中正嶺學報 第三十七卷 第一期 民國 97.11.
JOURNAL OF C.C.I.T., VOL.37, NO.1, NOV., 2008

Integrated Batch Encryption to Still Images

Tzung-Her Chen and Chang-Sian Wu

Department of Computer Science and Information Engineering, National Chiayi University

ABSTRACT

Thanks to the rapid growth of Internet bandwidth, it is popular to share still images via the Internet in batch transmission. It is well-known that the size of image is generally much larger than that of text. Furthermore, partial information loss of images without drawing visual attention is imperceptibly allowed. Hence, traditional cryptographic encryption algorithms are sometimes not suitable for direct encrypting of a batch of images. In this paper, a novel batch image encryption algorithm for images is presented to benefit from its efficiency, low transmission bandwidth and security requirement. The experimental results show the effectiveness in terms of compression rate and encryption computation cost.
Keywords: batch image encryption, vector quantization, Huffman coding.

靜態影像之整合性批次加密

陳宗和　巫昌憲

國立嘉義大學資訊工程學系

摘　　要

由於網際網路頻寬的快速成長，讓整批式大量靜態影像的傳輸及分享變得普及。然而，跟文字資料比起來，影像資料大小顯然大得多；並且，影像資料容許些許失真。這些原因讓傳統密碼技術無法直接適用於大批影像資料的加密。本研究的目的在於提出一個具有高效率、低頻寬及安全性的批次影像加密技術。實驗結果說明本方法可以在壓縮效能及加密計算量上有好的效能表現。
關鍵字：批次影像加密，向量量化，霍夫曼編碼

文稿收件日期 96.3.6; 文稿修正後接受日期 97.7.30.
Manuscript received March 6, 2007; revised July 30, 2008.

I. INTRODUCTION

The market of digital camera, digital video camera recorder and camera phone have grown rapidly so that photographic devices are regarded as an essential daily item by millions of people. Consumers capture more images than ever before. Usually they send their digital pictures to others via e-mail and make good use of an online photo printing service to share their pictures in batch-of-images transmission over the public network.

Intuitively, cryptographic tools are well-defined to encrypt/decrypt multimedia. However, these tools are so sensitive that even just one-bit distortion is not allowed, while a little distortion of images due to compression could be visually neglected by human naked eyes. Since the size of multimedia is always much larger than that of text, digital multimedia can be turned into a compressed form by some compression technologies in order to reduce communication burden. Hence, it is reasonable and beneficial to guarantee the confidentiality of images over public networks by combining both compression and encryption techniques.

In the literature, image encryption methods can be categorized into 1) full, 2) selective, and 3) integrated encryption.

1) *Full encryption*: The image is fully encrypted with traditional encryption algorithms, such as AES, DES, etc., where the computation overload becomes a concern. Another method is to adopt a sophisticated scrambling/chaotic technique to render images in either spatial domains or transformed domains rather than encrypting images directly. Literature review shows many schemes adopt either SCAN patterns [3, 5, 9, 19, 20, 24] or chaos systems [2, 7, 10-14, 18, 21, 29, 31, 34]. The common goal is to rearrange the pixels of the image or change the pixel values. Encryption using the SCAN language involves a sample substitution rule. Each SCAN language is defined by a grammar and each has a set of basic scan patterns. That is, a set of transformations and rules are used simultaneously to compose simple scan patterns to obtain complex ones. Chaos systems usually exploit Torus Automorphisms function or chaotic maps to disturb the pixels of an image. However, the computation cost is also high.

2) *Selective encryption*: In selective encryption approaches [1, 8, 17, 23, 26, 30], images are turned into transform domains, such as DWT and DCT. Then, only some parts of coefficients in the transform domains are scrambled or encrypted. However, selective encryption algorithms have a potential security drawback pointed out in Ref. [1] and [23]. That is, the coefficients not encrypted may disclose information of the original images. In strict definition of security, the encrypted content must be meaningless even if the rough sketch is not allowed

3) *Integrated encryption*: This method skillfully combines encryption with compression [4, 6, 19]. At first glance, full encryption is a good candidate; however, computational cost is high especially for real-time applications. Furthermore, selective encryption is usually not secure enough. Nowadays, multimedia is usually distributed in the form of compression. Hence it is straightforward to make profit from combining encryption with compression.

