 JCS, vol.1, no.1, pp.29-41, 2019

A Block Compressed Sensing for Images Selective Encryption in Cloud

Xingting Liu[1], Jianming Zhang[2, *], Xudong Li[2], Siwang Zhou[1], Siyuan Zhou[2] and Hye-JinKim[3]

Abstract: The theory of compressed sensing (CS) has been proposed to reduce the processing time and accelerate the scanning process. In this paper, the image recovery task is considered to outsource to the cloud server for its abundant computing and storage resources. However, the cloud server is untrusted then may pose a considerable amount of concern for potential privacy leakage. How to protect data privacy and simultaneously maintain management of the image remains challenging. Motivated by the above challenge, we propose an image encryption algorithm based on chaotic system, CS and image saliency. In our scheme, we outsource the image CS samples to cloud for reduced storage and portable computing. Consider privacy, the scheme ensures the cloud to securely reconstruct image. Theoretical analysis and experiment show the scheme achieves effectiveness, efficiency and high security simultaneously.

Keywords: Compressed sensing, Image encryption, privacy preserving, cloud security.

1 Introduction

In recent years, the Compressed sensing (CS) emerged as an image transmission and processing framework, due to the Compressive sensing (CS), which allows the original signal to be determined from even fewer measurements than the Shannon sampling theorem requests by utilizing the signal's compressibility in some domains. CS finds a sparse solution of an ill-posed inverse problem when the signal of interest is known to be sparse and compressible. CS theory demonstrates that only O(M) random measurements are enough to represent the transformed data x, where $K<M\leq N$. Signal x must be K-sparse if x has only K significant elements when other elements are zero or close to zero. Each measurement y_i is the inner product of x and the measurement vector $\Phi_i \in R_N$, i.e.,

$y_i =< \Phi_i , x >$.*Define* $\Phi = [\Phi_1,...,\Phi_M]^T$, we have

$$y = \Phi X = \Phi Bs \tag{1}$$

where $\Phi \in R_{M\times N}, and M << N$

[1] College of Computer Science and Electrical Engineering, Hunan University, Changsha, 410082, China.

[2] School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, 410114, China.

[3] Business Administration Research Institute, Sungshin W. University, Seoul, 02844, Republic of Korea.

[*] Corresponding Author: Jianming Zhang. Email: jmzhang@csust.edu.cn.

The CS-based cryptosystem has some inherent advantages. Firstly, the low cost of CS sampling process makes the CS-based cryptosystem very suitable for low-complexity restricted system. Secondly, during the CS sampling process, compression and encryption can be jointly guaranteed by a simple matrix multiplication operation. It is worth mentioning that the combined compression and encryption of CS sampling is an appealing option for real-world communications [Xiang, Li, Hao et al. (2018)].

More and more digital images are generated because digital technologies and Internet, transmitted over the networks and stored on various platforms, such as cloud server, hard drive, and others. Some image information may be involved in personal privacy, trade secrets, military secrets and even national security, thus it will be very serious that attackers copy, malicious spread and tamper with the images in the transmission process through the network. for protect the image information over the network, many image encryption algorithms have been proposed using chaotic system, [Shah, Li and Sodhro (2016); Alam and Hamida (2015); Naganawa, Wangchuk, Kim et al. (2017)], DNA computing, [MosavatJahromi, Maham and Tsiftsis (2016); Zhou, Cao, Dong et al. (2015); Zhu, Gao and Li (2016)], cellular automata (CA), optical transform [Dautov and Tsouri (2014); Cheng, Tsai and Huang (2016); Yan, Wang and Shen (2014)], Brownian motion [Norouzi, Seyedzadeh, Mirzakuchaki et al. (2015)]; Latin squares and others. These algorithms can actually encrypt image information effectively and ensure data security.

Compressed sensing allows reducing the number of samples required for high dimensional signal acquisition while retaining important information. However, the tradeoff is that the image recovery process could be computationally demanding. Owing to the limited resources, performing such computationally intensive image recovery tasks is impractical from the viewpoint of sensors and end users.

