod T\}.
\]
which means
\[
\#\{\{k \mid (I'_k - I''_k)(i_k, j_k, k) \}\} = 1.
\]

As a result, the “only if” part of the property is also proved.

Assume that \( Y_t \) uniformly distributes over \( \{0, 1, 2\} \) for \( l = 0 \sim 3MN - 1 \), one can calculate the probability that condition (14) in Property 2 holds for a given \( l \) and \( T \),
\[
Prob[ Y_{t+l} \not\in \{Y_{t+l-1}^{3MN-1}\} ] = \left( \frac{2}{3} \right)^S \cdot \frac{1}{3} = \left( \frac{2}{3} \right)^S,
\]
where \( (S \mod T) = 0 \). Then an upper bound of the probability that condition (14) holds can be derived as
\[
Prob(MN) = \sum_{k=1}^{\lfloor MN/T \rfloor} (3MN - kT) \left( \frac{2}{3} \right)^{kT}.
\]
When \( T = 128 \), one can calculate \( Prob(2272 \cdot 1704) \approx 3.352 \times 10^{-16} \) for a relatively large plain-image of size 2272 \( \times \) 1704. As for plain-images of a smaller size, one can assure that the success probability of this attack is much greater than \( (1 - 3.352 \times 10^{-16}) \) since the following points hold at the same time.

- The upper bound probability \( Prob(MN) \) is a strictly increasing function with respect to \( MN \);
- Even Eq. (14) holds, \( \tilde{Y}_t = Y_t \) would still occur with probability \( \frac{1}{3} \) or \( \frac{1}{3} \);
- The value of \( Prob(MN) \) is calculated by adding the probabilities of occurrence of some cases that may happen simultaneously and its real value should be smaller.

Based on the above analyses, one can conclude that breaking the Substitution part can be implemented successfully with an extremely high probability.

Once the equivalent secret key governing the Substitution process is recovered, the image encryption algorithm under study becomes a position permutation-only gray-scale image encryption algorithm composing of Row permutation and Column permutation. Considering the number of possible positions of each plain-pixel as \( 3MN \), the bit length of each element of the chosen plain-image should be \( \lceil \log_2(3MN) \rceil \) to assure that the permuted elements are different from each other. As the pixel length of each plain-image channel is fixed to 8 bits, only \( \lceil \log_2(3MN) \rceil / 8 \) pairs of chosen plain-images are required to recover an equivalent version of \( \{T_{l,t}^{3MN-1}\} \) and \( \{T_{l,t}^S\} \). Referring to the quantitative cryptanalysis of permutation-only encryption algorithms in [12, 13], the complexity of breaking the position permutation part is only \( O(3MN) \).

To validate the effectiveness of the proposed attack, a large number of experiments on some plain-images of size 512 \( \times \) 512 were made using randomly selected secret keys. When \( \mu_0 = 4.0 \), \( x_0 = 0.123456789764 \), \( m_1 = 1000 \), \( \mu_0^s = 3.999999 \), \( x_0^s = 0.567891234567 \), and \( m_2 = 2000 \), two chosen plain-images of fixed pixel values 127 and 0, shown in Fig. 1(a) and (b), respectively, are used to recover the PRNS \( \{Y_t\}^{3MN-1} \). Then \( \lceil (\log_2(3 \times 2^9 \cdot 2^9))/8 \rceil = 3 \) pairs of chosen plain-image are constructed to recover the equivalent secret of the position permutation-only part. Finally, the equivalent versions of the sub-keys controlling the two main encryption operations are jointly used to break a cipher-image encrypted by the same secret key, which is shown in Fig. 1(c). The output of our cryptanalysis is depicted in Fig. 1(d), which is identical to the original plain-image. Thus, the effectiveness of the proposed attack is verified.

4 Conclusion

The security of a novel colour image encryption algorithm based on chaos [19] has been analyzed. It is found that this encryption algorithm can be efficiently cryptanalysed by chosen-plaintext attack. The number of required chosen plain-images is proportional to the logarithm value of the image size while the attack complexity is proportional to the image size itself. As a conclusion, the image encryption algorithm under study is not recommended in applications requiring a high level of security.