Many researchers have come up with a variety of image encryption techniques [2, 3, 5, 7-10, 14, 17, 18, 20, 29-31]. Although the techniques proposed so far have secured some extent in the area of image confidentiality, most current image encryption techniques aim at encrypting a single image rather than a batch of images. The existing research neglects the fact that people usually distribute digital images in the way of batch transmission.

In addition, the other inevitable fact should be taken into account at the same time. Due to limited communication bandwidth, almost all images traveling over the Internet are in a compressed form to save transmission time and storage space.

As analyzed above, these two requirements in practice will signal the dawn of spectacular new opportunities to combine compression and encryption to a batch of images. To the best of our knowledge, the scheme in Ref. [4] is the first to provide an approach to encrypt a batch of images at the same time by means of compressing images using VQ and then encrypting the VQ indices using traditional cryptosystem. Unfortunately, Lee *et al.* [19] pointed out that the scheme [4] suffers from the weaknesses of chosen-plainimage attacks and cipherimage-only attacks.

This paper proposed a novel batch encryption algorithm to encrypt a large number of images at a time. We first facilitate VQ compression technique to compress a batch of images and then further encrypt them using randomized Huffman coding. VQ is adopted as an efficient approach to achieve low bit-rate image compression. A second reason to adopt VQ is mainly that it needs a simple hardware. In the meantime, Huffman coding, a no-loss coding technique, is adopted to obtain the extra advantage that the bit rate can be further reduced without extra loss of image quality. Furthermore, confidentiality is achieved by a skillful design of randomized Huffman coding in the processes of image compression.

The rest of paper is organized as follows. Section 2 proposes the present batch image encryption method. Section 3 gives the experimental results and then security analysis and discussions are described in Section 4. Finally, the conclusions are showed in Section 5.

II. PROPOSED METHOD

A batch image encryption algorithm based on VQ and Huffman coding is proposed. VQ used to firstly compress a batch of original images is a lossy compression technology. Huffman coding used to further compress and scramble the index sets generated by VQ is a lossless compression technology. Two advantages are found if VQ is involved in image compression.

1) The required bit rate of VQ compression is comparatively small and thus it saves a lot of storage space and transmission bandwidth.

2) VQ needs a simple hardware structure to provide fast encoding/decoding procedures.

To further improve compression performance and lower computation cost alternatives include variable-length coding (VLC) techniques such as Huffman coding or arithmetic coding, and index compression techniques such as the scheme in Ref. [16]. For simplicity, the basic VQ technique is introduced to compress the still images into the indices. All the sophisticated VQ techniques are suitable for the proposed scheme.

2.1 Batch Image Encryption

To transmit a batch of images to the receiver (his friends or an online photo printing), a sender firstly encrypts these images for confidentiality over hostile networks. The batch image encryption process is illustrated in Figure 1 and the details are described as follows.

Step 1. Consider a set of grayscale images, say m images, X_p (p=1, 2, …, m) with $M\times M$ pixels. Firstly, a common codebook $CB=\{C_i \mid i=0,1,2,...,L-1\}$ is generated by the LBG algorithm [22], where the codeword $C_i=\{c_{ij} \mid j=1,2,3,...,k\}$ and k are the dimension of codewords.

Step 2. Each image X_p is independently compressed by VQ. An image is divided into nonoverlapped image blocks $X_{pq}=\{X_{pq}(i) \mid i=1,2,3,...,k\}$ with size of $N\times N$, i.e., k, pixels, where $q=1,2,...,\frac{M\times M}{N\times N}$. Each image block X_{pq} is compared with each codeword in the codebook to evaluate the difference by computing their Euclidean distance to get the neatest codeword C_i for X_{pq}. The Euclidean distance is defined as follows.

$$d_{ED}(X_{pq},C_i)=\min_{i\in\{0,1,...,L-1\}}\sqrt{\sum_{j=1}^{k}(X_{pq}(j)-c_{ij})^2} \qquad (1)$$

So we can obtain a set of corresponding index tables with size of $\frac{M\times M}{N\times N}$, denoted

$$I_j=\{I_j(i) \mid I_j(i)\in\{0,1,2,...,L-1\}, i=1,2,...,\frac{M\times M}{N\times N}\} \qquad (2)$$

where j = 1, 2, …, m.

