Image Encryption Method Based on the B-Transform for the Improvement of the DCT Compression Efficiency

H. Jeong and Y. Choe

***Abstract*—This paper presents the encryption method followed by compression with image. It encrypts the image using the B-transform and then compresses by the DCT (Discrete Cosine Transform) based the standard image compression method (e.g. JPEG). The output of B-transform is the partially sorted string and the additional position information from the original permutation string. The additional position information generates the B-code. This code used by the encryption key whose space is 10^{19500} enough to avoid to brute-force attack. Also, when the compression ratio of the reconstructed image is same, the PSNR of our method is about 1.5 times better than the conventional scheme. So, the proposed algorithm provides the secure encryption and the improvement of compression efficiency.**

***Index Terms*—B-Transform, compression, DCT, encryption.**

I. Introduction

Due to the rapid development of digital media and communication technologies, it becomes so frequent and fast-speed access to the Internet via a wired or wireless network connection that large amounts of multimedia data is more actively transferred. So, the intellectual property and the real time data protection for large amounts of multimedia is the important research area. These multimedia data should be protected to ensure the reliability of multimedia information, the confidentiality of the security policies for the contents transfer, and the copy protection against the illegal diffusion of contents [1]-[3].

For this protection, the image encryption techniques have been researched in [4], [5]. With these methods, the image is encrypted by changing the pixel positions and values. Since these methods do not consider the compression, the image after encryption is not easy to compress by the standard compression technique such as JPEG. As a result, both the compression efficiency and the quality of the decompressed image are very low. In the most cases, to recover this inefficiency, the compression is followed by the encryption. However, in some application scenarios, when a sender needs to transmit some data to a receiver, the sender hopes to keep the information confidentially to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data [6], [7].

Both [6], [7] are the compression technique for the encrypted image by the customized encryption method. In [6], it shows new technique which is customized by the encryption method changing the pixel position. The quality of the reconstructed image is good due to using the neighbor pixels. But, it is an iterative method and needs too much memory allocation to make orthogonal matrix. On the other hand, it can be used by applying spatial characteristic in [7]. It is customized by the encryption method only changing the pixel values without changing the pixel positions. The quality of the reconstructed image which has many edges and textures is good due to predicting them.

Although these methods are customized by the encrypted image, their compression efficiency is not better than the standard compression method (e.g. JPEG). So, we propose the novel encryption method using B-transform to improve the compression efficiency by the DCT-based standard compression method. The remaining sections of this paper are organized as following. In the Section II, we describe the B-transform. The Section III will show the compression and encryption process. And in the Section IV, we evaluate the performance of our proposed method by comparing to the combination of the previous encryption methods and compression methods. The conclusion of this paper will be presented in the Section V.

II. B-Transform

A. B-Transform Using Order Relation

From the set theoretical point of view, the image can be separated by a pixel set and an intensity set. The pixel set is a totally ordered one whose elements can be comparable by lexicographical order relation, and the range of elements in the intensity set is from 0 to 255 with the same size of the pixel set. According to this, RSTIM (Relation-based Set Theoretical Image Model) defines the function relation between two sets. Also, we can analyze the RSTIM by information theoretical approach. Because the pixel set is totally ordered, the amount of information is zero. So, the information quantity of image is concentrated only to the intensity set. Therefore, by the technique of information partitioning, we can divide the information with two sets. These two set can be compressed respectively.

From this property, there is B-transform which is the ordering transform. Assume that there is a data set, X and P_X denotes the set of all permutations of the set X. At this time, if

Manuscript received November 20, 2012; revised January 28, 2013.

H. Jeong is with the Electrical and Electronic Engineering Department, Yonsei University, Sinchon-dong, Seodaemun-gu, Seoul, 120-749, Rep. of Korea (e-mail: hee.jeong@yonsei.ac.kr).

Y. Choe is with the Electrical and Electronic Engineering Department, Yonsei University, Sinchon-dong, Seodaemun-gu, Seoul, 120-749, Rep. of Korea (e-mail: yschoe@yonsei.ac.kr).

DOI: 10.7763/IJCCE.2013.V2.203

p is an element of the P_X, p can be like $(x_1 x_2 x_3 \ldots x_k)$ [8]. Then, B-transform function $B(.)$ and its inverse $B^{-1}(.)$ of p can be defined as following:

Forward transform:

$$B(p) = (\bar{p}; \delta) = (\bar{x}_1, \bar{x}_2, ..., \bar{x}_k; d_1, d_2, ..., d_{k-1}) \quad (1)$$

Backward transform:

$$B^{-1}(\bar{p}; \delta) = (x_1, x_2, ..., x_k) = p \quad (2)$$

where, if $p_0 = p$, the projection function $\pi_i(p) = x_i$, then $\bar{x}_i = \pi_i(O_i(p_{i-1}))$ $(0 < i < k)$ and $O(.)$ is an ordering function.

