Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 25 (2016) 60 – 67

Procedia Technology

Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016)

Efficient Compression of Secured Images using Subservient Data and Huffman Coding

Kasmeera K S[a]*, Shine P James[a], Sreekumar K[b]

[a]*College of Engineering Poonjar,Kottayam, Kerala, 686582, India*
[b]*College of Engineering Cherthala, Kerala, India*

Abstract

While transmitting redundant data through an insecure and bandwidth limited channel, it is mandatory to encrypt and compress it. Generally encryption is followed by compression as the statistical properties of encrypted images are not suitable for applying conventional compression schemes. The problem is that many situations demand the reverse procedure. This paper proposes a scheme of compressing encrypted data with the help of a subservient data and Huffman coding. For encrypting the original image, it is manipulated with a pseudorandom number sequence generated using a secret key. The subservient data is also created by the content owner. The encrypted data is then compressed using a quantization mechanism and Huffman coding. For quantizing the image the subservient data produced by the content owner is used. The quantized values are then coded using Huffman coding. At the reconstruction side the principal content of the data is reconstructed. Experimental results show that the compression ratio distortion performance of this method is superior to the existing Techniques. The compression ratio of encrypted image is improved to the range 10 to 20.

Peer-review under responsibility of the organizing committee of RAEREST 2016

*Keywords:*Image encryption;Image compression; Compression ratio-distortion performance

1. Introduction

Nowadays multimedia, computers and networks have a big influence in our lives. Especially the internet is becoming highly important for nearly everybody. The security and protection of the data has become an important

* Tel.: 9497285037;
*E-mail address:*kasmeera290@gmail.com

Peer-review under responsibility of the organizing committee of RAEREST 2016
doi:10.1016/j.protcy.2016.08.081

issue. There are several schemes for performing the encryption and compression of image. Generally, compression is followed by encryption as the conventional compression schemes cannot be applied in the encrypted image. However there are situations where encryption followed by compression is preferred. Consider for example a data distribution scenario where the content owner and the network operator are two separate entities, and do not trust each other. If the content owner is interested to protect the privacy of the data through encryption, the network operator is forced to compress the encrypted data. Encrypted image is purely random in nature and does not contain any kind of redundancies. Thus compression of encrypted images is not up to that of natural images. This paper deals with a scheme of compressing encrypted images using subservient data and Huffman coding. In encryption phase, the content owner performs the encryption of original uncompressed image, and subservient data is also created when the channel bandwidth is not enough. In compression phase, a quantization mechanism is used to compress the encrypted data in various DCT sub-bands. The quantized values are coded using Huffman coding. The quantization parameter is optimized by using an optimizing mechanism which employs the subservient data. At a receiver side an intended user with secret key can reconstruct the principal content. The experimental result shows the ratio-distortion performance of this work is significantly better than thatof existing techniques.

2. Related works

The field of encryption and compression encompasses diverse schemes, ranging from the order of the process to variety of techniques. Here the schemes in which encryption is followed by compression only is considered. A.Kingston proposed a scheme [19] in 2007 which was motivated by a French project that was intended to securely store the digital data base of Louvre museum. Instead of encrypting the entire image only selective encryption is performed. The proposed technique takes advantage of a kind of Discrete Randon Transform (DRT) called the Mojette transform properties. This method enables perfect reconstruction of image. But as we increase the number of blocks that should be encrypted the time requirement increases exponentially. So it is impossible to completely encrypt the image using this method. In 2008, another method was proposed by A. Anil Kumar [7], which applies encryption on the prediction errors instead of directly applying on the images and use distributed source coding for compressing the cipher texts. The simulation results show that by using the proposed technique comparable compression gains, with compression ratios varying from 1.5to 2.5 can be achieved despite encryption. In order to increase the compression gain the quality of the image should be sacrificed. In 2009, another work was proposed by A. Anil Kumar [12] which considers the problem of lossy compression of encrypted image by compressive sensing technique. Denoising of output image will improve the PSNR of the result. Through this method compression ratio could be improved up to 3.2.X. Zhang [15] proposed a novel scheme for lossy compression of an encrypted image with flexible compression ratio. This method is based on iterative reconstruction. The data sender pseudo randomly permutes the pixels and the permutation way is determined by a secret key. For compression permuted pixels are divided into two sets as rigid pixels and elastic pixels. Rigid pixels will be kept as such. Orthogonal transform is performed for the elastic pixels. Compression ratio increased to 4 in this method. The method of scalable coding [16] of encrypted images was proposed by X. Zhang. The encrypted image will be down sampled by 2 and the remaining pixels are converted to different sets. As more and more sets in Q are transmitted, the PSNR increases but CR decreases. Because of the hierarchical coding mechanism, the compression ratio varies between2.7 to 4.5.

