Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.720 – 723

RESEARCH ARTICLE

Multi View Compressed Images Based On Distributed Coding Scheme

Kattera Srinivasa Rao[1], Bangaru BalaKrishna[2]

[1]M.Tech 2ndYear, Dept. of CSE, TITS, JNTU, HYDERABAD, INDIA

[2]Asst Professor, Dept. of CSE, TITS, JNTU, HYDERABAD, INDIA

[1] srinivas.kattera@gmail.com; [2] balakrishna.bangaru@gmail.com

Abstract - Joint reconstruction is a process in which the compressed and encrypted image can be reconstructed sequentially. This paper analyses various methods of joint reconstruction techniques and its performance. The main objective is to provide security through encryption and efficiency via compression. These are normally applicable in secure medical image sharing system. In this paper, Prediction error clustering and random permutations can be exploited to encrypt the images. Then an arithmetic coding based approach is proposed for compressing the encrypted images. To recover the original image, joint reconstruction is applied. Theoretical result shows that reasonably high level of security has been attained. By using this approach, the compression efficiency obtained is close to that of state-of-the-art lossless/lossy image codec.

I. Introduction

In recent years, the cryptography technique provides a great help to satisfy the security requirements in variety of applications such as medical image sharing and army security system. Consider the problem of transmitting the data over an untrusted channel provider. The traditional method of accomplishing this is shown in Fig.1. In traditional method, initially input image is compressed for redundancy and encrypted to provide security. At the receiver side, decryption and decompression operations are performed. Even though the above compression and then encryption technique meets the requirements, the process is reversed in some situations. If the content owner is in need to protect privacy through encryption, then the proposed scheme is efficient to utilize all the computational resources.

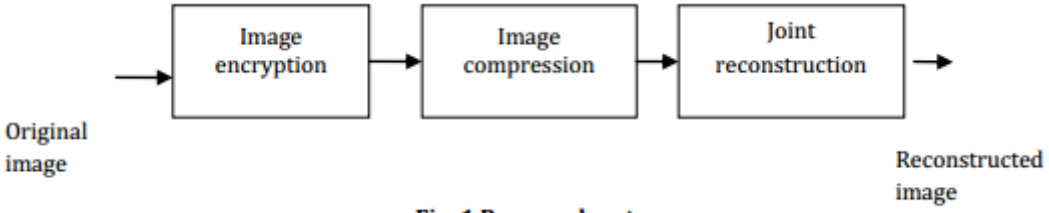

Fig: 1 Proposed system

II. Image Encryption

Image encryption is a process of representing a particular image in hidden format for the purpose of providing security. It includes privacy or confidentiality, data integrity, authentication, authorization, validation, access control, certification, time stamping, witnessing, confirmation, ownership and revocation. Fig.2. shows the encrypted image. Image encryption is conducted for the purpose of providing security and ease of compressing the data. The proposed method uses prediction error clustering and random permutation technique

Figure 2: Image Encryption

Stream cipher:

It factors the larger encryption process into smaller one. It is constructed by mapping the source into Cipher text using key k. Here the variables used are hidden and hence it needs to estimate observed quantities.

Compressed sensing:

Plain text is encrypted into cipher text using key k. In compressed sensing, key is shared by transmitter and receiver. It is assumed that the posterior probabilityof the plain text is same as that of the priori probabilities of the cipher text.

Pailler cryptosystem:

Pailler cryptosystem depends on whether the number is an N-th residue modulo N2. This calculation is computationally hard. It is a homomorphismcryptosystem. Hence it allows us o do multiplications through addition.

Wyner-sense:

In Wyner-Ziv encryption, the block length consists of a secret codebook, an encoder map and a decoder map. The set of Wyner-Ziv cryptosystem is said to have Wyner-sense perfect secrecy.

Prediction error clustering:

Each predicted pixel is grouped based on the nearest closet. Then for each cluster, permutation is performed using key k. Mapping is used to reduce the range of pixels. This is an efficient encryption technique in terms of security.

III. Image Compression

Compression is a process of reducing the number of bits required to represent the particular image. It provides efficiency during data transmission. Fig.3. shows the compressed image. It consists of three components, namely, De-Assembler, encoder, Assembler.

FIGURE 3: Image Compression

Transform coding:

Fourier transform such as discrete cosine transform or discrete wavelet transform is used for compressing the image. It includes quantization and permutation. This is a common method used in most of the application.

Chroma sub sampling:

It average or drops some chrominance information from the image. By using this human eye perceives changes of brightness than colour.

Reducing the colour space:

Each pixel refers the index of colours from the colourpalette. The colour palette contains a header which refers specified colours. Pasteurizations can be avoided with the help of dithering

Linear codes:

Linear codes use an inference algorithm and factor graph. It is based on the calculation of posterior distribution. It achieves good performance in term of computational cost. It works by passing messages between graphs.

Adaptive arithmetic coding:

In adaptive arithmetic coding random permutation is applied. This random permutation will not change values of prediction error but it changes the location. It implies that the probability mass function of prediction error sequence needs to be preserved.

IV. Joint Reconstruction

Distributed source coding paradigm is used to jointly reconstruct the original images. The original images are needed to be recovered in the receiver side. For the compressed encrypted images, it is necessary to perform decompression and decryption. Initially the compressed image is divided into clusters using De-assembler.

V. Security and Performance Analysis

In our proposed method, the permutation key is generated by stream cipher. Here, key generated for the same image will vary by time. It is vulnerable to cipher-text only attack.

In, DFT is implemented over an encrypted image based on homomorphism properties. Due to the complexity involved in computation, radix-4 FFT is best suited. This approach is efficient when it is unfeasible and is inefficient when it is feasible.

In, the application of the DCT to digital images encrypted with the help of homomorphism cryptosystem is considered. It is preferable to employ an BDCT, since this will reduce the bandwidth at the cost of a small increase in complexity.

In, very large algebraic structures are considered to convert plain text into encrypted signals due to the use of pailler cryptosystem. Simpler processing algorithm allows packing more samples than existing system.

Designing an efficient protocol which allows us to pass the sample-wise representation without sharing any secret information is considered as an open problem.

VI. CONCLUSION

In this paper, we analyzed an efficient image encryption system. In this proposed methodology, the image encryption is obtained by using prediction error clustering and random permutation. The compression efficiency is high with the help of arithmetic coding approach. To recover the original reconstructed images, sequential decryption and decompression methods are used. Our proposed scheme is efficient in terms of compression and encryption.

REFERENCES

[1] J. Zhou, X. Liu, and O. C. Au, "On the design of an Efficient Encryption then- compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
[2]T. Bianchi, A. Piva, and M. Barni, "On the implementation Of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar.2009.
[3]T. Bianchi, A. Piva, and M. Barni, "Encrypted Domain DCT based on homomorphismcryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357.
[4] T. Bianchi, A. Piva, and M. Barni, "Composite Signal representation for fast and storage-Efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.
[5] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T.Schneider, "Privacy- preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security

