An image joint compression-encryption algorithm based on adaptive arithmetic coding*

Deng Jia-Xian(邓家先)† and Deng Hai-Tao(邓海涛)

College of Information Science and Technology, Hainan University, Haikou 570228, *China*

(Received 9 January 2013; revised manuscript received 27 February 2013)

Through a series of studies on arithmetic coding and arithmetic encryption, a novel image joint compression-encryption algorithm based on adaptive arithmetic coding is proposed. The contexts produced in the process of image compression are modified by keys in order to achieve image joint compression encryption. Combined with the bit-plane coding technique, the discrete wavelet transform coefficients in different resolutions can be encrypted respectively with different keys, so that the resolution selective encryption is realized to meet different application needs. Zero-tree coding is improved, and adaptive arithmetic coding is introduced. Then, the proposed joint compression-encryption algorithm is simulated. The simulation results show that as long as the parameters are selected appropriately, the compression efficiency of proposed image joint compression-encryption algorithm is basically identical to that of the original image compression algorithm, and the security of the proposed algorithm is better than the joint encryption algorithm based on interval splitting.

Keywords: image compression, joint compression-encryption algorithm, arithmetic encryption, progressive classification encryption

PACS: 42.30.Va, 95.75.Mn, 42.30.Wb **DOI:** 10.1088/1674-1056/22/9/094202

1. Introduction

With the development of information theory and technology, when data compression and encryption need to be realized simultaneously, a new international trend appears, which has developed the encryption algorithm into an image data compression algorithm.[1–3] This kind of method is referred to as joint compression encryption. Some scholars have used a variety of Huffman trees to implement image joint compression encryption.[2] Some researchers have employed arithmetic coding to realize it, i.e., the interval splitting of arithmetic coding is controlled by keys to ensure data safety.[1,4]

Currently, the discussion about arithmetic encryption is mainly dedicated to the issue of only data encryption or the arithmetic compression encryption with all kinds of simple models.[4–7] Their common feature is that the arithmetic coding model is relatively simple. For example, the fixed probability distribution of symbols from a source or a simple first-order Markov source is assumed, so that it is easy to draw meaningful results. Moreover, the simple interval splitting arithmetic encryption technique is vulnerable when the replacement of input data or ciphertext is not finished.[2]

At present, discrete cosine transform (DCT) or discrete wavelet transform (DWT) has been used to remove the redundancy among image data, and then the bit-plane coding technique is used to encode the transformed coefficients.[8–14] Bit-plane coding mainly contains the set tree coding, block coding, or tree block coding. These algorithms have been implemented to achieve good compression efficiency by using the similarity among the sub-band coefficients, or correlation among the neighboring coefficients, and even correlation among the neighboring sub-band coefficients. The decision produced in these encoding algorithms can be sent into an arithmetic coder to further improve the coding efficiency. In the field of data compression, the arithmetic coder mainly includes Q encoders, QM encoders, and MQ encoders. A Markov source is assumed in these arithmetic encoders, so that this kind of arithmetic coding is adaptive. The results in the image compression field show that these encoders can realize data compression efficiently.

At present, researchers in the area of joint compression encryption are those who have been engaged in encryption research.[1–4] The theoretical significance of research results is self-evident. As the joint compression encryption is implemented by interval splitting arithmetic coding, the ciphertext security has the same shortcomings, i.e., it is vulnerable. In addition, the fixed probability division of the arithmetic coding is different from the actual probability distribution of image data, so it is not conducive to the achievement of good compression efficiency.

From the viewpoint of image compression researchers, the arithmetic encoder of joint compression encryption based on interval splitting is different from the arithmetic encoder in practice. Adaptive arithmetic coding has been widely used in image compression, and the results obtained showed that this type of arithmetic coding is more suitable for image data compression. However, the models and algorithms of arithmetic coding in arithmetic encryption are relatively simple,

*Project supported by the Natural Science Foundation of Hainan Province, China (Grant No. 613155).

