An Evaluation on Irretrievable Compression of Encrypted Image

K.Porkumaran S.Manimurugan Pradeep P Mathew

ABSTRACT
This paper may deals with the diverse troubles that may be occurs during the irretrievable compression applied on an encrypted image. This work is a relative learn with different methods of irretrievable compression such as Compressive sensing technique and Iterative reconstruction technique on encrypted image. But they practiced a variety of limitations. The major obscurity is to attain a higher compression ratio as well as the better quality of the reconstructed image. The higher compression ratio and the smoother the original image may supply the better quality of the reconstructed image.

Keywords
Image compression, image encryption, image decryption, image decompression, image reconstruction.

1. INTRODUCTION
Compression of encrypted image has attracted in the recent years with great research interest. To reduce redundancy first compress the image then encryption is applied to the compressed image is the traditional method of securely transmitting the image[1]. The decryption operation as well as the decompression operation may be performed at the receiver side to obtain the reconstructed image. In case of some applications, some data needs to transmit from sender to receiver and keeps the information confidential to a network operator. So sender should encrypt the original image and the network provider may compress the encrypted image without any knowledge regarding the original data. Decompression as well as decryption may be performed to reconstruct the original image.

Compressive sensing is an emerging area, which gained a lot of interest due to its ability to reconstruct the sparse signal from relatively smaller sample set[2]. This may provides a new method of signal compression whose particular application is the irretrievable compression of encrypted data. Compression as well as the encryption is necessary while an image is transmitting over insecure bandwidth limited channel. Comprehensible structure of the image may be converted to incomprehensible structure by an encryption technique, which makes the encrypted image difficult to perform compression by using any simple classical compression algorithm. But the network operator is forced to compress the encrypted image due to the limitation of bandwidth.

For such scenarios to compress the data, proposed methods are based on distributed source encoding (DSC) [3]. Since the encryption key is known at the decoder, DSC exploits the correlation between the encryption key and encrypted data. In this case, correlation such as statistics of the information source affected the compression efficiency. Correlation can be modeled by a binary symmetric correlation, while [4] the binary image is assumed to be sparse. To improve the compression efficiency, higher memory models [5] were used to model correlation. Since good compression does not achieve by extending these to gray scale images and hence [6] propose to apply encryption on the prediction errors follow a Laplacian density function to achieve good compression along with good security. Good compression can be obtained, since the prediction errors follow a Laplacian density function.

On the basis of theory of source coding with the side information at the decoder, the performance of compressing encrypted data is similar [15] that of nonencrypted data. Lossy compression of encrypted Gaussian sequence is presented in [16]. The original binary image is encrypted by adding pseudorandom string and with respect to low-density parity-check (LDPC) channel code [17], the encrypted data are compressed by finding the syndromes. Using LDPC codes, for both memory less sources and sources with hidden [18] Markov correlation are studied. In [19], a few methods are introduced for lossless compression of encrypted color and gray images. In a progressive manner, the encrypted image is decomposed in [20] and the most significant bits in high levels are compressed using rate-compatible punctured turbo codes. Some algorithms for compressing encrypted data and demonstrate blind compression of encrypted video are presented in [21]. In the encryption domain, the signal processing using homomorphic calculation is discussed in [22] and [23].

2. COMPRESSIVE SENSING TECHNIQUE ON ENCRYPTED IMAGE
Compressive sensing technique is one of the irretrievable compression method developed on the encrypted image to overcome the problems that faced on this area. This technique is introduced to achieve lossy compression on encrypted image and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. The encryption is applied on the image in the spatial domain and which is performed by some linear operation. At the encoder, the image is not required to be transformed and transformation basis is only required at decoder. The compressed sensing encoded data itself is very secured [7] because of which information owner can relax his own security requirements.

2.1 Image Encryption
Cipher text can be generated by using a linear process on the image pixels. An encryption matrix is used to represent the linear process operation which generates some random seed.

Cipher text is generated by applying encryption on the image in the spatial domain. The image can be converted into a single column vector. Snake pattern is followed to vectorize the image, which improves compression efficiency. Encryption is applied upon single column vector by a linear transformation of the pixels to obtain the cipher text. A permutation matrix is a binary matrix that obtained by randomizing the rows of an identity matrix. The index for this randomization can be generated with an initial random seed by pseudo random index generator, shared to the decoder by a secured channel. Permutation based linear encryption techniques can be referred in [12]. Spectral permutation based encryption system for speech encryption may described in [13]. Hadamard transform can also be used in the encryption stage [14]. Encryption procedure can be represented by a linear transformation matrix.