Existing methods always encrypt the entire plain text or image. However, in case of real-time and resource-constrained security applications like mobile phone, such traditional encryption schemes are not feasible due to their huge computational complexity. To solve this limitation up to some extent, the concept of selective encryption is presented, where only the important data is encrypted, thereby reducing the amount of image data to be encrypted [Wan, Kai and Liu (2012); Ying, Wang and Zhang (2009)].

With cloud computing being more widely utilized, it provides a feasible solution to cost- and time-saving associated with image recovery for resource-constrained sensors and end users. The image signal usually contains confidential or sensitive information, then outsourcing the image recovery task to the untrusted cloud server may bring privacy leakage [Shuang and Zhou (2017)]. Another problem is that directly using compressed sensing recovering the original signals is computationally hard, only when the random measurement matrix is kept secret. We note that, although establishment of the symmetric key may introduce some overhead due to the complexity of public-key cryptography, it is a one-time procedure during system initialization only. Different symmetric keys can be established for different meters [Shuren, Wenlong, Junguo et al. (2018)].

The chaotic system has the characteristics of high sensitivity to initial conditions and control parameters, and is widely used in the field of image encryption to further enhance the random- ness of the algorithm and keys. Chaos is a kind of complex dynamical behavior with special properties [Yao, Yuan, Qiang et al. (2016)]. A chaotic sequence is

pseudorandom and finite, which is suitable for constructing the measurement matrix, [Dan, Geng and Pahlavan (2016)]. Chaotic system can generate measurement matrices by the deterministic method which means a sequence can be generated by a deterministic system while this sequence is pseudorandom meeting the condition of the measurement matrix. So, it can simplify the constructing process of the measurement matrix [Liao, Leeson, Higgins et al. (2016); Ayatollahitafti, Ngadi, Mohamad Sharif et al. (2016); Tsouri, Zambito and Venkataraman (2016)].

Block compressed sensing (BCS) is simpler and more efficient than other CS techniques, BCS can sufficiently capture the complicated geometric structures. BCS is a great success exploit of CS which can be widely used in many aspects. The main advantages of BCS includes: (a) Measurement operator can be easily stored and implemented through a random undersampled filter bank; (b) Block-based measurement is more advantageous for real-time applications as we only got part of the whole data; (c) Since process each block is dependent, we can easily got the initial solution and speeded up the reconstruction process [Raja and Kiruthika (2015)].

Based on the above analyses, in the premise of guaranteeing information security, we introduce an image encryption algorithm based on the chaotic system, image saliency and block compressive sensing. Our contributions are as follows. First, partition the image into small blocks, then through saliency and perturbation, the plain image measure become y. y and part secret key transferred to cloud server. The block perturbation image would transfer to decryption server. User using the secret key from encryption user, help get the correct reconstruct image [Ya, Yun, Jin et al. (2018); Daojian, Yuan, Feng et al. (2018)].

2 Preliminaries

2.1 Block compressive sensing

In 2006, Candes and Donoho proposed the concept of compressive sensing (CS), it compresses and samples simultaneously, and allows the exact recovery of a sparse signal from some projections lower than the Nyquist rate. The theory of CS points out that: by developing the sparse characteristic of the signal, the discrete sample of the signal is obtained by random sampling under the condition of far less than the Nyquist sampling rate, and then the reconstruction signal is perfect by the nonlinear reconstruction algorithm. Compressive sensing theory asserts that if the signal is naturally sparse or sparse in some transform domains, the high dimensional signal can be projected into a low dimensional space by a measurement matrix unrelated to the sparse base, and these few projections contain enough information about the reconstructed signal, so that the original signal can be reconstructed with high probability by solving the optimization problem with these projections [Mahsa, Mahdad Hosseini, Claudio et al. (2014); Gan, Zhi, Jian et al. (2014)].

2.2 Image saliency

So far, there has been a large number of saliency detection models proposed for various multimedia processing applications. Most existing saliency detection methods are implemented in uncompressed domain. Generally, most images over Internet are stored in the compressed domain of joint photographic expert group (JPEG). These existing

saliency detection methods must decompress these compressed images to extract features from the compressed images in compressed domain. However, this is a computation consuming and time-consuming process. It is advantageous to use the saliency detection model in the compressed domain to extract the salient regions in images in the proposed method. Therefore, as in, we follow a saliency detection model in the compressed domain to extract the salient region in the image. Firstly, the DCT coefficients are used to extract the intensity, color and texture features; then, the feature contrast is calculated by the feature differences between image patches; the final salient regions can be extracted by the spatially weighted feature contrast [Rouf, Mustafa, Xu et al. (2012)].