†Corresponding author. E-mail: jxiandeng@126.com

© 2013 Chinese Physical Society and IOP Publishing Ltd

and arithmetic encryption mainly focuses on theoretical research. There is a gap between theoretical research and practical applications, which is not conducive to the improvement of efficiency of image compression.

Considering the disadvantages (e.g., the arithmetic coding used in joint compression encryption is relatively simple, security is difficult to guarantee, and higher compression efficiency is hard to achieve), a joint compression-encryption algorithm based on adaptive arithmetic coding is proposed, which is able to achieve data compression and arithmetic encryption synchronously, while its compression efficiency is not affected by the encryption algorithm. Meanwhile, resolution selective encryption can be realized, i.e., different keys are used in different resolutions, and users who have different permissions can obtain different qualities of reconstructed images. As an adaptive arithmetic coder is used, the efficiency of arithmetic coding of the proposed algorithm is better than that of interval splitting arithmetic coding as regards security.

2. Principle and safety analysis of adaptive arithmetic encryption

Let $\boldsymbol{D} = [D_0, D_1, \ldots, D_{N-1}]$ be a binary sequence with length N, and D_i $(i = 0, 1, \ldots, N-1)$ is in the set $\{0,1\}$. The D_i which is subjected to an independent and identical distribution is assumed to follow

$$\begin{bmatrix} D_i \\ P_{D_i} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ p & 1-p \end{bmatrix}. \tag{1}$$

Let n be the number of the sequences of values,

$$n = \sum_{i=0}^{N-1} d_i 2^{N-i-1}, \tag{2}$$

where d_i denotes the value of D_i. Then, the joint probability of the n-th sequence is

$$p_n = p^{N-\sum_{i=0}^{N-1} d_i} (1-p)^{\sum_{i=0}^{N-1} d_i}. \tag{3}$$

The cumulative probability of the n-th sequence is

$$P_n = \sum_{i=0}^{n-1} p_i. \tag{4}$$

The basic principle of arithmetic coding is that the probability interval is divided into 2^N sub-intervals, so that each sequence only corresponds to the probability sub-interval, i.e., the n-th sequence can be expressed by the probability interval $[P_n, P_{n+1})$. Then, the binary symbols whose length is $\lfloor -lb(p_n) \rfloor$ bits are output as the result of the arithmetic encoder. It is the same as the basic idea of the arithmetic encryption based on interval splitting.[1,2] An attacker can obtain the corresponding probability p by analyzing the relevant ciphertext, so the password security of interval splitting is not satisfactory. In order to ensure the security of arithmetic password, the input data and output ciphertext can be permutated by keys to increase the disguised encryption output.

From the above, we can know that the main cause for the lack of security is the fixed probability p used in interval splitting arithmetic encryption. If the data requiring encryption are classified, and the relevant probability distribution of each kind of data is different, the corresponding probability intervals of each sequence will be more complicated, and then the ciphertext will be more secret. The basic theorem of the adaptive arithmetic coding is given below.

We suppose that there are M classes of data, and the i-th variable D_i of the sequence belongs to one of the M categories. For convenience, let symbol CX be the variable categories, and the variable D_i can be expressed as $D_i(\mathrm{CX})$, where CX values are $0, 1, \ldots, M-1$. The conditional probability of the j-th variable in the CX-th class can be expressed as

$$\begin{aligned} & p(\mathrm{CX}, D_j(\mathrm{CX})) \\ = \; & p\{(\mathrm{CX}, D_j(\mathrm{CX}))|(\mathrm{CX}, D_{j-1}(\mathrm{CX})), \ldots, \\ & (\mathrm{CX}, D_0(\mathrm{CX}))\}. \end{aligned} \tag{5}$$