2.2 Compression

Compressing sensing technique is used for the compression of cipher text. The encryption matrix is unavailable at the compressor while the compressor receives the encrypted data. Random measurements are computed by projecting the encrypted data onto the Gaussian random measurements basis F of size M x N at the compressor. Compression is achieved since the number of measurements M < N. Compression ratio as well as the reconstruction performance decided by the factor M the number of measurements. It is very difficult to calculate M, since the original image is unavailable at the compressor and it depends on the sparsity factor. The sparsity may be adjusted by transforming and making the coefficients to go to zero which is impossible in this case due to the unavailability of original image. So M is choose for a given target bit rate. The decoder will estimate the sparsity factor which depends on the value of M. The quality of the image reconstruction is enhanced by higher values of M, which enables more coefficients.

A second level of security can be provided by the compressive sensing technique along with compression. The measurement matrix cannot be generated exactly without the access to the random key. Without the access to the actual measurement matrix, computationally it is impossible to decode properly as shown [7]. This reduce the encryption time which helps the information owner to relax his security requirements of the encryption function. The sampled values was quantized by a Lloyd quantizer for a given bit rate and that was transmitted to the decoder. The final bit rate is a function that depends on both the quantization levels and the number of measurements. To obtain best performance , target bit rate a trade off is required between the quantizer levels and M. It is difficult to optimize the cost function involving the quantizer levels and M with final rate, since the original image is unavailable at the encoder. At lower quantization levels, both sparse location estimation accuracy and spare signal amplitudes depends on the quantization noise. The effect of quantization noise become negligible and quality of image reconstruction depends only on the factor M while the quantization level increases beyond a certain level. Fix the number of quantization levels and only vary M for a given bit rate to obtain a good performance.

2.3 Image Reconstruction

The compressed data stream received from a public channel along with keys from a separate secure channel at the decoder. The exact matrices will be generated with the help of these keys. Image reconstruction process may involve both decompression and decryption. Here decoding based on basis pursuit, since it performs better than existing algorithms. Greedy based algorithms are computationally efficient is direct and easy. The modified optimization problem is solved to recover the sparse signal, as it's the first step of joint decoding. The whole of the of the image of block size N was considered to be encoded and decoded in this sensing technique. Dimension N increases with the increase in reconstruction performance [9]. $O(N^3)$ is the computational complexity of solving decoding. Thus there exist a swapping between performance and complexity. The data can be divided into smaller blocks and encoding and decoding is performed on each of the smaller blocks to reduce the computational complexity.

3. ITERATIVE RECONSTRUCTION TECHNIQUE ON ENCRYPTED IMAGE

Lossy Compression and iterative reconstruction technique is a novel system for irretrievable compression of encrypted image with flexible compression ratio, which can be obtained by image encryption, tailor-made compression and iterative decompression phases[2]. Redundant and trivial data may be removed by the network provider and iterative procedure may be used to retrieve the principal content of the original image. Compression parameters are the important factors that affect the compression ratio as well as the quality of the reconstructed image. The better quality of reconstructed image can be achieved by higher compression ratio as well as smoother the image. With a slight degradation of encryption security and reconstruction quality, improve the compression efficiency.

A pseudorandom permutation is used to encrypt an image and then by discarding the excessively rough and fine information of coefficients in the transform domain to compress the encrypted data. The receiver have the compressed data as well as the permutation way, with the aid of spatial correlation in natural image. By iteratively updating the values of the coefficients, the receiver can reconstruct the principal content of the actual image.

3.1 Image Encryption

In [23] and [24], there are a number of permutation-based image methods used. The original image should be in uncompressed format and each pixel have a gray value which may be between 0 and 255 , and that can be represented by 8 bits. Total number of pixels is the product of number of rows and number of columns and the total number of bits is the product of total number of pixel and 8. The data sender pseudorandomly permutes the total number of pixels for the image encryption and by the help of secret key, the permutation way is determined. The pixel-sequence can be shown as encrypted data. In the encryption phase, the pixel values are not masked and only the pixel positions are permuted. The attacker cannot recover the original content from the encrypted image with ordinary size and fluctuation. The permutation-based encryption can be used in most scenarios without a requirement of perfect secrecy although there is a leakage of statistical information.