We outsource the image CS samples to cloud for reduced storage and portable computing. Consider privacy, the scheme ensures the cloud to securely reconstruct image. Theoretical analysis and experiment show the scheme achieves effectiveness, efficiency and high security simultaneously [Shahrasbi and Rahnavard (2016); Khan, Ahmad and Hwang (2015)].

2.3 BCS-SPL

Block-based random image sampling is coupled with a projection driven compressed sensing recovery that encourages sparsity in the domain of directional transforms simultaneously with a smooth reconstructed image. Both contourlets as well as complex valued dual-tree wavelets are considered for their highly directional representation, while bivariate shrinkage is adapted to their multiscale decomposition structure to provide the requisite sparsity constraint. Smoothing is achieved via a Wiener filter incorporated into iterative projected Landweber compressed-sensing recovery, yielding fast reconstruction. The proposed approach yields images with quality that matches or exceeds that produced by a popular, yet computationally expensive, technique which minimizes total variation. Additionally, reconstruction quality is substantially superior to that from several prominent pursuits-based algorithms that do not include any smoothing. Adopted the general paradigm of block-based random image sampling coupled with a projection-based reconstruction promoting not only sparsity but also smoothness of the reconstruction. This framework facilitates the incorporation into the CS-recovery process of directional transforms based on contourlets and complex-valued dual-tree wavelets. [Zhou, Zhang, Wu et al. (2014); Wu and Liu (2012)].

3 Proposed scheme

In this section, we will present our BCS-based privacy-preserving image recovery scheme based on cloud. We assume a semi-trusted cloud as the adversary in our scheme throughout this paper, i.e., the cloud performs the reconstruction service honestly, but is curious in learning content of the client data. The cloud involves two entities: the data owner and the end user, which are assumed to mobile devices with only limited computational resources. Fig. 1 demonstrates the detail of the scheme. The scheme consists of three parts: encryption, cloud work, decryption. In encryption part, plain image measure becomes y through block, saliency and perturbation. Then transfer y and part of the secret key to cloud server. The cloud server solves the BCS reconstruction problem using BCS-SPL recoding algorithm. Then the block perturbation image would

transfer to decryption server. Decryption user using the secret key from encryption user, help get the correct reconstruct image. The detail of the three part will be introduce in the next subsection.

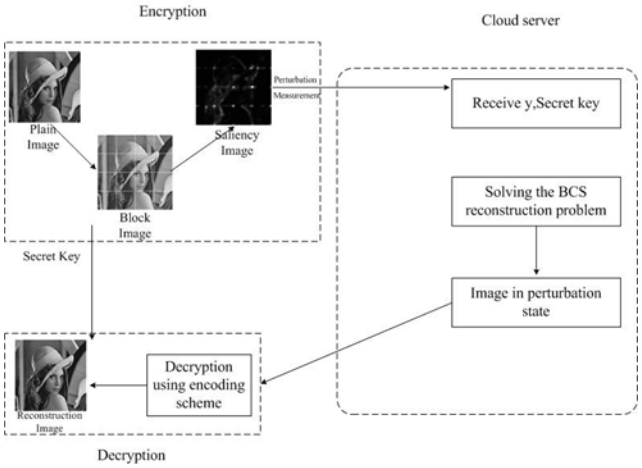

Figure 1: Scheme architecture

Although CS prevents the recovery of the original signal under wireless eavesdropping, we identify the following vulnerability of CS in leaking statistics of the original signal.

Note that x represent important privacy information of the user. Tab. 1 shows an example of the leak of statistics. We can see that, when transfer matrix is used, the 2-norm of the original signal can be accurately estimated. The estimated upper bound of x is close to x. When random measurement matrix is used, the x can be exactly estimated.

Table 1: Signal feature change

	L2	Estimated	variance
True value	12678	435.2	21.43
Estimated	13568	[12.1 482.1]	411
Estimated(psi)	584621	[842 18942]	19212

Figure 2: Energy leakage of CS encryption

Information entropy is an important criterion to measure the feature of randomness. 11 is the image shown in Fig. 2. We can see that the entropies of the cipher images are very close to the ideal value, which can be seen in Fig. 3. It means the information leakage of the proposed coding scheme is negligible.