3. Proposed Scheme

In this scheme, the content owner firstly encrypts the image using a secret key and the encrypted data is provided to the channel provider. In this method encrypted data has two parts. If the bandwidth of the channel is enough for transmission of the data, the channel provider transmits the encrypted data. Otherwise, the channel provider sends a bandwidth insufficiency message to the content owner, and then the content owner generates the subservient data according to the image and provides it to the channel provider. Then, the channel provider who cannot access the original content may compress the coefficients in encrypted domain by a quantization method with the subservient data, and transmits the compressed data, which include an encrypted sub-image, and subsidiary part of encrypted data, the quantized data, and the quantization parameters through a channel. At receiver side, an authorized user can

reconstruct the principal content of original image by retrieving the coefficient values. Using this method the compression ratio distortion performance is improved. The sketch of this work is shown in Fig.1.

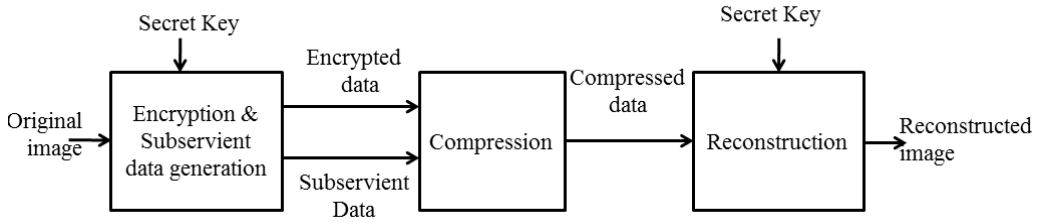

Fig. 1. Block Diagram of Proposed System

3.1. Encryption

A pseudorandom number sequence in the range of 0 to 255 and in the same size of original image is used for encrypting the original image. The pseudorandom numbers are generated using a secret key, which is known to the content owner and the authorized user alone. Modulo256 addition is performed between the input image and PN sequence. The encrypted data has two parts. Let, the input image be represented as *p*, with a size of m×n. Pseudorandom number sequence, *k* of same size is generated using the secret key. It is desirable that the value of the PN sequence vary in between 0 to 255. The first part of Encrypted data [16] is calculated as in (1). Clearly for reconstruction we should have the information about the quotient of this Modulo 256 addition. Since the value of image and PN sequence varies in between zero and 255, the quotient of Modulo 256 addition will be a binary sequence. It is calculated as shown in (2). In order to improve the compression ratio it is desirable to perform bilinear interpolation on the input image to a desirable size.

$$c = \mathrm{mod}[(p+k),256] \tag{1}$$

$$s = floor[(p+k)/256] \tag{2}$$

It is advisable to encrypt this data as well. Thus, it is XORed with pseudorandom binary sequence. *s* has the same size of original image, and the values are binary in nature. Any biplane of the previously generated pseudorandom number sequence can be used for the encryption of *s*.

3.2. Subservient Data Generation

Subservient Data is generated for efficient compression and reconstruction of encrypted data. For generating subservient data, the input image is first down sampled by a factor of 8. More specifically, we are dividing the image into blocks of 8×8, and from each block the last pixel is selected. Down sampled image is then interpolated using bilinear interpolation. The input image and interpolated image are divided into blocks of 8×8 and block wise 2D discrete cosine transform is calculated. With viewing the coefficients as 64 sub-bands, calculate the square roots of the average interpolation distortion [18] as shown below.

$$\sigma^{(u,v)} = \sqrt{\frac{\sum_{i=0}^{m/8-1}\sum_{j=0}^{n/8-1}[P(8i+u,8j+v)-G(8i+u,8j+v)]^2}{mn/64}} \tag{3}$$

Thus the subservient data σ can be generated where P and G are the block wise 2D DCTs of original image and interpolated image respectively. The values of u and v vary from 1 to 8.