Acknowledgements This research was supported by the National Natural Science Foundation of China (Nos. 61100216, 61202398), Scientific Research Fund of Hunan Provincial Education Department (Nos. 11B124, 2011FJ0211), and Start-up Fund of Xiangtan University (No. 10QDZ40).
Fig. 1 Chosen-plaintext attack: (a) the chosen plain-image of fixed pixel value 127; (b) the chosen plain-image of fixed pixel value 0; (c) the cipher-image of plain-image “Peppers”; (d) the recovered plain-image from the image shown in (c)

References

1. Álvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos Appl. Sci. Eng. 16(8), 2129–2151 (2006)
2. Arroyo, D., Diaz, J., Rodriguez, F.B.: Cryptanalysis of a one round chaos-based substitution permutation network. arXiv:1203.6866 (2012)
3. Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V.: On the security of a new image encryption scheme based on chaotic map lattices. Chaos 18(3), 033112 (2008)
4. Chen, F., Wong, K.W., Liao, X., Xiang, T.: Period distribution of generalized discrete Arnold cat map for $N = pe$. IEEE Trans. Inf. Theory 58(1), 445–452 (2012)
5. Chen, G., Mao, Y., Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 21(3), 749–761 (2004)
6. Chen, J., Zhou, J., Wong, K.W.: A modified chaos-based joint compression and encryption scheme. IEEE Trans. Circuits Syst. II 58(2), 110–114 (2011)
7. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 6th edn. Oxford University Press, Oxford (2008)
8. Jakimoski, G., Subbalakshmi, K.: Cryptanalysis of some multimedia encryption schemes. IEEE Trans. Multimed. 10(3), 330–338 (2008)
9. Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G., Chen, G.: On the security defects of an image encryption scheme. Image Vis. Comput. 27(9), 1371–1381 (2009)
10. Li, C., Li, S., Chen, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a compound chaotic sequence. Image Vis. Comput. 27(8), 1035–1039 (2009)
11. Li, C., Li, S., Zhang, D., Chen, G.: Cryptanalysis of a data security protection scheme for VoIP. IEEE Proc., Vis. Image Signal Process. 153(1), 1–10 (2006)
12. Li, C., Lo, K.T.: Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. 91(4), 949–954 (2011)
13. Li, S., Li, C., Chen, G., Bourbakis, N.G., Lo, K.T.: A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Process. Image Commun. 23(3), 212–223 (2008)
14. Mao, Y., Wu, M.: A joint signal processing and cryptographic approach to multimedia encryption. IEEE Trans. Image Process. 15(7), 2061–2075 (2006)
15. Seyedzadeh, S.M., Mirzakuchaki, S.: A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Process. 92(5), 1202–1215 (2012)
16. Solak, E., Cokal, C., Yildiz, O.T., Biyikoglu, T.: Cryptanalysis of Fridrich’s chaotic image encryption. Int. J. Bifurc. Chaos Appl. Sci. Eng. 20(5), 1405–1413 (2010)
17. Stutz, T., Uhl, A.: A survey of H.264 AVC/SVC encryption. IEEE Trans. Circuits Syst. Video Technol. 22(3), 325–339 (2012)
18. Tong, X., Cui, M.: Image encryption scheme based on 3d baker with dynamical compound chaotic sequence cipher generator. Signal Process. 89(4), 480–491 (2009)
19. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. 92(4), 1101–1108 (2012)
20. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron mode. Nonlinear Dyn. 62(3), 615–621 (2010)
21. Zhang, Y., Li, C., Li, Q., Zhang, D., Shu, S.: Breaking a chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. 69(3), 1091–1096 (2012)
22. Zhou, J., Au, O.C., Wong, P.H.W.: Adaptive chosen-ciphertext attack on secure arithmetic coding. IEEE Trans. Signal Process. 57(5), 1825–1838 (2009)