B. B-Code Using Order Complexity

As you can see above, the information of p is separated into two parts by the B-transform, namely the partially sorted string ($\bar{p}$) and the additional position information (δ). After the B-transform is successively applied to p m times, where m depends on order complexity, p is perfectly sorted and there is no information. So, the information of p is changed into the binary form of the additional information δ s, and it can be more compact binary representation as the following two properties, where $\delta_i(j)$ denotes the j^{th} digit in the i^{th} B-transform. [8]

P1. In the i^{th} B-transform for any symbol string of size n, the digits of $\delta_i(j)$ $(n-i < j < n)$ are all zero.

P2. If $\delta_i(j) = 0$, then $\delta_{i+1}(j-1) = 0$.

Finally, with these two conditions, P1 and P2, a new binary representation becomes the B-code.

III. The Encryption and Compression

A. Encryption by B-Transform

To encrypt an image, we should choose the user key 1, 2. The user keys determine the size of the sub-block for B-transform. But, if the value of user key 1, 2 is too small, the degree of encryption is very low like Fig. 1. So, the criterion of user key should be defined. The summation of two keys has to be larger than the standard deviation of original image. And the sub-blocks by user keys may not be overlapped.

Fig. 1. Lena image (a) original image (b) user key = (8,1) encrypted image.

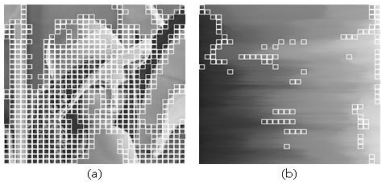

Fig. 2. Discontinuous sub-block (a) original image (b) after B-transform.

Because B-Ttransform is the ordering transform, the discontinuity of image is removed well as Fig. 2. To prove this, we can define the discontinuity by MAE (Mean Absolute Error). According to central limit theorem, we can estimate the sample mean, β for Gaussian distribution using MLE (Maximum Likelihood Estimation). As the result, the estimated value is like (3).

$$L(x_1, x_2, ..., x_N) = \prod_{i=1}^{N} f(x_i - \beta) = \left(\frac{1}{2\pi\sigma^2}\right)^{N/2} \exp\left(-\sum_{i=1}^{N} \frac{(x_i - \beta)^2}{2\sigma^2}\right)$$

$$\beta = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3)$$

Since we use JPEG for the compression, the image is divided by 8x8 sub-block. The local MAE for a sub-block is $|\beta - x_i|$. The global MAE can be calculated by local MAEs like (4).

$$globalMAE = \frac{1}{n}\sum_{i=1}^{n} localMAE \quad (4)$$

By using this global MAE, if there is a point larger than global MAE in sub-block, we can define the discontinuity. (a) of Fig. 2 shows that the discontinuity of the edges or textures detect well. (b) of Fig. 2 shows the amount of discontinuity reduced by applying B-transform.

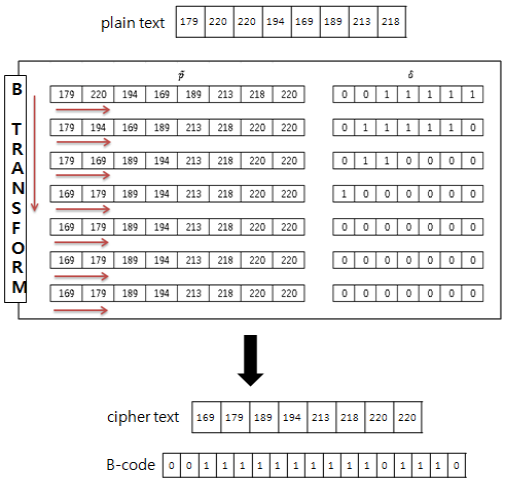

Fig. 3. Encryption by B-transform.

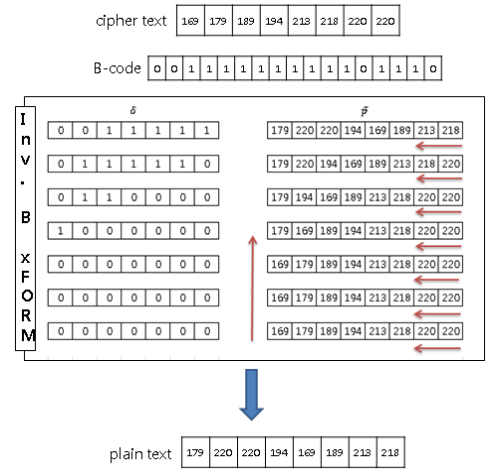

Fig. 4. Decryption by inverse B-transform.