3.2 Compression of encrypted image

A majority of pixels are converted to a series of coefficients using an orthogonal transform in the compression stage. To reduce the data amount, the excessively rough and fine information in the coefficients is removed. The network provider divides the permuted pixel sequence into two parts. The first part is called rigid pixels, which is made up of a set of pixels. The remaining pixels are called elastic pixels, which

is the second part. This classification of pixels may be depends on a variable whose value is within zero and one. To calculate the coefficients, orthogonal transform is performed in the elastic pixels. Public orthogonal matrix can be generated by othogonalizing a random matrix. Calculate the s_k value [1] for each coefficient where M is the system parameter the values can be assigned for the purpose of implementation. Mod operation as well as round operation may perform here whereas the round operation returns the nearest integer and the mod operation gets the remainder. The data amount for representing the elastic pixels are reduced within a small M. The fine information as well as the rough information is discarded and the information on the medium level only remains. The loss of the fine information cannot affect the quality of the reconstructed image seriously and an iterative reconstruction procedure will be used to retrieve rough information. Consider the values of s_k as a set of digits in a notational system with a base M, since its value is within zero and M-1. The set of s_k is segmented into many pieces with L_1 digits and calculated the decimal value of each digit piece. Each decimal value is converted into L_2 bits in a binary notation system. The data of rigid pixels, the bits generated from all pieces of s_k and the values of different parameters are collected to produce the compressed data of encrypted image. The compression ratio is the ratio between the amounts of the compressed data and the original image data is calculated, which may depends only on the value of M and the value of the variable used to classify pixels into rigid and elastic, since the data amount of parameters is small.

3.3 Image Reconstruction

A receiver can reconstruct the principal content of the original image with the compressed data and the secret key. Obtain the gray values of rigid pixels, the values of each s_k, and the values of all the parameters by decompose the compressed data. Receiver can calculate L_2 with the knowledge of M and L_1 and by converting binary blocks with L_2 bits into digit pieces in an M-ary notational system to get the values of s_k. Then the receiver can retrieve the positions of the rigid pixels, according to the secret key. The original gray values at the positions can be exactly recovered, which distribute over the entire image.

The values of the elastic pixels are estimated as the values of rigid pixels nearest to them. We can find the nearest rigid pixel for each elastic pixel and regard the value of rigid pixel as the estimated value of the elastic pixel. Consider the average value as the estimated value of the elastic pixel, if there are several nearest pixels with the same distance. The estimated values are similar to the corresponding original values due to the spatial correlation in the natural image. By exploiting the information of s_k, the estimation will be iteratively updated. Calculate the coefficients by rearranging the estimated values of elastic pixels using the same permutation way. Modify the coefficients to the closest values consistent with the corresponding s_k and perform inverse transform. The average energy difference between the two versions of elastic pixels can be calculated. If the average energy difference is not less than given threshold, for each elastic pixel, compare the average value of its four neighbor pixels as its new estimated value. Otherwise terminate the iteration process and output the image made up of the rigid pixels and the final version of elastic pixels as a reconstructed image.

The relative study of irretrievable compression methods such as Compressive sensing technique and Iterative reconstruction technique of encrypted image, on the basis of various parameters such as Compression Ratio, PSNR value, Resolution, Complexity and the quality of the image is represented as follows.

Table 1. : Comparison of the irretrievable compression methods on encrypted image.

	Comprehensive Sensing Technique	**Iterative Reconstruction Method**
Compression Ratio	Low	High
PSNR Value	High	High
Resolution	----	Good
Complexity	High	Low
Quality	Poor	Good

4. CONCLUSIONS

In this paper we discussed about diverse irretrievable compression techniques on the encrypted image. We have considered the difficulty of irretrievable compression of encrypted image data. The practice of classical compression techniques is unfeasible for the compression of encrypted image. Compression sensing technique helps to realize lossy compression on encrypted image, where a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. The encryption is functional on the image in the spatial domain and which is performed by some linear operation. At the encoder, the image is not required to be altered and transformation basis is only required at decoder. This compression technique provides a better compression ratio where as the quality of the reconstructed image is not considered. Lossy Compression and iterative reconstruction technique helps to accomplish irretrievable compression of encrypted image with flexible compression ratio, which can be obtained by image encryption, tailor-made compression and iterative decompression phases. Redundant and trivial data may be detached by the network provider and iterative procedure may be used to recover the principal content of the original image. This technique provides higher compression ratio as well as the better quality of reconstructed image but the security of encryption is weaker. In the future, the irretrievable compression of image encrypted by more secure methods will be studied.

5. ACKNOWLEDGMENTS

The authors would like to thank the reviewers for their valuable comments.

