

Joint Reconstruction of Multiview Compressed Images Based on Distributed Coding Scheme

Authors: P. Jancy Malar¹; A. Vinotha Vasuki²

Affiliation: PG Research Scholar¹; Assistant Professor²

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.

Keywords

Image encryption, Compression system, Secure signal processing, Cryptography, Source coding.

1. 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.

The opportunity of proceeding encrypted images directly in the encrypted field has been obtaining a great attention in recent years. To achieve higher

compression ratios, a compressive sensing (CS) mechanism was utilized in [15]. To estimate the original image from the compressed and encrypted data, a modified form of pursuit algorithm can be applied. A different CS based method intended for encrypting compressed data was accounted in [16]. Moreover, Zhang proposed an image encryption system by means of pixel-domain permutation, and showed that the encrypted file can be compressed by removing the extremely coarse and fine sequence of coefficients in the transform domain [17].

Although extensive attempts in current years, the existing ETC approach still drop significantly small in the compression results, compared with the state-of-the-art lossless video and image coders that requires unencrypted data as an input. The main goal of this paper is on the design of a image encryption and compression schemes, in which compressing the processed digital images is almost equally efficient as compressing their original, unencrypted equivalents. Temporarily, high level of security needs to be guaranteed. If not otherwise specified, 8-bit grayscale images are assumed. Both lossless and lossy compression of encrypted images will be considered. Particularly, we suggest a permutation-based image encryption technique accomplished in the prediction error domain. A context-adaptive arithmetic Coding (AC) is exposed to be able to effectively compress the encrypted data.

2. 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, timestamping, 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.

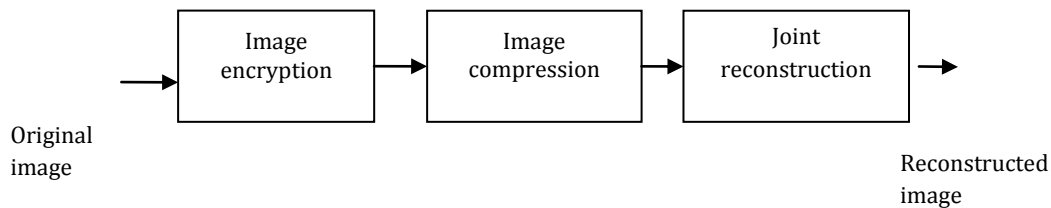


Fig: 1 Proposed system

The input image I is initially processed by means of image predictor; e.g. GAP [11] or MED [12]. Then the prediction error is calculated by

$$e_{i,j} = I_{i,j} - \bar{I}_{i,j} \tag{1}$$

For a eight-bit image prediction, it takes values from -255 to 255. The possible prediction errors are mapped in the range of [0, 255]. Then the mapped prediction errors are divided into L clusters. Permutation is performed to each cluster using two key-driven cyclic shift operations. Assembler concatenates all the permuted clusters \bar{C}_k . The encrypted image is calculated by

$$I_s = \bar{C}_0 \bar{C}_1 \dots \bar{C}_{L-1} \tag{2}$$

in which each prediction error is characterized by 8 bits. As the number of prediction errors equals that of the pixels, the file size before and after the encryption conserves.

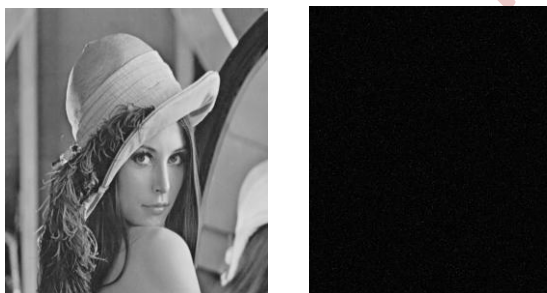


Fig 2: Image encryption

2.1 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.

2.2 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 probability

of the plain text is same as that of the priori probabilities of the cipher text.

2.3 Pailler cryptosystem:

Pailler cryptosystem depends on whether the number is an N -th residue modulo N^2 . This calculation is computationally hard. It is a homomorphic cryptosystem. Hence it allows us to do multiplications through addition.

2.4 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.

2.5 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.

3. 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. De-assembler splits the encrypted image I_s into L clusters. For each cluster encoding is performed using Arithmetic coding based approach. Then the assembler concatenates all the encoded clusters into a group. The compressed image is calculated by

$$B = B_0 B_1 \dots B_{L-1} \tag{3}$$

The length of the resulting compressed bit stream can then be computed by

$$L_c = |B| + (L - 1)[\log_2 |B|] \tag{4}$$

where $|B|$ is calculated by bits, and the second term indicates the overhead produced by the side information $|B_k|$, for $0 \leq k \leq L - 2$.

3.1 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.