3.3. Compression

After encrypting the image, if the channel resource is sufficiently abundant any compression is needless. In this case the channel provider may transmit the encrypted image directly. Thus an authorized can decrypt the received data to reconstruct the original image without any distortion. If the channel resource is limited, the channel provider should obtain the subservient data from the content owner, and then perform a data-compression using a quantization and entropy coding before transmission. The compression procedure is as follows.

The compression will be performed in 64 sub-bands of discrete cosine transform with different optimized quantization parameters. The channel provider performs 2 dimensional DCT in the encrypted image with a block-by-block manner with a block size of 8×8. Each block is of size 8×8 and considered as 64 different sub-bands. It is converted into row vector. Such vectors corresponding to every block are concatenated downwards to obtain a matrix of size *(mn/64×64).* Next step is orthogonal transform of the matrix. Orthogonal transform will help to obtain better visual quality as it is uniformly scattering the reconstruction error. In orthogonal transform the matrix of size *(mn/64×64)*is multiplied with an orthogonal matrix of size *(mn/64×mn/64).* Then quantization of the orthogonally transformed matrix is performed as follows

$$Q^{(u,v)}(t) = \mathrm{mod}\{round\left[\frac{D^{(u,v)}}{\Delta^{(u,v)}}\right], M\}, 1 \le u, v \le 8, 1 \le t \le mn/64 \tag{4}$$

D represents the orthogonally transformed matrix. The quantization parameters, M and Δ are optimized using the procedure explained in section 3.5. The quantized values are encoded using Huffman coding.

Sub image of the encrypted image is calculated simply by down sampling the encrypted image by a factor of 8. Thus the sub-image, the encrypted binary data, Huffman coded data and the quantization parameter values are transmitted to the receiver.

3.4. Reconstruction

With the compressed data and secret key the receiver should perform the following operations to reconstruct the principal image content. Decompose the compressed data and decode the Huffman coded data to obtain quantized values i.e., Q. Then decrypt the sub-image to retrieve the original sub image and bilinear interpolation of this sub-image is performed. Interpolated image is denoted as *g*. Then decrypt binary encrypted data as well. Find an estimate of encrypted image using (5) where $\bar{k}$ is equal to *k* if corresponding binary data is zero, else 256 is subtracted from k to obtain $\bar{k}$. The estimate of the encrypted image is transformed using block wise 2D discrete cosine transform. The coefficients in each block are converted into vectors. Such vectors of every block are concatenated to obtain a matrix of size *(mn/64×64).* This vector is orthogonally transformed to obtain $\tilde{D}$. $\tilde{D}$ is approximated to closest value [18] of original value using (6) Inverse orthogonal transform of $\hat{D}$ is calculated to obtain $\hat{C}$. Inverse 2D DCT is also performed on $\hat{C}$ in block by block manner to obtain $\hat{c}$. Finally, the reconstructed image is obtained [18] as (7).

$$\tilde{c} = g + \bar{k} \tag{5}$$

$$\hat{D}^{(u,v)}(t) = round\left[\frac{\tilde{D}^{(u,v)}(t) - Q^{(u,v)}(t).\Delta^{(u,v)}}{\Delta^{(u,v)} M}\right]\Delta^{(u,v)}.M + Q^{(u,v)}\Delta^{(u,v)} \tag{6}$$

$$\hat{p} = \hat{c} - \bar{k} \tag{7}$$

3.5. Optimization of compression parameters

For optimization of Δ the subservient data is required. The following steps are performed to optimize Δ. The difference between D and $\tilde{D}$ is calculated as,

$$\varepsilon^{(u,v)}(t) = \tilde{D}^{(u,v)}(t) - D^{(u,v)}(t), 1 \le u, v \le 8, 1 \le t \le mn/64 \tag{8}$$

$$D_Q^{(u,v)} = round\left[\frac{D^{(u,v)}}{\Delta^{(u,v)}}\right]\Delta^{(u,v)} \tag{9}$$

$$\delta^{(u,v)}(t) = D_Q^{(u,v)}(t) - D^{(u,v)}(t) \tag{10}$$

Using these values the function f is calculated as in (11). *f* is the measure of expectation of error in each sub-band. It is calculated for various values of Δ. And the value Δ which provides the minimum f for each sub band will be selected [18].