Let $n(\mathrm{CX})$ be the number of the CX-th class variables, the joint probability distribution of the CX-th class variable is

$$\begin{aligned} p_{n(\mathrm{CX})} = & \prod_{j=0}^{n(\mathrm{CX})-1} p(\mathrm{CX}, D_j(\mathrm{CX})) \\ = \; & p(\mathrm{CX}, D_0(\mathrm{CX})) p(\mathrm{CX}, D_1(\mathrm{CX})|(\mathrm{CX}, D_0(\mathrm{CX}))) \ldots \\ & p(\mathrm{CX}, D_{n(\mathrm{CX})-1}(\mathrm{CX})|(\mathrm{CX}, D_{n(\mathrm{CX})-1}(\mathrm{CX})) \ldots \\ & (\mathrm{CX}, D_0(\mathrm{CX}))), \end{aligned} \tag{6}$$

which satisfies

$$\sum_{i=0}^{M-1} n(\mathrm{CX}) = N, \tag{7}$$

where $p(\mathrm{CX}, D_0(\mathrm{CX}))$ is the initial variable distribution of CX class. The conditional probability of the adaptive arithmetic coding is very complicated. It is related to not only the value and category of current variable, but also the value of the previous variables.

The correlation among variables of different categories is not considered. For a sequence with length N, its number n is still obtained by expression (2), and the joint probability of the sequence can be expressed as

$$p_n = \prod_{i=0}^{N-1} p(\mathrm{CX}, D_i(\mathrm{CX})) = \prod_{i=0}^{M-1} \prod_{j=0}^{n(\mathrm{CX})-1} p(i, D_j(i)). \tag{8}$$

As $p(\mathrm{CX}, D_j(\mathrm{CX}))$ is no longer so simple as expression (3), the joint probability of the sequence is much more complicated than that of the interval splitting. The cumulative probability of the corresponding sequence can be calculated via adding the sequence joint probability obtained by Eq. (4)–(8), so it is very complex. The probability interval $[P_n, P_{n+1})$

used to describe the sequence is not only related to the values of sequence, but also closely related to the distribution of the sequence context. Thus, the ciphertext produced by adaptive arithmetic coding is more complicated than by the arithmetic coding based on interval splitting in data encryption. Thus, the adaptive arithmetic encryption is relatively safe.

Currently, the MQ or QM arithmetic coder which has been widely used in the field of image compression is adaptive, and the basic principle is the same as that described above. The proposed image joint compression-encryption algorithm is based on the MQ arithmetic coding.

3. Arithmetic encryption based on context modification

As shown in Fig. 1, the arithmetic encoder inputs the context CX and the decision D, where CX is used to classify the input data (the context variable category) and D refers to the decision of the corresponding class. The decision D is binary datum, and CX is the measure of the correlation among the data, so that the correlation among the data of same classes can be described by the conditional probability and the initial distribution of the context.

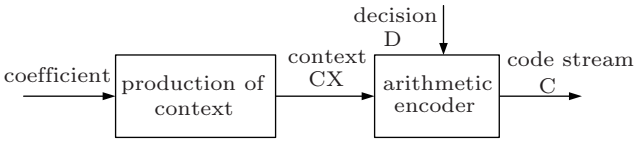


Fig. 1. MQ encoding model.

The number of context CX can be chosen as needed, so the initial distribution $p(\mathrm{CX}, D_0(\mathrm{CX}))$of each class of context must be chosen according to the actual initial probability distribution of the variable of this class.

From the above, we know the cumulative probability of a given sequence is closely related to context, and the output code stream is the description of cumulative probability, so the output code stream from the adaptive arithmetic encoder is related to context. Specifically, for a given sequence, the output code stream from arithmetic encoder is related to the category of context (the value of M mentioned above), and also to the number of every class context and the order of context. Thus, we can draw the conclusion that data encryption can be implemented by using the key to modify the context. The schematic diagram of context modification is shown in Fig. 2, which can be expressed as

$$\mathrm{CX} = \mathrm{CX}_1 \oplus \mathrm{KEY}, \tag{9}$$

where CX_1 is the original context, the term KEY denotes the key, CX represents the modified context, and $\oplus$ denotes the addition operator. The original context is generated by the input data, and it operates with keys to produce CX.