Step 3. To further encode these index tables in an efficient way, We apply a lossless variable-length coding technique; generate a Huffman tree, called T_1, for all VQ index tables; then change the encoding way based on the randomized T_1. To scramble all the indices, one generates the other Huffman tree T_2 according to T_1. If the right-hand-side branch of T_1 is labeled '0', then we set the right-hand-side branch of T_2 to be labeled '1'. If the left-hand-side branch of T_1 is labeled '1', then we set the left-hand-side branch of T_2 to be labeled '0'.

Step 4. We encrypt each index $I_j(i)$ with Huffman tree either T_1 or T_2 which is determined by the secret key SK. Finally, we obtain encrypted code E.

Step 5. The sender sends the compressed and encrypted code E, and Huffman tree T_1 to the receiver.

For enhancing the security, inspired from the approaches in Ref. [32] and [33], the aforementioned scheme can be enhanced by involving more than two Huffman coding trees derived from T_1 as follows.

First, the first Huffman tree is determined to generate $r=2^h$ Huffman trees accordingly which are numbered from 1 to r by a mutation key MK. Assume that h is the height of the original Huffman tree. For each level i, i=1, 2, ..., h, the two branches may swap according to the bit sequence generated by MK. In such a way, the other Huffman trees T_j, j=2, …, r, are obtained in another form of the original T_1.

Secondly, we generate a long bit sequence S using a one-way hash function with the secret key SK as the seed. This bit sequence S is then partitioned into $m\times\frac{M\times M}{N\times N}$ subsequences S_i with the bit size of h, where i=1, 2, …, $m\times\frac{M\times M}{N\times N}$. Finally, we encrypt each index $I_j(i)$ with Huffman trees T_j which is determined by S_i. Finally, the ciphertext E and the original Huffman tree T_1 are sent to the receiver.

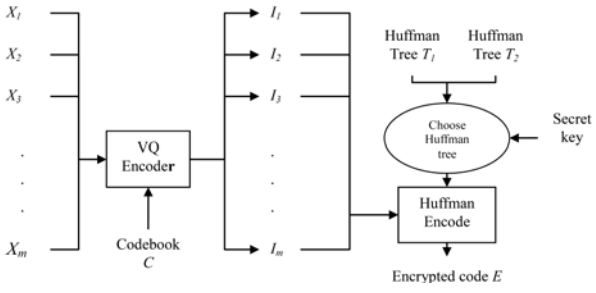


Figure 1. Batch image encryption.

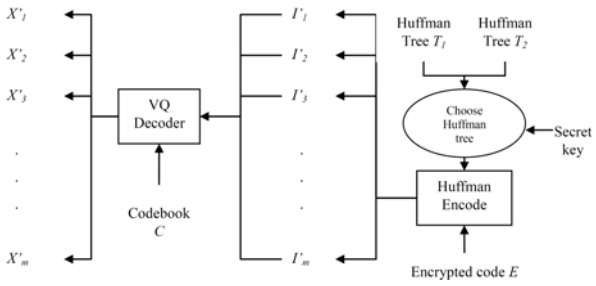


Figure 2. Batch image decryption.

2.2 **Batch Image Decryption**

Suppose the receiver has shared the keys *SK*, and *MK* with the sender in advance. The codebook *C* is public. The sketch of the decryption process is shown in Figure 2.

Step 1. According to *SK*, the receiver generates the bit sequence *S* and then partitions *S* into $m \times \frac{M \times M}{N \times N}$ subsequences S_i with the bit size of *h*. According to the bit sequence S_i, a Huffman tree T_j is decided to decrypt *E* to obtain all decrypted $I_j(i)$. Here T_j can be reconstructed by T_1 and *MK*.