3.1 Encryption

The proposed image encryption scheme is illustrated in Fig. 4, and the detailed encryption steps are as follows:

Step 1: Assume the size of the plain image I is N×N, then it is split into $N_1 \times N_1$ blocks. N_1 is set to 32 in our experiments.

Step 2: Do saliency detection for all blocks, calculate the saliency value of each block.

Step 3: Perform zigzag confusion on I with (x_0, y_0), which is produce from chaotic sequence

Step 4: Then the image I is sparse by use of discrete wavelet transform (DWT), and the sparse coefficient matrix I_1 with the same size of N×N is obtained.

Step 5: Select Reference Block using saliency value, the blocks which has smallest value would choose to be reference block, the other blocks would encrypt based reference block. The encrypted blocks were $B_i = B_{i-1} - B_{i-2}$, the order of i is produce from the same chaotic sequence. And B_1 is reference block.

Step 6: We get the same secret key from chaotic sequence, produce (r, z_0), using skew tent map produce random measurement matrix, then produce Eq. (1) get measurement y, after that we quantization y.

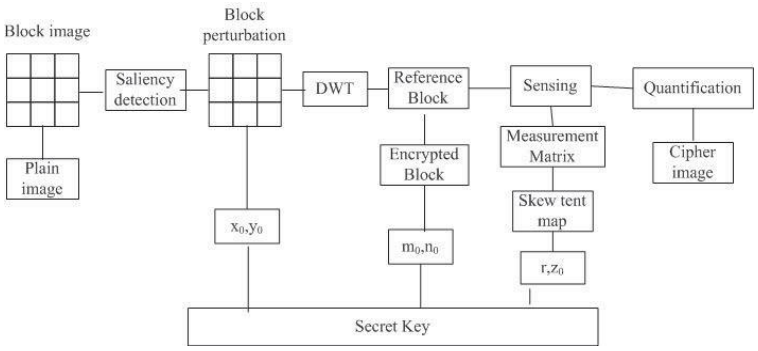

Figure 3: Encryption

3.2 Cloud work

For the cloud, the access request is processed by calling Data Detect to resolve the rightful ownership of the image. If the detection result reveals match, the cloud would call Problem Solve to solve the problem and output the answer e to the authorized end user. Otherwise, the cloud would refuse to serve.

To avoid the cloud servers being lazy or intentionally corrupting the computation result, we propose to design a result verification method to handle these two malicious behaviors. After the end user recovers original f, he only needs to perform a simple matrix-vector multiplication and verify whether. If so, the results returned from the two cloud servers are trusted; otherwise, we can consider that the cloud servers are cheating.

3.3 Decryption

The decryption process is depicted in Fig. 4, which is the inverse operation of the encryption process. Before the decryption, secret keys including 512-bit hash value K, abandoning number n0 of chaotic sequences, the total number e of evolutions, the total number w of scrambling rounds, four parameters: x0,y0,z0,r , initial location (x0,y0) and the measurement matrix dare firstly computed as described in section 3.1 . When got cipher image, decoding using BCS-SPL algorithm take advantage of chaotic measurement matrix, then do dwt inverse transfer. The last step is zigzag perturbation inverse.

Noting that block-based random image sampling coupled with a projection-based reconstruction promotes not only sparsity but also smoothness of the reconstruction. This framework facilitates the incorporation into the CS-recovery process of directional transforms based on sparse wavelets. The resulting algorithms inherit the fast execution speed of the projection-based CS reconstruction while the enhanced directionality coupled with a smoothing step encourages superior image quality, particularly at low sampling rates.

