Secure Image Transcoding technique using chaotic key based algorithm

Anoop B N[1], Sudhish N George[2], Deepthi P P[3]
Department of Electronics and Communication Engineering[1, 2,3]
National Institute of Technology Calicut, India

Abstract

Transcoding is the direct digital-to-digital data conversion of one encoding to another. This paper proposes a system of secure image transcoder which mainly focuses on multimedia applications such as web browsing through mobile phones, in order to improve their delivery to client devices with wide range of communication, storage and display capabilities. This system based on CKBA encryption ensures end to end security. The performance of the system has been evaluated for different images.

Keywords

Transcoding, CKBA, Encryption

1. Introduction

Now a day the growth in the processing of digital multimedia data is rapid, by the increasing demands of the content consumers with a widening variety of digital equipment's, require bit streams to be modified after transmission. A transcoder can be placed in the channel to reduce the bit rate prior to retransmission to end user devices [1],[2]. A simplified view of a typical broadcasting system is shown in Fig.1

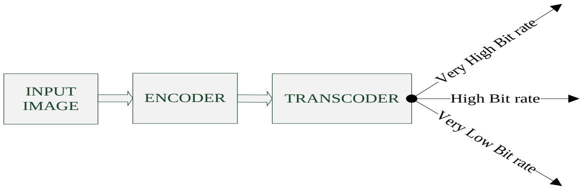

Fig.1: A potential broadcasting network

One of the challenges in using such network is protecting the intellectual property rights of the content owners and producers when the data is transmitted over a public channel. In traditional crypto system a secret key is used to encrypt and decrypt the data. There are two main drawbacks in using traditional crypto-systems to protect image data. First one is that the traditional systems are either too slow or in need of excessive complexity in real time operations with large volume of data. The second one is that any modification of the cipher text generated using on and off-the shelf cipher would render the resulting bit stream undecipherable. An intuitive approach is to allow the transcoder to decrypt the bit stream, prior to transcoding, re-encryption and retransmission, as shown in Fig. 2(a). While this approach is very effective in ensuring efficient content delivery, it does not allow end to end security.

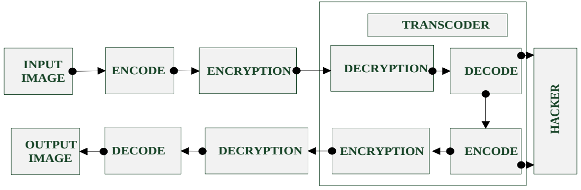

Fig.2 (a): Traditional transcoder with encrypted data

To ensure end to end security one of the possible approaches is shown in Fig.2 (b).Here transcoder stage is made such that no plain text is freely available in the intermediate stages of transcoding. For this purpose a decode and re-encode stage is used with different quantization values.

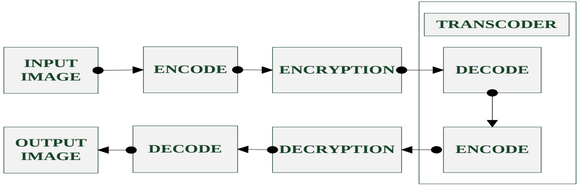

Fig .2(b): Secure transcoder using ciphers designed for transcoding

In this paper, we are implementing a secure image transcoder which is having too many multimedia applications such as medical imaging [3], mobile web browsing [4],[5], etc.

2. Literature survey

Transcoding is the process of manipulating an encoded bit stream with or without decoding it. Various types of transcoders exist that deal with different aspects of the sequence such as bitrate, spatial resolution, encoding standard etc. This paper mainly focuses on bitrate transcoding. Recently many papers have been proposed with the idea of stream ciphering. Generally encryption can be categorized into three viz complete encryption, selective encryption and joint encryption. In complete encryption entire data will be encrypted whereas in selective encryption only a part of data. Joint encryption refers to the encryption performed during compression. This paper uses Chaotic Key Based Algorithm (CKBA), complete encryption algorithm for security.

2.1. Image transcoder

In image transcoder, the picture size is changed and is used if the output resolution differs from the resolution of the media. It can also be done by re-encoding, particularly as a part of translating (such as a down sampled image requiring a lower bitrate).
Another important application is web browsing through mobile phones. The advantages of transcoding are the dynamic reduction in web downloading time over low-bandwidth links and reduction of per byte cost over tariffed links via data compression. Transcoding images in the internet improve delivery to client devices with a wide range of communication, processing, storage and display capabilities.