$$f = \sum_{-\alpha}^{\alpha}\sum_{-\Delta/2}^{\Delta/2}\frac{\exp(-\varepsilon^2/2\sigma^2)}{\sqrt{2\pi}}\left(round\left[\frac{\varepsilon-\delta}{\Delta.M}\right]\Delta.M + \delta\right)^2 \tag{11}$$

From (4), it is clear that as the value of M decreases, the range of values of Q will decrease and hence the compression ratio will increase with a trade off in the quality of the image. For optimizing M a negative value of λ is selected and a condition is set such that as the value of λ becomes more and more negative the compression ratio increases. The condition is in (12) where m_k is the trail values which should be preferably in the range of 1 to 64. The value of m_k satisfying (12) is selected as M for each sub band. Likewise the optimized compression parameters are calculated as $M^{(u,v)}$ and $\Delta^{(u,v)}$ where u and v varies from 1 to 8.

$$\begin{aligned}\frac{\sigma^{(u,v)2}[f(m_{k-1}) - f(m_k)]}{\log_2(m_{k-1}) - \log_2(m_k)} &\le \lambda \\ \frac{\sigma^{(u,v)2}[f(m_k) - f(m_{k+1})]}{\log_2(m_k) - \log_2(m_{k+1})} &> \lambda\end{aligned} \tag{12}$$

4. Experimental Results

The test image Lena sized 512 ×512 was used as the original in the experiment. Image used for the experiments and it's encrypted versions are shown below.

Fig. 2. (a) Input image Lena (b) Encrypted image

When producing an encrypted version, we also generated the subservient data. For generation of subservient data, the original image is down sampled and then bilinearly interpolated. These images are obtained as shown in Fig.3.

Fig. 3. (a) Downsampled image (b) Interpolated image

The subservient data generated for Lena image in gif format is shown in Table 1.

Table 1. Subservient Data generated for Lena.gif of size 512×512

77.7625	42.40857	35.46888	19.95584	12.65996	8.746655	6.632905	4.751187
35.80099	23.63785	23.85513	14.56859	10.88474	7.40233	5.250137	3.901758
18.8984	18.06758	16.61955	12.51748	9.193477	6.582822	4.495953	3.808209
10.61505	11.05452	9.734604	9.025581	7.468964	5.598245	4.076743	3.312393
5.995669	6.835529	6.789681	5.855751	5.323113	4.089382	3.151376	2.609989
4.064488	4.532727	4.357729	4.230052	3.825474	3.200274	2.72246	2.251332
3.000554	2.858269	3.03227	2.742975	2.704609	2.535005	2.220658	2.037143
2.226691	2.295044	2.209036	2.282222	2.133696	1.999293	1.842401	1.683565

The value of λ is given as -20 and -50 and the optimized values of M are shown in Table 2.

Table 2. Optimized values of M for (a) λ =-20 and λ =-50

(a)

63	63	63	55	34	23	9	1
63	62	63	40	19	11	9	1
54	53	55	23	21	15	17	8
19	29	22	17	10	7	1	1
10	18	12	7	4	2	1	4
1	1	8	1	7	1	1	1
1	1	1	6	1	4	1	1
1	1	1	4	1	1	1	1

(b)

63	63	63	49	35	22	12	6
63	63	58	48	22	13	11	5
42	57	62	25	24	17	18	9
26	33	26	22	14	9	4	2
12	20	13	9	8	6	2	5
5	6	10	5	9	2	1	1
2	2	4	8	1	6	3	1
1	1	1	5	3	1	1	1

Table 3.Optimized values of Δ for λ =-20 and λ =-50

(a)