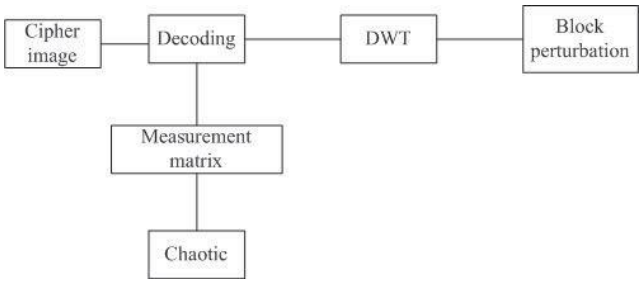

Figure 4: Decryption

4 Simulation results

Fig. 5 is the original figure. We set block 1 as reference block, the following encoding scheme is all based reference block, the other block transform make use of it, and Reference block only encrypted using traditional chaotic compressed sensing. Other blocks all first transform, then encrypt. This is because reference block has the least image information and do not need too many encrypt. Experiment shows in Fig. 6. Block 1 is the reference block.

Figure 5: Original figure

Figure 6: Image block based saliency

4.1 Privacy analysis

Consider for security, chaotic compressed sensing cryptosystem is computational security under brute-force attack and cipher text only attack, because of its key security. In the signal encryption step, the signal y is encrypted by perturbation block, which are encrypted by two different keys, which make X is computationally-infeasible in practice. We claim that the confidentiality of the sensed signal is well protected. Correspondingly, the cloud servers cannot recover the original image content either. So in our scheme, the

cloud finish storage and computation mask but cannot produce information leakage.

We analyze the privacy of transmitted data packets through experiment implementation. We use the sized 256x256 image Lena as test image. Chaotic system produces a random seed a=0.1, encoder uses this seed to produce the measurement matrix A. y=A*x, the decoded file is shown in Fig. 7, and assume the adversary produces a newly same seed a=0.1+0.01, the decoded file is in Fig. 7, very different from Fig. 8.

4.2 Computation complexity

The computational complexity of our scheme mainly contains the following three parts: (1) the key generation; (2) perturbation; (3) measurement Time complexity is also an important index to evaluate the performance of the encryption scheme. The encryption process consists of compression and encryption of the plain image, and embedding process, and the decryption one is composed of extraction process of the compressed cipher image and reconstruction process of the plain image. we can watch that firstly, for the total encryption and decryption times, embedding and extraction times of the compressed cipher image are very little, in detail, in encryption process, compression and encryption of the plain image accounts for about 60 total time, and in decryption process, the reconstruction process costs around 95 G to 1024 G, the encryption time is from 0.4049 s to 3.9024 s, but the decryption time is from 1.4724 s to 122.4369 s. Thus, the proposed encryption scheme is suitable for the small and medium size images, when the size of the image is larger, the time complexity is very higher. In the following work, we will plan to substitute block compressive sensing (BCS) for compressive sensing (CS) to reduce the computation complexity and shorten the encryption and decryption time.

Figure 7: Measurement when a=0.1

4.3 Efficiency analysis

In our scheme, we shift the image reconstruction task to the cloud side to make the compressed sensing technique much more practical. The sensor side and the user side

only need to do simple addition and subtraction operations Moreover, there will be no difference even for different sizes of images. Therefore, our design can reduce the computation burden of the sensor side and the end user side tremendously.

4.3 Time complexity analysis

Regardless of the security considerations, encryption speed is also important, especially in real-time internet applications. In this paper, we analyze the encryption and decryption time of different size images at different compression ratios (CR), and the results are listed in Tab. 2 and Tab. 3.

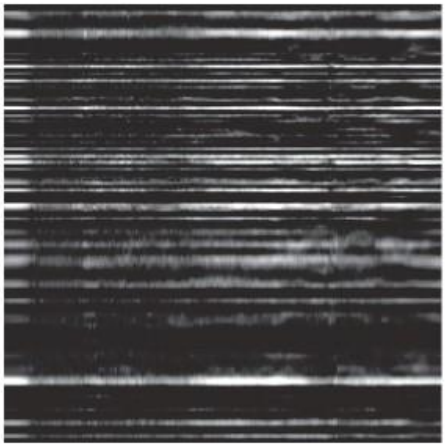

Figure 8: Measurement when a=0.1+0.01

Table 2: Encryption time

Image Size	Lena	Cameraman	Peppers
CR=0.15	0.4472	0.4607	0.4921
CR=0.35	0.4742	0.4682	0.5166
CR=0.55	0.4830	0.4852	0.5225

From Tab. 2, we can watch that (1) for the same plain image, the change of CR has a slight impact on the encryption time. When CR varies from 0.15 to 0.55, the encryption time for 256×256 images is about 0.46 s. (2) for the same original image, the decryption time under different compression ratios is different. And with the increasing of CR, the decryption time also increases. As shown in Tab. 3, when CR changes from 0.15 to 0.55, the time of decrypting Lena image is varying from 1.1 s to 15 s. The reason lays in solving the optimal solution in the reconstruction process, and the larger the measurement matrix, the more time needs.