The example of encryption process by B-transform is shown in Fig. 3. The process is similar with popular bubble sort algorithm. Also, as you can see that, B-code is generated from B-transform coefficients by aforementioned properties.

B. Decryption

On the contrary to encryption, the decryption process is performed by inverse B-transform with B-code. Please refer to Fig. 4.

C. Overall System

Fig. 5 shows the overall system of proposed algorithm. Our proposed system includes the encryption and decryption module by applying B-transform and the compression & decompression module by applying JPEG. The DCT based compression technique is performed by the approximation to several basis vectors. So, if the image has many edges or textures, the compression efficiency gets lower. But, since our proposed algorithm reduces such a discontinuity, the compression efficiency is higher.

IV. Experimental Results and Analysis

In order to evaluate the performance of the proposed encryption method, this paper used MATLAB to simulate this algorithm. We took gray images of 256x256 as experimental images. Fig. 6 shows the encrypted image by the proposed method. The experimental results show that the encrypted images do not give any information that can analogize the original image. So, we can say that the purpose of encrypting images has been achieved. Also, we can analyze the degree of encryption and compression from the following quantitative analysis measures.

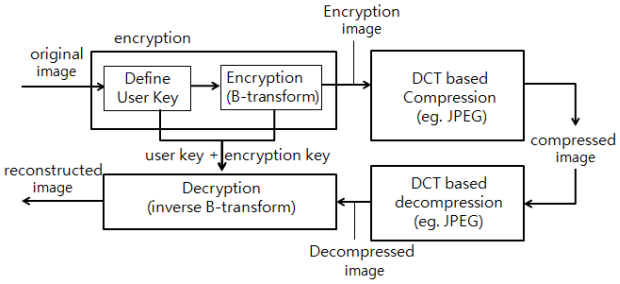

Fig. 5. The overall system of proposed algorithm.

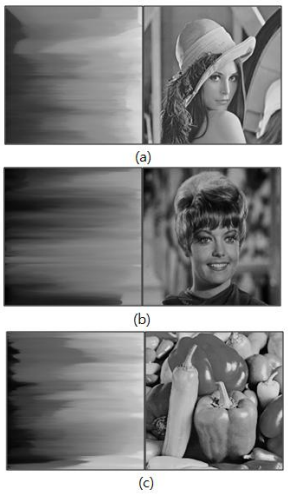

Fig. 6. The encryption image by proposed algorithm (a) Lena (b) Zelda (c) pepper.

A. Key Security Analysis

The key space for a good cryptosystem should be sufficiently large to make the brute force attack infeasible. Key space implies the total number of different keys which can be used for the purpose of encryption and decryption. According to [9], the key space in order to avoid the brute-force attack should be more than $2^{100} = 10^{30}$. Our proposed method generates the different length of encryption key sequence as two user keys. But, if the image size is N, its key space may be at least 2^N. For example 256x256 images, an intruder should try to break it by 2^{65536}. This is sufficient enough to resist the brute-force attacks. Fig.7 shows the image decrypting with wrong keys.

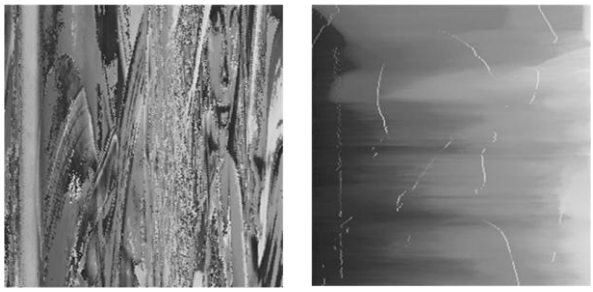

Fig. 7. The decryption image with wrong key for Lena image (a) wrong user key (b) wrong encryption key.

TABLE I: The Moving Distance

	convention		proposal	
	[4]	[5]	1x256	256x1
Lena	64	137	72	95
Zelda			94	75
Pepper			81	87
Goldhill			104	103
Boat			98	105
Barbara			90	94

B. Moving Distance Analysis

The average moving distance is described in [10] such as following,

$$f(i,j) \xrightarrow{encryption} F(u,v)$$
$$D = \frac{1}{r \times c} \sum_{i=1}^{r} \sum_{j=1}^{c} \sqrt{(w-i)^2 + (v-j)^2}\ , \quad (3)$$

where, (i, j) represents a pixel coordinate in the original image and (w, v) represents the pixel coordinate of that point in the encrypted image. A large value of average moving distance indicates that the original image and the encrypted image are less related. Hence the efficiency of the encryption technique is high. As you see Table I, [4] uses the mirroring technique to change the pixel position. So, it is always same value for the same size image. And [5] uses a randomly scrambling technique to change the pixel position. So, the moving distance is the largest of all. The result of our proposed algorithm is different by user key. But, in this case, our proposed algorithm is moderate in the moving distance.