2.2. Chaotic Key Based Algorithm (CKBA)

In [6], a chaotic key-based algorithm (CKBA) for image encryption was proposed. It is a complete encryption technique. The encryption procedure of CKBA can be briefly depicted as follows. Assume the size of the plain-image is M × N. Shuffle the DCT matrix using the generated random key. It can be performed before or after the quantization stage. Incorporating a shuffling algorithm in the spatial domain can result an immense reduction in the compression ratio. Since, in most of the multimedia applications, the larger compression is a mandatory requirement, we cannot implement the shuffling algorithm in the spatial domain. Hence, performing the shuffling operation in the transform domain, without affecting the compression ratio is favourable. Thus, block-wise shuffling of DCT matrix is performed so that compression remains intact. Shuffling is performed based on a chaotic map. Assume that the size of the plain-image is M × N. Select an initial condition x(0) of a one-dimensional chaotic system as the secret key of the encryption system defined by the following logistic map (1).

$$x(n+1) = \mu * x(n)(1 - x(n)) \qquad (1)$$

It has been proved that the system behaves chaotically if the value of $\mu > 3.5699$. This chaotic system is run to make a chaotic sequence x(i) for I varying from 0 to (MN/8) − 1. It is then grouped into 8 bits to form an integer so that a pseudo random array of MN/64 integers is formed. By avoiding the repeating elements, it is possible to form an array of length 256. This array can be taken as an index to shuffle the columns of input DCT matrix. This system is a well encrypted system providing good compression by suitably selecting the quantization matrix.

3. Secure Image transcoder-(Proposed system)

The proposed secure image transcoder block diagram is shown in Fig.3. The system is basically a modification of the existing jpeg encoder- decoder algorithm. The main modifications are

3.1 Encryption
3.2 Transcoding

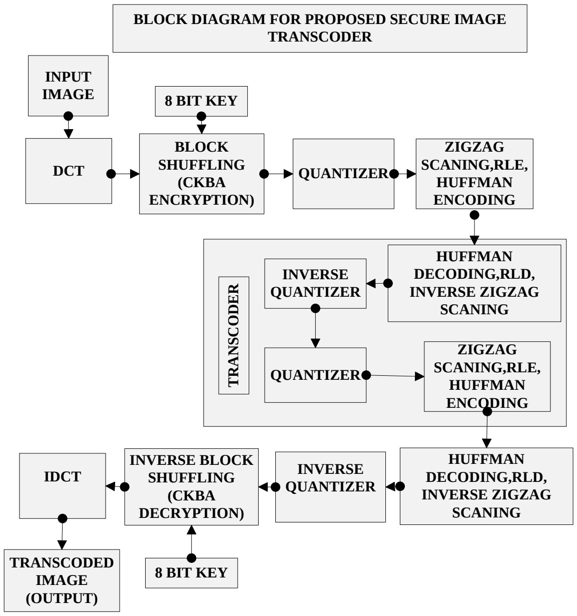
BLOCK DIAGRAM FOR PROPOSED SECURE IMAGE TRANSCODER
INPUT IMAGE
8 BIT KEY
DCT
BLOCK SHUFFLING (CKBA ENCRYPTION)
QUANTIZER
ZIGZAG SCANING,RLE, HUFFMAN ENCODING
TRANSCODER
INVERSE QUANTIZER
HUFFMAN DECODING,RLD, INVERSE ZIGZAG SCANING
QUANTIZER
ZIGZAG SCANING,RLE, HUFFMAN ENCODING
IDCT
INVERSE BLOCK SHUFFLING (CKBA DECRYPTION)
INVERSE QUANTIZER
HUFFMAN DECODING,RLD, INVERSE ZIGZAG SCANING
TRANSCODED IMAGE (OUTPUT)
8 BIT KEY

Fig.3: Block diagram for proposed secure image transcoder

3.1 Encryption

Normal JPEG algorithm is implemented with block shuffling using an 8 bit key generated by linear feedback shift register (LFSR) [7]. First the whole image is separated as small variable size blocks. Then each block is shuffled and zigzag scanned .The generated 8 bit pseudo random key is XOR with plain text bit by bit. So the randomness of 8 bit key destroys the statistical properties in the plain text. The reverse algorithm with same key can reconstruct the image.