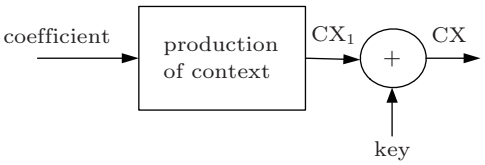


Fig. 2. Schematic diagram of context modification.

If the original contexts produced in the process of encryption and decryption are the same, and if keys used in the process of encryption and decryption are the same too, the context of decryption and the context of encryption will be identical in the system when the same operation is adopted. Conversely, if the key used in the process of decryption is different from the one used in the encryption process, it will lead to the difference between the context used in the process of decryption and the one used in the process of encryption, which will result in a data classification error. Thus, the decryption data will be different from the original data, which leads to a decryption error. Furthermore, once the decryption data error appears, the original context generated by follow-up data may be wrong, and a chain reaction will appear, so consecutive decryption errors will be produced. On the other hand, the cumulative probability used in follow-up data decryption will be wrong, and the same decryption error will also appear. The defined addition operator should make the keys as unique as possible, i.e., the context sequence generated by different keys should be as unique as possible.

4. Image joint compression encryption

The MQ or QM adaptive arithmetic encoders have been widely used in image compression algorithms. The QM arithmetic encoder is used in the extension algorithm of JPEG compression standard. The MQ arithmetic encoder appears in the core algorithm of JPEG2000, and can be used in other algorithms based on bit-plane to compress the image data further. The basic principle of the QM or MQ arithmetic code is the same as the one above.

The image joint compression-encryption algorithm based on context modification is shown in Fig. 3. There is a strong correlation among the original image data. In order to reduce the encoding complexity and achieve better encoding effect, data are analyzed using a transform tool. The correlation among transformed coefficients is weakened (the redundancy among data maps to the statistical redundancy of transformed coefficients), so the encoding model is simplified. Discrete cosine transform (DCT) and discrete wavelet transform (DWT) are widely used as transform tools in the field of image compression.

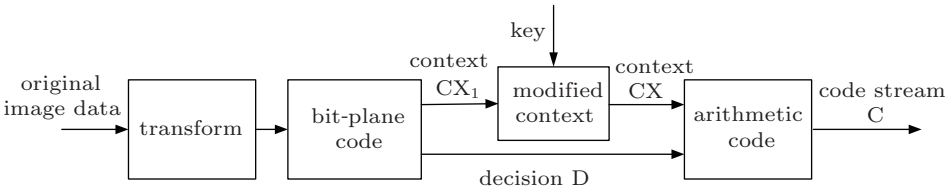


Fig. 3. Diagram of the image joint compression-encryption algorithm.

Binary decision D and the corresponding original context CX_1 are produced by bit-plane coding. In order to achieve the joint compression encryption, the original context CX_1 is modified by keys to obtain context CX, which is fed to arithmetic coder together with decision D to produce the encoding code stream.

The original context is produced by the coefficient significance, the neighbor coefficient significance, the set significance, the coefficient sign, and the neighbor coefficient sign in bit-plane coding. The method of producing the appropriate context can be determined according to users' needs. As an example, the improved zero-tree code is used to introduce the work principle of production of original context and the corresponding context modification.

The DWT coefficients are coded in accordance with the zero-tree code. If the wavelet level is 3, the corresponding zero-tree is shown in Fig. 4. In the improved algorithm, the coefficients of LL band are encoded independently to produce an independent code stream. The coefficients of HL3, LH3, and HH3 bands, and their descendants constitute a corresponding set. The coefficients of a 2-level band and their corresponding descendants also constitute a corresponding set. For example, HL3 band is divided into HL2_1, HL2_2, HL2_3, and HL2_4 sets. The coefficients of a three-level band and their sets are encoded together, and then corresponding code streams are generated separately. By such an analogy, the coefficients of every resolution band are coded independently and corresponding code stream is produced. There are 10 output code streams. This kind of encoding method brings convenience to the implementation of resolution compression and resolution encryption.