Step 2. Let $I_j(i)$ be further decoded by the same codebook *C*. The receiver turns $I_j(i)$ into the image block C_i. Repeat this process $m \times \frac{M \times M}{N \times N}$ times. Finally, the receiver obtains a set of still images X'_p.

III. EXPERIMENTAL RESULTS

Some experiments are conducted to demonstrate the feasibility of our batch image encryption scheme. We present the experiments with 4 to 49 images that are 256 gray-level images of size 512 x 512 pixels. The original total size of four images is 1024 KB. For example, the four original test images (Lena, F16, Spaceman and Pepper) and the corresponding decrypted images (the PSNR values tell the distortion and quality of images) are as shown in Figure 3. If we adopt *r* Huffman tables, the entries of each Huffman table are *L* because the index values of the codebook *CB* are between 0 and *L*-1. In all Huffman trees, the lengths of the Huffman codes with respect to the same index are the same. For example, there is a VQ index with value of 168, the corresponding Huffman code from T_1 is '001' and the corresponding Huffman code from T_2 is '010'. The length of two codes from T_1 and T_2 for the index value 168 is 3 bits. The length of the code from the other T_j for the index value 168 is also 3 bits.

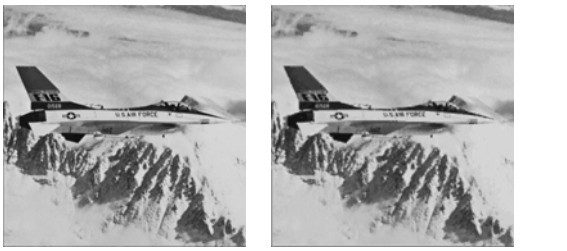
All images in our experiments are divided into 4 x 4 pixel blocks with the same size of each codeword. The number of codewords in the codebook is 256. After compression, the size of VQ indices is 64 KB, shown in Table 1. Figure 4 shows that the decrypted images are meaningless in case of a wrong secret key involved.

From the perspective of comparison with traditional cryptosystems, AES and DES are used to directly encrypt/decrypt the images. The source programs of AES and DES from Ref. [15] are used. The computer we used for the experiments is a PC with a 2.4 GHz Pentium IV CPU and 512 Mbytes of memory.

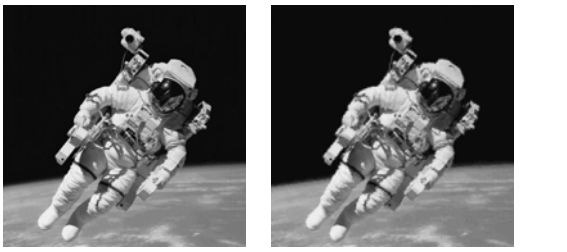
Table 1. Comparison of compression performance

	4 images	9 images	16 images	25 images	36 images	49 images
Original size	1024 KB	2304 KB	4096 KB	6400 KB	9216 KB	12544 KB
Compressed size	64 KB	144 KB	256 KB	400 KB	576 KB	784 KB
Encrypted size	60.6 KB	137 KB	241 KB	369 KB	524 KB	710 KB

(a) The original Lena and the decrypted image with PSNR 30.57 dB



(b) The original F16 and the decrypted image with PSNR 27.98 dB



(c) The original Spaceman and the decrypted image with PSNR 28.36 dB

(d) The original Pepper and the decrypted image with PSNR 30.59 dB

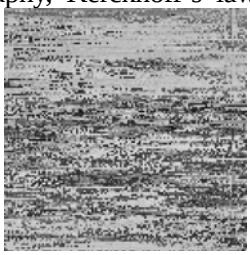
Fig.3. The original images and the corresponding decrypted images with an exact key.

IV. SECURITY ANALYSIS AND DISCUSSIONS

4.1 Security analysis

The security of the proposed scheme depends upon the fact that an attacker is not able to correctly decode the index tables to obtain the original images without knowing the particular Huffman tables and the order they are selected. If the default Huffman table is used to decode, the rendering will be completely garbled nonsense.