Table 3: Signal feature change

Image Size	Lena	Cameraman	Peppers
CR=0.15	1.1267	1.1413	2.3156
CR=0.35	6.0213	2.0684	8.1423
CR=0.55	13.2451	5.2635	14.2513

5 Conclusions

In this paper, a block compressed sensing for Images selective encryption based privacy preserving in cloud is proposed, which integrates the technique of CS domain processing into the secure computation outsourcing. We outsource the image CS samples to cloud for reduced storage and portable computing. Consider privacy, the scheme ensures the cloud to securely reconstruct image. Theoretical analysis and experiment show the scheme achieves effectiveness, efficiency and high security simultaneously.

References

Alam, M. M.; Hamida, E. B. (2015): Interference mitigation and coexistence strategies in IEEE 802.15.6 Based Wearable Body-to-Body Networks. *International Conference on Cognitive Radio Oriented Wireless Networks*, pp. 665-677.

Ayatollahitafti, V.; Ngadi, M. A.; Mohamad Sharif, J. B.; Abdullahi, M. (2016): An efficient next hop selection algorithm for multi-hop body area networks. *Plos On*e, vol. 11, no. 1, e0146464.

Cheng, Y. C.; Tsai, P. Y.; Huang, M. H. (2016): Matrix-inversion-free compressed sensing with variable orthogonal multi-matching pursuit based on prior information for ECG signals. *IEEE Transactions on Biomedical Circuits & Systems*, vol. 10, no. 4, pp. 864-873.

Dan, L.; Geng, Y.; Pahlavan, K. (2016): End-to-end power optimization in nonhomogenous relay environment for wireless body area networks (WBANs). *International Symposium on Medical Information & Communication Technology*, pp. 1-5.

Daojian, Z.; Yuan, D.; Feng, L.; Sherratt, R. S. (2018): Adversarial learning for distant supervised relation extraction. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 121-136.

Dautov, R.; Tsouri, G. R. (2014): Securing while sampling in wireless body area networks with application to electrocardiography. *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 1, pp. 135-142.

Gan, H.; Zhi, L.; Jian, L.; Xi, W.; Cheng, Z. (2014): Compressive sensing using chaotic sequence based on chebyshev map. *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2429-2438.

Guo, J. B.; Ren, W.; Lab, S. K. (2014): Construction of a circulant compressive measurement matrix based on chaotic sequence and ripless theory. *Acta Physica Sinica*,

vol. 63, no. 19, pp. 198402-198402.

Khan, J. S.; Ahmad, J.; Hwang, S. O. (2015): An efficient image encryption scheme based on: Henon map, skew tent map and s-box scheme based on: Henon map, skew tent map and s-box. *International Conference on Modeling*, pp. 1-6.

Liao, Y.; Leeson, M. S.; Higgins, M. D.; Bai, C. (2016): An incremental relay based cooperative routing protocol for wireless in-body sensor networks. *IEEE International Conference on Wireless & Mobile Computing*, pp. 1-6.

Xiang, L.; Li, Y.; Hao, W.; Yang, P. (2018): Reversible natural language watermarking using synonym substitution and arithmetic coding. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 541-559.

Liu, H.; Kadir, A. (2015): Asymmetric color image encryption scheme using 2D discretetime map. *Signal Processing*, vol. 113, pp. 104-112.

Mahsa, S.; Mahdad Hosseini, K.; Claudio, P.; Pierre, V.; Alexandre, S. (2014): Compact low-power cortical recording architecture for compressive multichannel data acquisition. *IEEE Transactions on Biomedical Circuits & Systems*, vol. 8, no. 6, pp. 857-870.