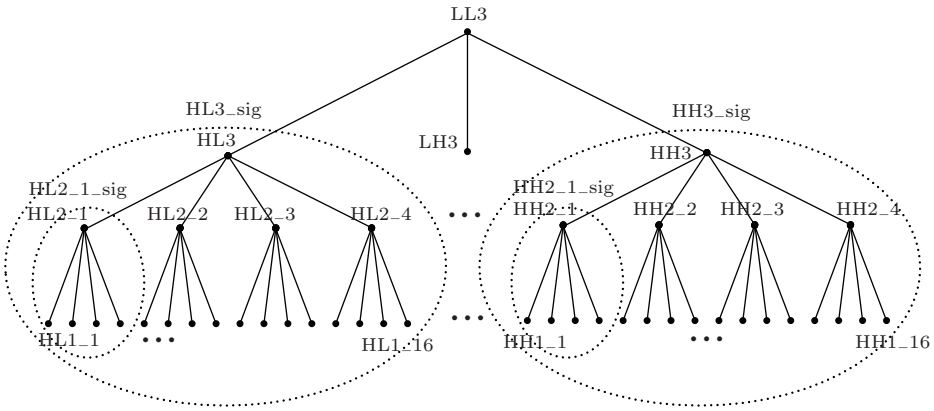


Fig. 4. Structure of zero-tree.

The original context is divided into two types, i.e., set context and coefficient context. The set context can be generated by the neighbor set significance of the same resolution, and can also be extended. The set significance of other resolutions and the set significance of the same resolution form the context together. In this paper, a simple method is adopted, i.e., the context is formed by the neighbor significance in the same resolution. The number "0" indicates that the set is not significant, while "1" indicates that the set is significant. The set context CX_S can be defined as

$$CX_S = (V0|V1|H0|H1) \times 2 + (D0|D1|D2|D3), \qquad (10)$$

where | is the logical OR operator. Obviously, if all the neighbor sets are not significant, $CX_S = 0$. If the horizontal and vertical sets are not significant, but at least one of the diagonal neighbor sets is significant, $CX_S = 1$. If at least one of the horizontal and vertical sets is significant, but all of the diagonal neighbor sets are not significant, $CX_S = 2$. If one of the horizontal and vertical sets is significant, and the same for the diagonal neighbor sets, $CX_S = 3$.

As in embedded block coding with optimized truncation (EBCOT), the coefficient context is divided into the context for zero coding, the context for magnitude refinement and the context for sign coding.[10–14] The method of calculating the context is the same as the one in EBCOT.

The key is shifted cyclically first, and several low bit-planes of the shift data are used to produce data d_k, and then d_k is operated together with original context to produce the

context described as

$$\mathrm{CX} = (d_k + \mathrm{CX}_1) \bmod (L), \tag{11}$$

where mod() is the modulo operation. The selection of L is complicated, and the user is allowed to select it as needed. For example, there are 4 kinds of set contexts described above. If the number of kinds of modified contexts is 5, then $L = 5$. If the required number of kinds of modified contexts is 3, then $L = 3$. Let the number of a kind of original context be L_1, in order to reduce the influence of compression resulting from context modification, we may let $L = L_1$. In principle, L should satisfy the following inequality:

$$L \leq \max(d_k) + L_1. \tag{12}$$

If the above inequality does not hold, the modulo operation itself is not significant. If different keys are used in data encryption of different resolutions, the resolution selective encryption is implemented.

5. Experimental results and analysis

The 'GoldHill' image is used to test the proposed algorithm. Let $L = L_1$ in Eq. (11). When the output rates are 0.5, 0.75, 1.0, 1.25, 1.5, 1.75, and 2.0, the comparison of reconstruction quality between the proposed algorithm and the original algorithm (PSNR) is shown in Table 1. The results show that the image reconstruction qualities are basically the same. When the rate is 1.0, the reconstructed image qualities of different images are shown in Table 2, and the quality of the original algorithm is basically equal to that of our scheme.

These results indicate that when the parameter is selected reasonably, joint compression-encryption algorithm can achieve the same compression efficiency as the original algorithm.