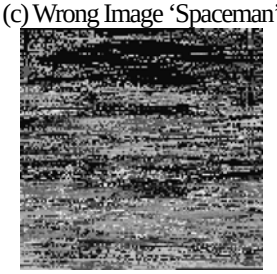
In cryptography, Kerckhoff's law is famous as:



(a)Wrong Image 'Lena'

(b)Wrong Image 'f16'

(c) Wrong Image 'Spaceman'



(d) Wrong Image 'Pepper'

Fig.4. The decrypted images with a wrong key

a cryptosystem should be still secure even if everything about the cryptosystem, except the secret key, is known [16]. If the attacker knows the algorithm, the following three types of cryptanalytic are discussed:

Under cipherimage-only attacks, cryptanalyst has obtained the cipherimage. The common approach is the brute-force attack (exhaustive key search) without any information of plainimage. The key space is obviously important to counteract against this attack. In our scheme, all indices are encrypted into Huffman code before transmission. For example of m index tables with size of b, i.e., if $M = 512$ and $N = 4$, then $b = \frac{M \times M}{N \times N} = 128 \times 128$, each index in table is encoded with Huffman tree T_1 or T_2. The size of key space is $min(2^{m \times b}, 2^{|SK|})$. The function $min(.,.)$ returns the minimal value and $|.|$ denotes the bit size of SK. If $|SK| = 128$, it is large enough to resist against the brute-force method. In the security-enhanced scheme the size of key space is $min(2^{h \times m \times b}, 2^{|SK|})$ because the number of Huffman tables is added up to $r = 2^h$. Thus cipherimage-only attacks are impractical.

On the other hand, under known-plainimage attacks and chosen-plainimage attacks, they are more powerful than cipherimage-only attacks. Suppose that the legal user encrypts all plainimages into corresponding cipherimages by an identical key SK, the attacker may break the image cryptosystem easily. If the attacker obtains certain of pairs of plainimages and cipherimages, he has many clues by analyzing these pairs to deduce SK. Therefore, the encryption key must be disposable. In other words, the encryption key must be for one-time-use. In this way, even if the attacker figures out the current encryption key, it is not of any help to deduce the next encryption key. Thus, these two attacks alone are also impractical.

4.2 Discussions

(1) Generalization: Since VQ has valuable advantages such as high compression ratio and simple implementation hardware, it is a good candidate for lossy compression with acceptable image quality. If image quality is a main concern, some compression technologies can be taken into account such as JPEG and JPEG2000. That is, the proposed batch image encryption could be integrated with existing compression standards.

(2) Compression performance: It is both a methodology and art how to integrate the methods of image compression and encryption with respect to the proper operation sequence. First-compression-then-encryption may lower the security level [30] while first-encryption-then-compression is often compression-ineffective because scrambling itself increases entropy in such a way that further diminution in compression returns. For image communication, it is

unfavorable for the image size to become larger after encrypting. In [28], random permutation of discrete wavelet coefficients before encoding using SPIHT or JPEG2000 has been studied. However, the authors found that this significantly reduced compression performance up to 27% for test images. In the present scheme, lossless index compression techniques are adopted to obtain the advantages that the bit rate can be further reduced without extra loss of images and thus the time for the subsequent encryption operation will also be reduced. Table 1 shows that the proposed scheme can further enhance the compression performance after compression; for example, it further reduces the file size from 64 KB to 57.37 KB.

(3) Computation cost: Compared with AES and DES, the proposed scheme has the characteristics. In Table 2, for example, the encryption time to four test images by means of AES, DES and the proposed scheme is 688, 969 and 2,155 ms, respectively. The last encompasses 1) 2094 ms for VQ encoding and 2) 61 ms for Huffman coding. On the other hand, the corresponding decryption time is 740, 953 and 95 ms, respectively. It implies the proposed scheme has much lower computation cost on the decryption side. This feature is suitable for the case in which the receiver is a mobile device equipped with lightweight computation capability.

(4) Bandwidth complexity: Thanks to combining encryption with compression technique, in the proposed scheme only 57.37 KB , which is much less than those of the method directly adopting traditional cryptosystems, will be transmitted over the public network, shown in Table 2. In fact, the encrypted images using AES and DES, the file size of encrypted images is still the same or even larger than that of original images.