3.2 Transcoding

In a transcoder, the first block is the decoder, which can be followed by another system, and the last one is the encoder. For now, we will restrict our scenario by assuming that no intermediate processing is done between decoder and encoder. Therefore, the goal is to achieve the same file as the original at the end of the encoder. One key issue that is still left to explain is why a regular decoding/ re-encoding process are lossy. The key here is the colour model conversion processes (YCbCr->RGB and RGB->YCbCr). They introduce some quantization, and so the decoding/re-encoding process is subject to the loss of quality.

For colour image transcoding algorithm, the RGB image is converted to YCbCr form and each matrix applied the jpeg algorithm with different quantization matrix. Then in the re-encoding stage, the quantization matrix is scaled in such a way that to get a compressed image. The transcoded image can be reconstructed by repeating the reverse process.

4 Results

For simulation we used 7 grey scale images and performed the secure transcoding. Results are shown in the tables 1-3. Also one cameraman image showing the secure image transcoding for grey images (Fig.4(a)) with quantization factor 2 and (Fig.4(b)) with quantization factor 10 . Colour image secure transcoder result is shown in Fig.5.

From the tables [1-3] it is clear that by changing the quantization values we will get better compression for the images. In these results, Table-1 shows the variation of compression ratio and average bit per image for different quantization values on camera man image. Before transcoding this image has a compression ratio of 13.0517 and average bit per image is 0.6129, after transcoding with quantizing with a factor of 2 the compression ratio changed to 20.1944 and average bit per image changed to 0.3961.

Table 2 shows the compression ratios of seven different test images for a quantization factor of 5 and table 3 shows the variations of average bits per image in these seven test images for the same quantization factor.

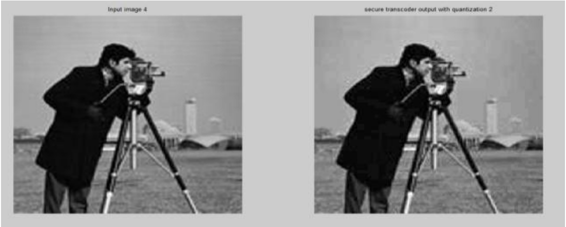

Fig. 4(a): secure transcoder for grey scale image with quantization value 2. Left image is the input cameraman test image and right most images is the output

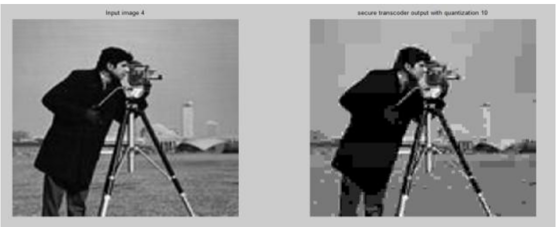

Fig. 4(b): secure transcoder for gray scale image with quantization value 10. Left image is the input cameraman test image and right most images is the output

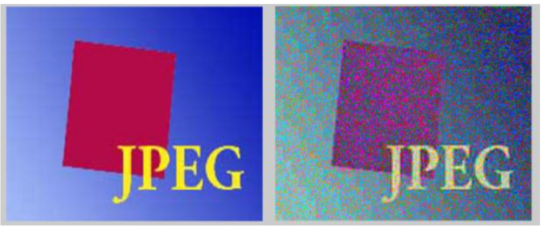

Fig.5: Secure image transcoder for colour image. Left image is the input test image colour image and right most images is the output

Table.1: Analysis of compression ratio and average bit per image with respect to various quantization values

Quantization factor	Compression ratio	Average Bit per image
1	15.0519	0.5315
2	20.1944	0.3961
3	25.2280	0.3171

4	28.9310	0.2765
5	32.2084	0.2484
10	45.1505	0.1772

Table.2: For different images: Compression ratio for quantization value 5

No	Name of the test image	Before Transcoding	After Transcoding
1	Lena	10.6856	27.5825
2	Washington dc band4	11.5829	31.6332
3	Woman blonde	9.2586	26.1987
4	Cameraman	13.0517	32.2084
5	Chest x-ray	24.3413	46.5289
6	Woman dark hair	13.4907	34.6019
7	Einstein high contrast	10.4172	28.7628