Table 1. Comparison of reconstructed image quality between the original algorithm and the joint compression-encryption algorithm (in units of dB).

Rate	Original compression algorithm	Joint compression encryption
0.5	32.07	32.05
0.75	34.00	34.01
1.0	35.20	35.20
1.25	36.86	36.84
1.5	38.04	38.02
1.75	38.88	38.86
2.0	39.96	39.90

Table 2. Comparison of the reconstructed image quality between the original algorithm and the joint compression-encryption algorithm (in units of dB).

Image	Original compression algorithm	Joint compression encryption
Barbara	34.94	34.92
Airplane	39.92	39.88
Girl	37.69	37.71
River1	31.43	31.37

The 'Lena' image is used to test the effect of resolution selective encryption. Corresponding to the resolution of wavelet transform, three sub-bands of the same resolution (HL, LH, and HH) use the same keys, and we call them first-level sub-band key, second-level sub-band key, and third-level sub-band key, respectively.

When the key is erroneous, the algorithm uses the erroneous key to decrypt. Table 3 shows that the reconstructed quality (PSNR) changes with code stream when the decrypted key in different resolutions is erroneous. From this table, when the key is right, the reconstructed image quality improves as the rate increases; once the key is erroneous the reconstructed image quality slightly reduces as the rate increases. When the sub-band key in some resolution is erroneous, the reconstructed data quality of a higher-level sub-band increases with the rate increasing. However, when the key of the corresponding sub-band is erroneous, the reconstructed coefficients would be erroneous, and the error in its lower level sub-band would be more serious. After the inverse wavelet transform, the image data error resulting from the error coefficient is more serious, so it induces the reconstructed image quality to be slightly lower as the rate increases.

From Table 3, we can see that the influence of reconstructed image quality is different if the sub-band key is erroneous at a different level, because the contribution of the first-level sub-band coefficient to the reconstructed image is relatively low. When its key is erroneous, the reconstructed image quality is about 30 dB.

Table 3. Influence of an erroneous key on the reconstructed image quality.

Rate	Non-key error	First-level band key error	Second-level band key error	Third-level band key error
0.5	36.00	30.97	23.42	17.74
0.75	37.80	30.77	22.43	16.14
1.0	39.15	30.70	22.50	15.87
1.25	40.50	30.64	21.75	15.54
1.5	41.15	30.56	21.74	15.37
1.75	42.66	30.52	21.60	15.31
2.0	43.39	30.50	21.50	15.28

When the second-level sub-band key is erroneous, the reconstructed coefficient in the second level is erroneous. The set significance error may occur. Once set significance error occurs, the reconstruction of the first-level sub-band coefficient will be affected, and the reconstructed error in the first-level band will be introduced. In other words, the error of the reconstructed coefficient spreads to lower-level sub-band. Therefore, the reconstructed image quality drops down to 22 dB when the second-level sub-band key is erroneous. Similarly, when the third-level sub-band key is erroneous, the reconstructed image quality is about 16 dB. The decline in quality is more serious.