C. PSNR Analysis

Our proposed method is for the improvement of compression efficiency. Although the compression ratio is very low, if the quality of decrypted image is very noisy, it can not be guaranteed that the compression efficiency is high. Therefore, the PSNR at the same compression ratio represents compression efficiency. As you can see Fig. 8, since [6] is iterative method with the information of neighbor pixels, it is better than [7]. But, our proposed method is superior to others, and about 1.5 times better.

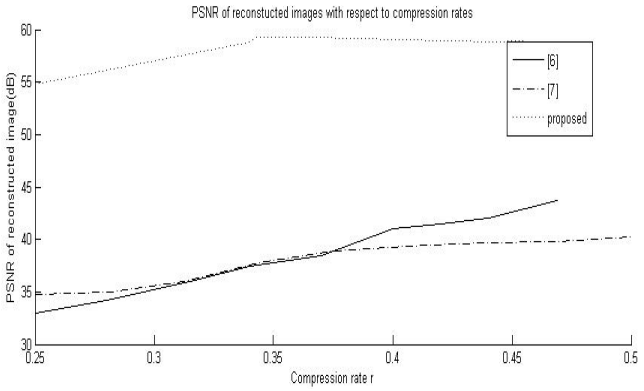

Fig. 8. PSNR versus compression ratio for Lena image.

V. Conclusion

Because the existing encryption methods do not consider compression, to compress the encrypted image, the new compression algorithm was needed. According to this necessity, several algorithms were proposed. But, the compression efficiency of them is worse than the standard compression technique. So, we proposed the novel image encryption method which can improve the compression efficiency for the DCT-based standard compression method. By reducing the discontinuity of the image using B-transform, the compression efficiency of proposed method is better than the standard compression method for the normal image.

Acknowledgment

This work was supported by the Samsung Electronics Co., Ltd.

References

[1] A. M. Eskicioglu, "Protecting intellectual property in digital multimedia networks," *IEEE Trans. on Computer*, vol. 36, no. 7, pp. 39-45, July 2003.

[2] H. H. Yu, D. Kundur, and C. Y. Lin, "Spies, thieves, and lies: The bottle for multimedia in the digital era," *IEEE Trans. On Multimedia*, vol. 8, no. 3, pp. 8-12, Jul.-Sep. 2001.

[3] J. M. Justin and S. Manimurugan, "A survey on various encryption techniques," in *Proc. Int. Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 1, Mar. 2012, pp. 429-432.

[4] W. Yanling, Image scrambling method based on chaotic sequences and mapping, in *Proc. 1st Int. Workshop on Education Technology and Computer Science (ETCS)*, Mar. 2009, pp. 453-457.

[5] N. S. Kulkarni, I. Gupta, and S. N. Kulkarni, "A robust image encryption technique based on random vector," in *Proc. 1st Int. Conf. on Emerging Trends in Engineering and Technology (ICETET)*, July 2008, pp. 15-19.

[6] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 1, pp. 53-58, Mar. 2011

[7] X. Kang, X. Xu, A. Peng, and W. Zeng, "Scalable lossy compression for pixel-value encrypted images," *Data Compression Conference (DCC)*, Apr. 2012.

[8] S. Hong, M. Eom, and Y. Choe, "Variable-length code based on an order complexity," *Picture Coding Symposium (PCS)*, May 2009.

[9] A. N. Pisarchik, N. J. Flores-Carmona, and M. C. Valadez, "Encryption and decryption of images with chaotic map lattices," *Chaos: Interdiscip. Journal of Nonlinear Sci.*, vol. 16, no. 3, pp. 033118, Aug. 2006.

[10] X. Liu, J. Zhang, J. Zhang, and X. He, "Image scrambling algorithm based on chaos theory and sorting transformation," in *Proc. Int. J. of computer science and network security*, vol. 8, no. 1, Jan. 2008, pp. 64-68.

Hee Jeong received the B.S. degree in Electronic Engineering and Avionics from Korea Aerospace University in 2003. Presently she is pursuing her PG degree in Electrical and Electronic Engineering from Yonsei University, Korea. She works in Samsung Electronics Co. Ltd since 2003. Her research interest includes image processing and security.

Yoonsik Choe received a B.S. degree in electronic engineering from Yonsei University in 1979, and an MSEE in systems engineering, and MS and PhD degrees all in electrical engineering from the Case Western Reserve University, the Pennsylvania State University, and the Purdue University, in 1984, 1987, and 1990, respectively. From 1990 to 1993, he was a principal engineer at the industrial electronics research center in the Hyundai Electronics Industries, Co. Ltd. Since 1993 he has been with the Department of Electrical and Electronic Engineering at the Yonsei University where he is professor. His research interests include video coding, video communication, statistical signal processing, and digital image processing.