(5) Huffman trees: In the proposed scheme, only one Huffman tree is constructed according all the VQ indices. Upon the Huffman tree generated, the others are generated as the disturbed versions of the first. Actually, the Huffman tree may be global, i.e., a public one which is well-defined or well-known for users.

Table 2. Comparison of time and bandwidth complexity with four-image encryption

Methods	Encryption time	Decryption time	Total time	Final size
AES	688ms	704ms	1392 ms	1025 KB
DES	969ms	953 ms	1922 ms	1025 KB
Our scheme	VQ encode + Huffman encode	Huffman decode +VQ decode	2250 ms	57.37 KB
	2094+61 ms	63+32 ms		

V. CONCLUDING REMARKS

In this paper, a novel image batch encryption system combining both compression and encryption is proposed. Firstly, the VQ compression technique takes advantage of high compression performance and simple implementation hardware. Secondly, the lossless variable-length coding technique is utilized not only to enhance compression performance without any distortion but also to scramble the compressed content simultaneously. Within the next couple of years, batch image encryption will be in an early development stage. The main concept of the proposed scheme, disturbing the compressed result, i.e., VQ indices here, is also suitable for disturbing the quantized DCT coefficients in the JPEG standard adopting Huffman coding as the default entropy coding. However, the following reason makes the design not so intuitive and thus be our future work. Due to the JPEG-compliant problem, the decoder should be redesigned to fit the need of decrypting the encrypted JPEG files. Although a well-defined solution will be strengthened still further, the present approach can work well on the mobile clients standing in decryption ends.

ACKNOWLEDGEMENT

This research was partly supported by National Science Council under contract NSC 95-2221-E-415-009-MY3.

REFERENCES

[1] Agi, I., and Gong, L., “An empirical study of secure MPEG video transmission,” Proceedings of IEEE Symposium on Network and Distributed Systems Security, pp. 137-144, 1996.

[2] Billings, L., and Bollt, E. M., “Probability density functions of some skew tent maps,” Chaos, Solitons & Fractals, Vol. 12, No. 2, pp. 365-376, 2001.

[3] Bourbakis, N., and Alexopoulos, C., “Picture data encryption using SCAN patterns,” Pattern Recognition, Vol. 25, No. 6, pp. 567-581, 1992.

[4] Chang, C. C., Hwang, M. S., and Chen, T. S., “A new encryption algorithm for image cryptosystems,” The Journal of Systems and Software, Vol. 58, No. 2, pp.83-91, 2001.

[5] Chang, C. C., and Yu, T. X., “Cryptanalysis of an encryption scheme for binary images,” Pattern Recognition Letters, Vol. 23, No. 14, pp. 1847-1852, 2002.

[6] Chen, T. S., Chang, C. C., and Hwang, M. S., “A Virtual Image Cryptosystem Based upon Vector Quantization,” IEEE Transactions on Image Processing, Vol. 7, No. 10, pp. 1485-1488, 1998.

[7] Chen, G., Mao, Y., and Chui, C. K., "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons & Fractals, Vol. 21, No. 3, pp. 749-761, 2004.

[8] Cheng, H., and Li, X., "Partial encryption of compressed images and videos," IEEE Transactions on signal processing, Vol. 48, No. 8, pp. 2439-2451, 2000.

[9] Chung, K. L., and Chang, L.C., "Large encryption binary images with higher security," Pattern Recognition Letters, Vol. 19, No. 5-6, pp.461-468, 1998.

[10] Feng, Y., Li, L., and Huang, F., "A symmetric image encryption approach based on Line maps," Proceedings of 1st International Symposium on Systems and Control in Aerospace and Astronautics, Harbin, China, pp. 1362-1367, 2006.

[11] Fridrich, J., "Image encryption based on chaotic maps," Proceedings of the IEEE Conference on System ciphers, Man, Cybernetics, Orlando, FL, USA, pp. 1105-1110, 1997.

[12] Fridrich, J., "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, Vol. 8, No. 6, pp. 1259-1284, 1998.

[13] Gao, H., Zhang, Y., Liang, S., and Li, D., "A new chaotic algorithm for image encryption," Chaos, Solitons & Fractals, Vol. 29, Issue 2, pp. 393-399, 2006.