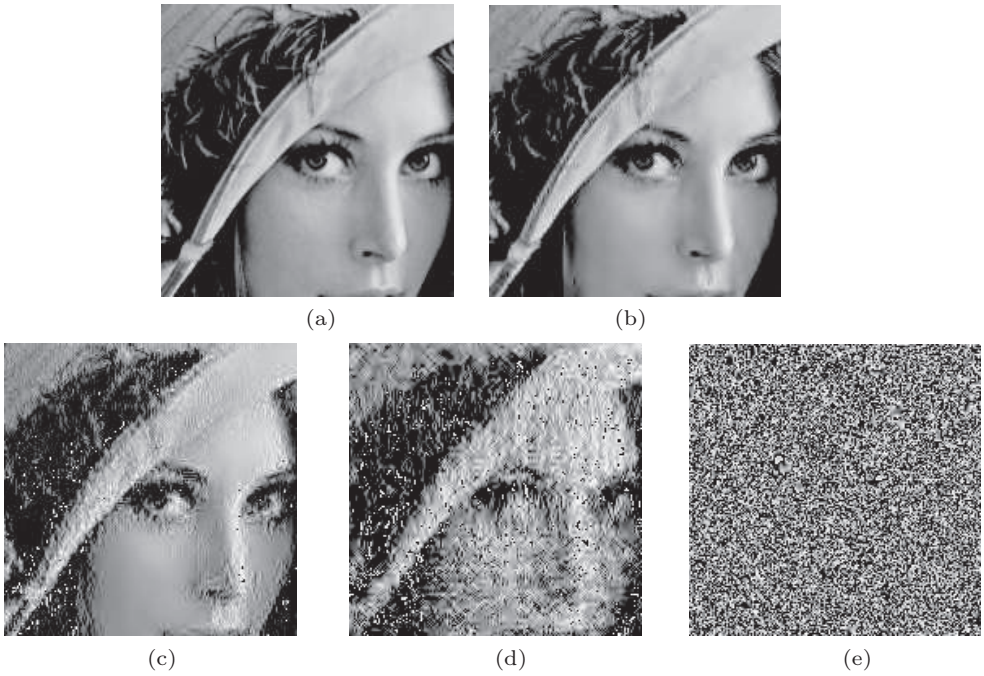


Fig. 5. Reconstructed images.

Figure 5 shows the sub-images taken from the reconstructed image. If the key error appears in the second-level and third-level sub-band, the visual effect of reconstructed image declines seriously. If the first-level sub-band key is erroneous, the image quality declines, but the visual effect is not particularly obvious. If the key error appears in LL band, it cannot obtain the normal image data from the reconstructed image.

6. Conclusions

From the theoretical analyses and experimental results above, the following conclusions can be drawn.

1) Image joint compression encryption can be implemented by using the method of context modification.

2) If the selection of parameters is appropriate, it can be ensured that the reconstructed image quality of image joint compression-encryption algorithm is almost the same as that of the original compression algorithm.

3) The image resolution selective encryption can be realized by modifying the zero-tree encoding structure and introducing adaptive arithmetic coding.

4) The probability distribution of the adaptive arithmetic coding adopted in the proposed algorithm is more complicated than in arithmetic encryption based on interval splitting, so the password is more secure.

Our future work will focus on the deeper theoretical research on the problems existing in joint compression encryption, including the influences of the context modification algorithm and decision encryption on the compression efficiency and the encryption security, and other joint compression-encryption algorithms.

References

[1] Katti R S, Srinivasan S K and Vosoughi A 2011 *IEEE Trans. Inf. Forensics Security* **6** 19
[2] Kim H, Wen J T and Villasenor J D 2007 *IEEE Trans. Signal Process.* **55** 2263
[3] Wu C P and Kuo C C J 2005 *IEEE Trans. Multimedia* **7** 828
[4] Grangetto M, Magli E and Olmo G 2006 *IEEE Trans. Multimedia* **8** 905
[5] Wen J T, Kim H and Villasenor J D 2006 *IEEE Tran. Signal Process. Lett.* **13** 69
[6] Bose R and Pathak S 2006 *IEEE Trans. Circuits Syst. I* **53** 848
[7] Mao Y and Wu M 2006 *IEEE Trans. Image Process.* **15** 2061
[8] Zheng H R and Jing C H 2003 *J. Commun.* **24** 73 (in Chinese)
[9] Duan L L, Liao X F and Xiang T 2010 *Acta Phys. Sin.* **59** 6744 (in Chinese)
[10] Deng J X, Wu C K and Chen J 2004 *Acta Opt. Sin.* **24** 299 (in Chinese)
[11] http://www.jpeg.org/public/jpeglinks.htm.
[12] Taubman D 2000 *IEEE Trans. Image Process.* **9** 1158
[13] Taubman D, Ordentlich E, Weinberger M and Seroussi G 2002 *Signal Process. Image Commun.* **17** 49
[14] Christopoulos C, AskelÖf J and Larsson M 2000 *IEEE Signal Process. Lett.* **7** 247