Table.3: for Different images: Average Bit per image for quantization value 5

No	Name of the test image	Before Transcoding	After Transcoding
1	Lena	0.7487	0.2900
2	Washington dc band4	0.6907	0.2529
3	Woman blonde	0.8641	0.3054
4	Cameraman	0.6129	0.2484
5	Chest x-ray	0.3287	0.1719
6	Woman dark hair	0.5930	0.2312
7	Einstein high contrast	0.7680	0.2781

5 Conclusion

Several Transcoding algorithms are already been examined for the effective utilization of bandwidth and user satisfaction. This paper gives the idea of how a high quality data like image can be securely transmitted to different environments with effective utilization of available bandwidth. From the results it is clear that, for transcoding we exploit the full efficiency of existing jpeg algorithm and gives better compression for different quantization values. Here we presented security in terms of CKBA.

References

[1] Nithin Thomas, David Redmill, David Bull, "Secure transcoders for single layer video data". Signal processing: image communication, pp, 196-207, 2010.

[2] Huafei Zhu ,"Adaptive and ComposableMulti-media ranscoders". Proceedings of the 3r IEEE International Conference on Ubi-media computing (U-media). 10.1109/UMEDIA.2010.5543914, pp, 113 – 117, 2010.

[3] Samit Desai, Usha b. "Medical image transcoder for telemedicine based on wireless communication devices", Proceedings of the 3rd IEEE International Conference on Electronics Computer Technology (ICECT). Vol.01, pp, 389 – 393, 2011.

[4] John r. Smith, Rakesh Mohan, Chung-Sheng li, **"**Content based transcoding of images in the internet", Proceedings of the IEEE International Conference on Image processing (ICIP98). Vol.03, pp, 7 – 11, 1998.

[5] Richard han, Pravin Bhagwat,Richard Lamaire, "Dynamic adaptation in an image transcoding proxy for mobile web browsing".IEEE Personal communications. Vol.05, issue: 6, pp, 8 – 17, 1998.

[6] Jui-Cheng Yen and Jiun-In Guo, "A new chaotic key-based design for image encryption and decryption", Proceedings of the IEEE International Conference on Circuits and Systems, vol. 4, pp. 49-52, 2000.

[7] M. Sahithi, B. MuraliKrishna, M. Jyothi, K. Purnima, A. Jhansi Rani, N. Naga Sudha." Implementation of Random Number Generator Using LFSR for High Secured Multi-Purpose Applications". M. Sahithi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (1), pp, 3287-3290,2012.

Anoop B N received the B.Tech degree in Electronics and Communication Engineering from College of Engineering Munnar, under the Cochin university of Science and Technology (CUSAT), Kochi (Cochin), Kerala, India, in 2007. Since 2008, he has been with St. Josephs College of Engineering and Technology, Palai- Kerala as Assistant Professor in the department of electronics and communication engineering. He is currently doing M.Tech degree in signal processing from NIT-Calicut, Kerala, India.

Sudhish N George received B.Tech Degree in Electronics & Communication Engineering from M.G University, Kerala, India, in 2004, M.Tech Degree in Signal processing from Kerala university, India, in 2007, Doing Ph.D in National Institute of Technology Calicut in the field of multimedia security. He is working as Assistant Professor in Department of Electronics and Communication, National Institute of Technology Calicut from 2010 onwards. His current interests include Signal Processing, Multimedia Security and Embedded System Design.

Deepthi P.P. received B.Tech Degree in Electronics & Communication Engineering from N.S.S.College of Engg, Palakkad (Calicut University) in 1991, M.Tech Degree in Instrumentation from Indian Institute of Science, Bangalore in 1997. Ph.D from National Institute of Technology Calicut in the field of Secure Communication. She has been working as Faculty in institutions under IHRD, Thiruvanthapuram from 1992 to 2001 and in the Department of Electronics & Communication Engineering, National Institute of Technology Calicut from 2001 onwards. Her current interests include Cryptography, Signal Processing with Security Applications, Information Theory and Coding Theory.