Mosavat-Jahromi, H.; Maham, B.; Tsiftsis, T. A. (2016): Maximizing spectral efficiency for energy harvesting-aware WBAN. *IEEE Journal of Biomedical & Health Informatics*, vol. 21, no. 3, pp. 732-742.

Naganawa, J. I.; Wangchuk, K.; Kim, M.; Aoyagi, T.; Takada, J. I. (2017): Simulationbased scenario-specific channel modeling for WBAN cooperative transmission schemes. *IEEE Journal of Biomedical & Health Informatics*, vol. 19, no. 2, pp. 559-570.

Norouzi, B.; Seyedzadeh, S. M.; Mirzakuchaki, S.; Mosavi, M. R. (2015): A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimedia Tools & Applications*, vol. 74, no. 3, pp. 781-811.

Raja, K. S.; Kiruthika, U. (2015): An energy efficient method for secure and reliable data transmission in wireless body area networks using RelAODV. *Wireless Personal Communications*, vol. 83, no. 4, pp. 2975-2997.

Rouf, I.; Mustafa, H.; Xu, M.; Xu, W.; Miller, R. et al. (2012): Neighborhood watch: security and privacy analysis of automatic meter reading systems. *ACM Conference on Computer & Communications Security*.

Shah, M. A.; Li, Y.; Sodhro, A. H. (2016): Energy-efficient adaptive transmission power control for wireless body area networks. *Communications IET*, vol. 10, no. 1, pp. 81-90.

Shahrasbi, B.; Rahnavard, N. (2016): Model-based nonuniform compressive sampling and recovery of natural images utilizing a wavelet-domain universal hidden markov model. *IEEE Transactions on Signal Processing*, vol. 65, no. 1, pp. 95-104.

Shuang, Y.; Zhou, Y. (2017): Binary-block embedding for reversible data hiding in encrypted images. *Signal Processing*, vol. 133, pp. 40-51.

Shuren, Z.; Wenlong, L.; Junguo, L.; Kim, J.-U. (2018): Improved VGG model for road traffic sign recognition. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 11-24.

Tsouri, G. R.; Zambito, S. R.; Venkataraman, J. (2016): On the benefits of creeping wave antennas in reducing interference between neighboring wireless body area networks. *IEEE Transactions on Biomedical Circuits & Systems*, vol. 11, no. 1, pp. 153-160.

Wan, Z.; Kai, X.; Liu, Y. (2012): Priv-code: preserving privacy against traffic analysis through network coding for multihop wireless networks. *Proceedings-IEEE INFOCOM*, vol. 131, no. 5, pp. 73-81.

Wu, X.; Liu, M. (2012): In-situ soil moisture sensing: Measurement scheduling and estimation using sparse sampling. *ACM/IEEE International Conference on Information Processing in Sensor Networks.*

Ya, T.; Yun, L.; Jin, W.; JeongUk, K. (2018): Semisupervised learning with generative adversarial networks on digital signal modulation classification. *Computers, Materials & Continua*, vol. 55, no. 2, pp. 243-254.

Yan, W.; Wang, Q.; Shen, Y. (2014): Shrinkage-based alternating projection algorithm for efficient measurement matrix construction in compressive sensing. *IEEE Transactions on Instrumentation & Measurement*, vol. 63, no. 5, pp. 1073-1084.

Yao, L. L.; Yuan, C. J.; Qiang, J. J.; Feng, S. T.; Nie, S. P. (2016): Asymmetric image encryption method based on gyrator transform and vector operation. *Acta Physica Sinica*, vol. 65, no. 21.

Ying, Y.; Wang, B.; Zhang, L. (2009): Hebbian-based neural networks for bottom-up visual attention systems. *International Conference on Neural Information Processing*, pp. 1-9.

Zhou, J.; Cao, Z.; Dong, X.; Xiong, N.; Vasilakos, A. V. (2015): 4s: a secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Information Sciences*, vol. 314, pp. 255-276.

Zhou, N.; Zhang, A.; Wu, J.; Pei, D.; Yang, Y. (2014): Novel hybrid image compression¨cencryption algorithm based on compressive sensing. *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 18, pp. 5075-5080.

Zhu, H.; Gao, L.; Li, H. (2016): Secure and privacy-preserving body sensor data collection and query scheme. *Sensors*, vol. 16, no. 2, pp. 179.