255.5054	254.4514	253.3492	182.4534	115.7482	1.249522	0.947558	0.678741
255.7214	216.1175	218.1041	131.1173	99.51761	1.057476	0.75002	0.557394
172.7854	165.1893	151.9501	114.4456	1.313354	0.940403	0.642279	0.54403
97.05187	101.0699	87.61143	1.289369	1.066995	0.799749	0.582392	0.946398
0.856524	0.976504	0.969954	0.836536	0.760445	0.584197	0.900393	0.745711
0.580641	0.647532	0.622533	0.604293	0.546496	0.914364	0.777846	0.964857
0.857301	0.816648	0.866363	0.783707	0.772745	0.724287	0.951711	0.873061
0.954296	0.98359	0.94673	0.978095	0.914441	0.85684	0.789601	0.962037

(b)

244.3964	242.3347	243.2152	182.4534	113.9396	1.249522	0.947558	0.678741
240.3781	216.1175	214.6962	126.9548	1.554963	1.057476	0.75002	0.557394
172.7854	165.1893	151.9501	114.4456	1.313354	0.940403	0.642279	0.54403
1.516435	101.0699	1.390658	1.289369	1.066995	0.799749	0.582392	0.946398
0.856524	0.976504	0.969954	0.836536	0.760445	0.584197	0.900393	0.745711
0.580641	0.647532	0.622533	0.604293	0.546496	0.914364	0.777846	0.964857
0.857301	0.816648	0.866363	0.783707	0.772745	0.724287	0.951711	0.873061
0.954296	0.98359	0.94673	0.978095	0.914441	0.85684	0.789601	0.962037

Thus we obtained the compressed values and the compression ratio is found to be 42.54 and 42.91 for λ values of -20 and -40 respectively which is very high compared to the existing works of encrypted image compression. The space saved due to this compression is above 96% with Huffman coding. The reconstructed image was of good subjective quality and with a PSNR above 36dB. The reconstructed image is as shown in Fig.4. Even without using Huffman coding this method could improve the compression ratio than the previous methods. The tradeoff between compression ratio and PSNR without using Huffman coding is shown in Fig 5 (a).

0Fig. 4 Reconstructed image (a) PSNR=37.78 Compression ratio without using Huffman coding is 5 and with Huffman coding 22.54 for λ =-20 (b)PSNR=36.72 Compression ratio without using Huffman coding is 6 and with Huffman coding 22.91 for λ =-50

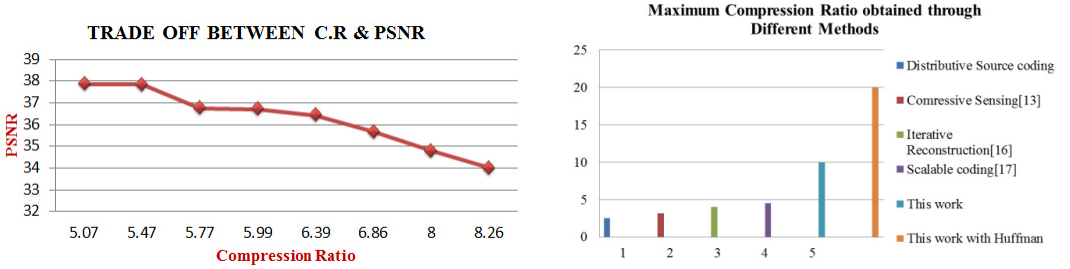

Fig 5. a)Tradeoff between Compression ratio and PSNR without using Huffman coding b) Comparison Chart of maximum compression ratio obtained though different methods

The system was tested for different outputs and obtained good results. Results are shown in Fig.6