6. REFERENCES

[1] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Images," *IEEE Trans. Information Forensics and Security.*, Vol. 6, No. 1, pp. 53-58, Mar. 2011.

[2] A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," *in Proc. IEEE Region 10 Conf. (TENCON 2009)*, 2009, pp. 1–6.

[3] Z. Xiong, A. D. Liveris and S. Cheng, "Distributed source coding for sensor networks", *IEEE Signal Processing Magazine,* Vol. 21, pp. 80-94, Sep. 2004.

[4] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramachandran, ”On compressing encrypted data”, *IEEE Trans. Signal Processing* Vol. 52, pp. 2992-3006, Oct. 2004.

[5] D. Schonberg, S. Draper and K. Ramachandran, ”On compression of encrypted images”, *Proc. International conference on Image processing, Atlanta, GA*, pp. 269-272, Oct. 2006.

[6] A. Kumar and A. Makur, ”Distributed source coding based encryption and lossless compression of gray scale and color images”, *Proc. IEEE 10th workshop on multimedia and signal processing, Cairns, Australia*, pp. 760-764, Oct. 2008.

[7] Y. Rachlin and D. Baron, ”The secrecy of compressive sensing measurements”, *Proc. 46th Allerton conference on commun., control, and computing, Monticello*, IL, Sep. 2008.

[8] E. J. Candes and M. B. Wakin, ”An introduction to compressive sampling”, *IEEE signal processing magazine,* Vol. 25, pp. 21-30, Mar. 2008.

[9] S. S. Chen, D. L. Donoho, and M. A. Saunders, ”Atomic decomposition by basis pursuit”, *SIAM J. Sci. Comput*., Vol. 20, No. 1, pp. 3361, 1988.

[10] R. Baranuik, ”Compressive Sensing”, *IEEE signal processing magazine,* Vol. 24, pp. 118-120, July 2007.

[11] A. M. Bruckstein, D. L. Donoho and M. Elad, ”From sparse solutions of systems of equations to sparse modeling of signals and images”, to appear in SIAM review.

[12] A. Mitra, Y. V. S. Rao and S. R. M. Prasanna, ” A new image encryption approach using combinational permutation techniques*”, International J. of comp. Sc.,* Vol. 1, pp. 127-131, May 2006.

[13] S. Sridharan, E. Dawson and B. Goldburg, ”Fast Fourier transform based speech encryption system”, *IEE Proceedings - I,* Vol. 138, pp. 215-223, June 1991.

[14] Y. Wu and B. P. Ng, ”Speech scrambling with hadamard transform in transform domain”, *Proc. 6th International conference on signal processing*, pp. 1560-1563, Aug. 2002.

[15] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” *IEEE Trans. Signal Process.,* Vol. 52, No. 10, Pt. 2, pp. 2992–3006, Oct. 2004.

[16] R. G. Gallager, “Low Density Parity Check Codes,” *Ph.D. dissertation, Mass. Inst. Technol.*, Cambridge, MA, 1963.

[17] D. Schonberg, S. C. Draper, and K. Ramchandran, “On blind compression of encrypted correlated data approaching the source entropy rate,” in *Proc. 43rd Annu. Allerton Conf., Allerton, IL,* 2005.

[18] R. Lazzeretti and M. Barni, “Lossless compression of encrypted grey-level and color images,” *in Proc.16th Eur. Signal Processing Conf. (EUSIPCO 2008), Lausanne, Switzerland*, Aug. 2008 [Online] Available: http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/pap-ers/1569105134.pdf

[19] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” *IEEE Trans. Image Process.,* Vol. 19, No. 4, pp. 1097–1102, Apr. 2010.

[20] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” *IEEE Trans. Image Process.,* Vol. 19, No. 4, pp. 1097–1102, Apr. 2010.

[21] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, “Toward compression of encrypted images and video sequences,” *IEEE Trans. Inf. Forensics Security,* Vol. 3, No. 4, pp. 749–762, Dec. 2008.

[22] 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.

[23] J.-C. Yen and J.-I. Guo, “Efficient hierarchical chaotic image encryption algorithm and its VLSI realization,” *Proc. Inst. Elect. Eng., Vis. Image Signal Process.,* Vol. 147, No. 2, pp. 167–175, 2000.

[24] N. Bourbakis and C. Alexopoulos, “Picture data encryption using SCAN patterns,” *Pattern Recognit.*, Vol. 25, No. 6, pp. 567–581, 1992.