3.2 Chroma subsampling:

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

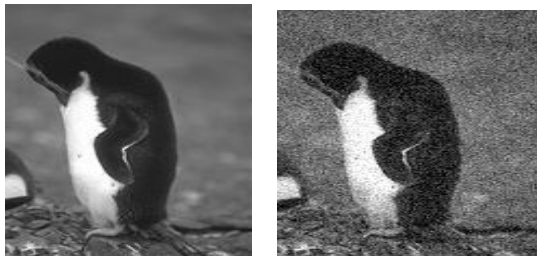


Fig: 3 Image compressions

3.3 Reducing the color space:

Each pixel refers the index of colors from the color palette. The color palette contains a header which refers specified colors. Posterization can be avoided with the help of dithering

3.4 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.

3.5 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.

4. 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 decompression and decryption. Initially the compressed image B is divided into clusters using De-assembler. Then de-arithmetic coding and de-permutations are performed. Now the image is having some prediction values. These values are estimated by error energy estimator $\Delta_{i,j}$. The reconstructed image is computed by,

$$\hat{I}_{i,j} = \bar{I}_{i,j} + e_{i,j} \tag{5}$$

where, $\bar{I}_{i,j}$ is the predicted value and $e_{i,j}$ is the prediction error. In case of lossless compression, $\hat{I}_{i,j} = I_{i,j}$ i.e. error free coding can be achieved.

5. SECURITY AND PERFORMANCE ANALYSIS

In our proposed method, the permutation key is generated by stream cipher [23]. Here, key generated for the same image will vary by time. It is vulnerable to cipher-text only attack.

In [2], DFT is implemented over an encrypted image based on homomorphic 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 [3], the application of the DCT to digital images encrypted with the help of homomorphic cryptosystem is considered. It is preferable to employ an s.p.e.d BDCT, since this will reduce the bandwidth at the cost of a small increase in complexity.

In [4], very large algebraic structures are considered to convert plain text into encrypted signals due to the use of pailler cryposystem. 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.

Table 1: Comparison results of encryption approaches

Approach	References	Pros	Cons
Stream cipher encryption	[19]	Perfect secrecy	Less efficient
Pailler cryptosystem	[2], [3], [4]	Protection from malicious processing device	Less tradeoff between feasibility and complexity
Distributed source coding	[9], [11]	Perfect secrecy	Not applicable in most of the cases

Table 2: Compression performance

Approach	Images	Bits per pixel
CALIC	Lena	4.096
	Peppers	4.394
	Gold hill	4.604
Clara	Fax balls	0.820
	Hotels	3.880
	Gold	3.880
L_{∞} constrained image coding	Farmland	4.001
	Highway	3.883
	Sea bay	3.962
Jpeg	Air2	4.900
	Bike	4.330
	Café	5.630
Felicis	Tools	5.420
	Woman	4.580
	Cats	3.300
Alcm	Water	1.820
	Chart	1.270
	Graph	2.410
Adaptive arithmetic coding	Boat	4.112
	Man	4.346
	Harbor	4.900

In [9], encrypted data can be compressed using distributed coding scheme and it doesn't have the knowledge of encryption key. The computational resources are available for the attacker and hence it has the possibility to break the encryption scheme.

In [11], lossless compression of encrypted gray-level and color images are investigated. YCbCr domain is used for the color images and xor-based algorithm can be proposed. It is applicable only if the lower

encrypted bit planes are needed to be removed to reduce the bit rate.

In [12], LDPC based compression with stream cipher and distributed coding scheme is implemented. 1-D, 2-D Markov models and blind compression provides significance performance. If there is a situation in which it is difficult to compress the least significant bit planes then it is less significant.

In [13], higher lossless compression can be achieved using context based, adaptive, lossless image codec (CALIC). Initially GAP predictor predicts pixel values. From the predicted pixels coding context is selected and then quantization can be applied.

In [14], L_{∞} -constrained image coding technique is proposed to achieve lower bit rate in lossless image coding. To reduce the L_2 distortion of L_{∞} -coded images, it will depend on soft decoding approach. By using this approach higher PSNR can be achieved.

6. 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.

7. 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 homomorphic cryptosystems," 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,

vol. 6, pp. 452–468, Jun. 2011.

- [6] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.
- [7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
- [8] D. Schonberg, S. C. Draper, and K. Ramchandran, "On approaching the source entropy rate," in *Proc. 43rd Annu. Allerton Conf.*, 2005, pp. 1–3.
- [9] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2006, pp. 269–272.
- [10] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.
- [11] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in *Proc. 16th Eur. Signal Process. Conf.*, Aug. 2008, pp. 1–5.
- [12] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in *Proc. MMSP*, 2008, pp. 760–764.
- [13] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Imag. Process.*, vol. 19, no. 4, pp. 1097–1102, Apr.
- [14] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Imag. Process.*, vol. 21, no. 6, pp. 3108–3114, Jun. 2012.
- [15] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in *Proc. IEEE Region 10 Conf. TENCN*, Jan. 2009, pp. 1–6.