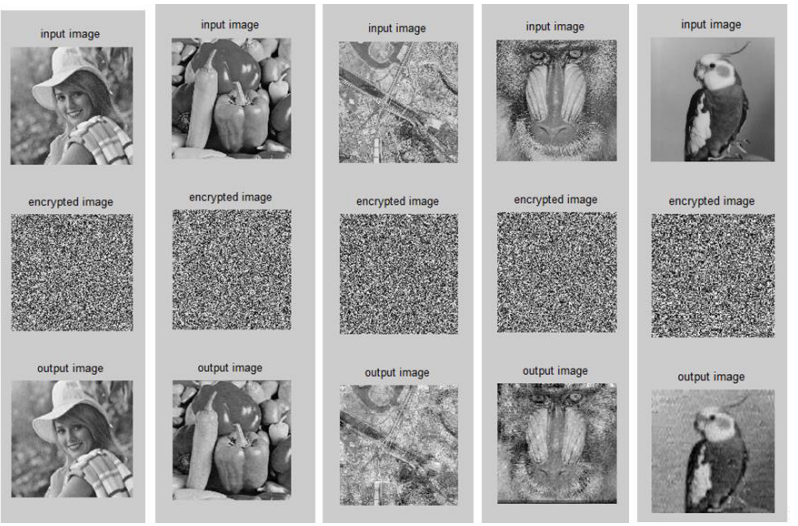

Fig. 6. Input image, Encrypted image and output images obtained for different test images

The graph shown in Fig.5(b) compares this method with other techniques which perform the compression of encrypted image. The maximum compression ratios obtained in different methods are displayed. The maximum compression ratio obtained through distributive source coding is 2.5. It is improved to 3.2 using compressive sensing method. Using iterative reconstruction and scalable coding compression ratio obtained is 4 and 4.5 respectively. Using this work a maximum compression ratio of 10 and 20 can be obtained with and without Huffman coding. The same input image is used for comparison.

5. Conclusion

This work proposes a scheme of compressing encrypted images with subservient data and Huffman coding. While the content owner produces the encrypted data and the subservient data, the channel provider quantizes the encrypted data using the optimal parameters derived from the subservient data, and then performs coding of the quantized values using Huffman coding. Then transmits an encrypted sub-image, the Huffman coded data, the quantization parameters and the encrypted binary data. At receiver side, the principal image content can be reconstructed using the compressed encrypted data and the secret key. Compared with existing methods, the compression performance is improved. In future, this method can be applied for standard encryption schemes such as AES or DES.

References

[1] 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.

[2] StrunkJrZ. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi,G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,"*EURASIP J. Inf. Security*, pp. 1–20, 2007.

[3] N. S. Kulkarni, B. Raman, and I. Gupta, "Multimedia encryption: Abrief overview," *Recent Adv. Multimedia Signal Process. Commun.*, vol. SCI 231, pp. 417–449, 2009.

[4]G. Jakimoski and K. P. Subbalakshmi, "Security of compressing encrypted sources," in *Proc. 41st Asilomar Conf. Signals, Systems and Computers (ACSSC 2007)*, 2007, pp. 901–903.

[5]D. Schonberg, S.C. Draper, and K. Ramchandran, "On blind compressionof encrypted correlated data approaching the source entropy rate," in*Proc. 43rd Annu.Allerton Conf.*, Allerton, IL, USA, 2005.

[6] 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.

[7] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in *Proc. IEEE 10th Workshop Multimedia Signal Processing*, 2008, pp.760–764.

[8] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Signal Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[9] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Towards compression of encrypted images and video sequences," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 749–762, 2008.

[10] D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, "Oncompression of data encrypted with block ciphers," in *Proc. IEEE DataCompression Conf. (DCC '09)*, 2009, pp. 213–222.

[11] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol.52, no. 4, pp. 1289–1306, 2006.

[12] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling ,"*IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar.2008.

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

[14] X. Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in *Proc. 7th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2011)*,2011, pp. 222–225.

[15] X. Zhang, "Lossy compression and iterative reconstruction for encryptedimage," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58, 2011.

[16] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encryptedimages," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108–3114,Jun. 2012.

[17] S.-W. Ho, L. Lai, and A. Grant, "On the separation of encryption andcompression in secure distributed source coding," in *Proc. IEEE InformationTheory Workshop*, 2011, pp. 653–657.

[18] Xinpeng Zhan, YanliRen, LiquanShen, ZhenxingQian, and GuoruiFeng "Compressing Encrypted ImagesWith Auxiliary Information " in IEEETransactions On Multimedia, Vol. 16, No. 5, August 2014

[19] A. Kingston et al. "Lossless Image Compression And Selective EncryptionUsing A Discrete Radon Transform" IEEE-1-4244-14377/07,ICIP, pp.IV465-468, 200777/07,ICIP, pp.IV465-468, 2007