[14] Guan, Z., Huang, H., and Guan, W., "Chaos-based image encryption algorithm," Physics Letters A, Vol. 346, Issues 1-3, pp. 153-157, 2005.

[15] Crypto++ Library 5.5.2, http://www.eskimo.com/~weidai/cryptlib.html

[16] Hsieh, C. H., and Tsai, J. C., "Lossless compression of VQ index with search-order coding," IEEE Transactions on Image Processing, Vol. 5, No. 11, pp. 1579-1582, 1996.

[17] Kundur, D., and Karthik, K., "Video fingerprinting and encryption principles for digital rights management," Proceedings of the IEEE, Vol. 92, No. 6, pp. 918-932, 2004.

[18] Kwok, H. S., and Tang Wallace, K. S., "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons & Fractals, Vol. 32, Issue 4, pp. 1518-1529, 2007.

[19] Lee, W. B., and Chen, T. H., and Lee, C. C., "Security of a new encryption algorithm for image cryptosystems," The Imaging Science Journal, Vol. 54, Issue 3, pp. 178-187, 2006.

[20] Lee, W. B., Chen, T. H., and Lee, C. C., "Improvement of an Encryption Scheme for Binary Images," Pakistan Journal of Information & Technology, Vol. 2, No. 2, 2003.

[21] Lian, S., Sun, J., and Wang, Z., "A block cipher based on a suitable use of the chaotic standard map," Chaos, Solitons and Fractals, Vol. 26, Issue 1, pp. 117-129, 2005.

[22] Linde, Y., Buzo, A., and Gray, R. M., "An algorithm for vector quantizer design," IEEE Transaction Communication, Vol. 28, No. 1, pp. 84-95, 1980.

[23] Liu, Z., and Li, X., "Motion vector encryption in multimedia streaming," Proceedings of 10th International Multimedia Modelling Conference, Brisbane, Australia, pp. 64-71, 2004.

[24] Maniccam, S. S., and Bourbakis, N. G., "Image and video encryption using SCAN patterns," Pattern Recognition, Vol. 37, Issue: 4, pp. 725-737, 2004.

[25] Maniccam, S. S., and Bourbakis, N. G., "Lossless image compression and encryption using SCAN," Pattern Recognition Vol. 34, Issue 6, pp. 1229-1245, 2001.

[26] Martin, K., Lukac, R., and Plataniotis, K. N., "Efficient encryption of wavelet-based color images," Pattern Recognition, Vol. 38, pp. 1111-1115, 2005.

[27] Menezes, A. J., Oorschot van, P. C., and Vanstone S. A., "Handbook of Applied Cryptography," CRC Press, 1997.

[28] Norcen, R., and Uhl, A., "Encryption of wavelet-coded imagery using random permutations," Proceedings of IEEE International Conference on Imaging Processing, Vol. 5, pp. 3431- 3434, 2004.

[29] Pareek, N. K., Patidar, V., and Sud, K. K., "Image encryption using chaotic logistic map," Image and Vision Computing, Vol. 24, Issue 9, pp. 926-934, 2006.

[30] Van Droogenbroeck, M., "Partial encryption of images for real-time applications," Proceedings of Fourth IEEE Benelux Signal Processing, Hilvarenbeek, The Netherlands, pp. 11-15, 2004.

[31] Wei, J., Liao, X., Wong, K. W., and Xiang, T., "A new chaotic cryptosystem," Chaos, Solitons and Fractals, Vol. 30, No. 5, pp. 1143-1152, 2005.

[32] Wu, C. P., and Kuo, C. C., "Efficient Multimedia Encryption via Entropy Codec Design," SPIE International Symposiun on Electronic Imaging, 2001.

[33] Xie, D., and Kuo, C. C., "An Enhanced MHT Encryption Scheme for Chosen Plaintext Attack," Proceedings of Internet Multimedia Management Systems IV, SPIE Vol. 5242, pp. 175-183, 2003.

[34] Zhang, L., Liao, X., and Wang, X., "An image encryption approach based on chaotic maps," Chaos, Solitons and Fractals, Vol. 24, Issue 3, pp. 759-765, 2005.