International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

SECURE INFORMATION TRANSMISSION SYSTEM BASED ON SEMI-TENSOR COMPRESSIVE SENSING IN WIRELESS NETWORKS

Kanimozhi.M[1], Rajeswari.P[2]

[1] *Department of Electronics and Communication Engineering,Dhanalakshmi Srinivasan Engineering College,Perambalur*

Email-[1]kanimozhimt@gmail.com

[2] *Department of Electronics and Communication Engineering,Dhanalakshmi Srinivasan Engineering College,Perambalur*

Email-[2] praeswari245@gmail.com

----------**********----------

Abstract:

Wireless body area networks (WBANs) gather a few physiological parameters of the human body. Each sensor uses limited power to maximize its personal life. There are three important troubles together with adaptiveness, energy and safety in WBANs. In order to solve these troubles, a bendy and cozy records transmission system is proposed in this undertaking. The proposed scheme consists of semi-tensor compressive sensing, hash feature, Arnold scrambling and chaotic scrambling (SC-HAC). For the adaptiveness trouble, our scheme uses semi-tensor compressive sensing to encrypt multiple signals with extraordinary dimensions. The chaotic sequence is applied to generate the semi tensor measurement matrix. On the only hand, we simplest transmit some chaotic parameters, which lessen the variety of information garage and transmission. On the alternative hand, the dimensions of the measurement matrix are small, and the computation overhead may be reduced. The protection is taken into consideration through the proposed scheme which combines Arnold scrambling and Logistic scrambling to enhance the encryption effect. Experimental simulations and security analyses are given to expose that our scheme performs nicely.

Index Terms— **Wireless body area network(WBAN), Arnold scrambling, Chaotic scrambling, Compressive sensing**

----------**********----------

I. INTRODUCTION

Image processing is a way to convert an image into virtual form and perform some operations on it, with a view to get an superior image or to extract some beneficial information from it. It is a sort of signal dispensation wherein enter is photo, like video frame or image and output may be image or characteristics associated with that image. Usually Image Processing machine includes treating images as dimensional signals even as making use of already set signal processing techniques to them. It is amongst hastily developing technologies today, with its programs in diverse factors of a commercial enterprise. Image Processing paperwork core

studies region inside engineering and pc science disciplines too.

The signals are despatched to the data center via wi-fi transmission nodes. For example, in Fig. 1, the sensor information are transmitted to the body sensor coordinator (together with computer, cellular smartphone and many others.) by wi-fi verbal exchange generation (for examples, ZigBee, Bluetooth) in WBANs.

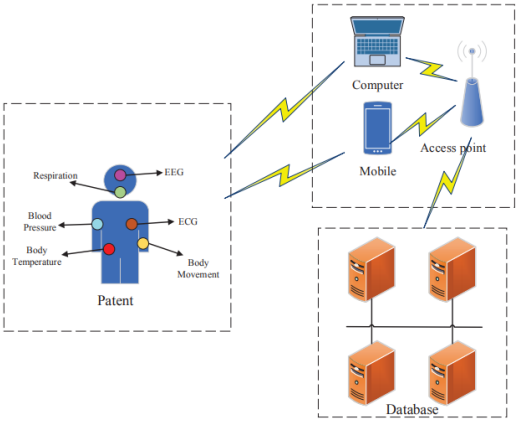


Fig. 1 Data transmission in wireless body area networks

ZigBee and Bluetooth have the characteristics of short distance and low power consumption. The signals are transmitted through the network to the terminal (for example, a hospital data center). Doctors can use these data to diagnose the patient without going to the patient's home or asking the patient to come to the hospital, which can save resources. Nowadays, WBANs are not only used in health monitoring, but also sport training, entertainment, military activities, etc.

In terms of protocol framework, IEEE 802.15.4 and IEEE 802.15.6 are two security protocols related to WBANs, and the latter is designed specifically according to the characteristics of the network.

These two protocols provide the international standard for security, reliability, low power consumption, and long distance transmission.

Adaptiveness is a key problem in wireless body area networks. The types of signals are different, such as ECG, EEG. And the sizes of signals are also different.

Compressive sensing (CS) can be applied to WBANs to measure signals. According to the rule of matrix multiplication in CS, the column number should equal to the signal length. To reduce the size of the measurement matrix, many works focused on reducing the row number of the measurement matrix. Besides, dividing the signals into blocks is another method to reduce the matrix size. However, these methods need to design a specific measurement matrix for a specific size.

II. RELATED WORKS

In the prevailing scheme, semi-tensor compressing sensing (STP-CS) is used to reduce the row and column numbers of the dimension matrix concurrently, and it can measure numerous sizes via the use of the same size matrix. Energy hindrance is any other vital problem in WBANs, due to the fact the battery energy is restrained and the alternative is inconvenient. Each sensor makes use of restricted power to maximise its own life. Sensors are worn on the body or implanted inside the skin in WBANs. However, present schemes seldom attention on the safety difficulty of clinical health information. In terms of safety in WBANs, the patient's fitness statistics are sensitive information. In wi-fi transmission, these health records are without problems stolen by means of the eavesdropper, so it is very essential to put into effect top security. They are based totally on cryptography and examine the security trouble of health records. However the corresponding algorithms are pretty complex and their jogging time is long. Therefore, it's far essential to layout a simple and comfy encryption scheme for strength saving. [1] Most of the prevailing deep-studying-primarily based strategies are tough to correctly cope with the demanding situations confronted for geospatial object detection along with rotation variations and appearance ambiguity. To deal with those problems, this paper proposes a singular deep-mastering-primarily based item detection framework including region inspiration network (RPN) and local-contextual characteristic fusion network designed for remote sensing pics. Specifically, the RPN includes additional multiangle

anchors besides the conventional multiscale and multiaspect-ratio ones, and for that reason can deal with the multiangle and multiscale characteristics of geospatial items.

A novel double photograph encryption scheme based on amplitude-segment encoding and discrete complicated random rework (DCRT) [2] is proposed. First, two pictures are merged right into a plural matrix with the aid of precoding, and the synthetic sign is modulated by way of the phase masks that's calculated from Chen chaotic sequences generated with the aid of using the self-adapting parameter as preliminary values. Then, the modulated sign is encrypted by way of amplitude-section encoding and the DCRT.

Although past work has referred to that contrasts in turbidity regularly are detectable on remotely sensed images of rivers downstream from confluences, no systematic technique has been advanced for assessing mixing over distance of confluent flows with differing surficial suspended sediment concentrations (SSSC). In assessment to subject measurements of blending under confluences, satellite tv for pc faraway-sensing can provide precise facts on spatial distributions of SSSC over long distances. [3] This paper offers a methodology that makes use of faraway-sensing facts to estimate spatial styles of SSSC downstream of confluences alongside large rivers and to decide modifications in the quantity of blending over distance from confluences. The method develops a calibrated Random Forest (RF) model by means of concerning schooling SSSC records from river gaging stations to derived spectral indices for the pixels corresponding to gaging-station locations. The calibrated model is then used to expect SSSC values for each river pixel in a remotely sensed picture, which presents the basis for mapping of spatial variability in SSSCs alongside the river.

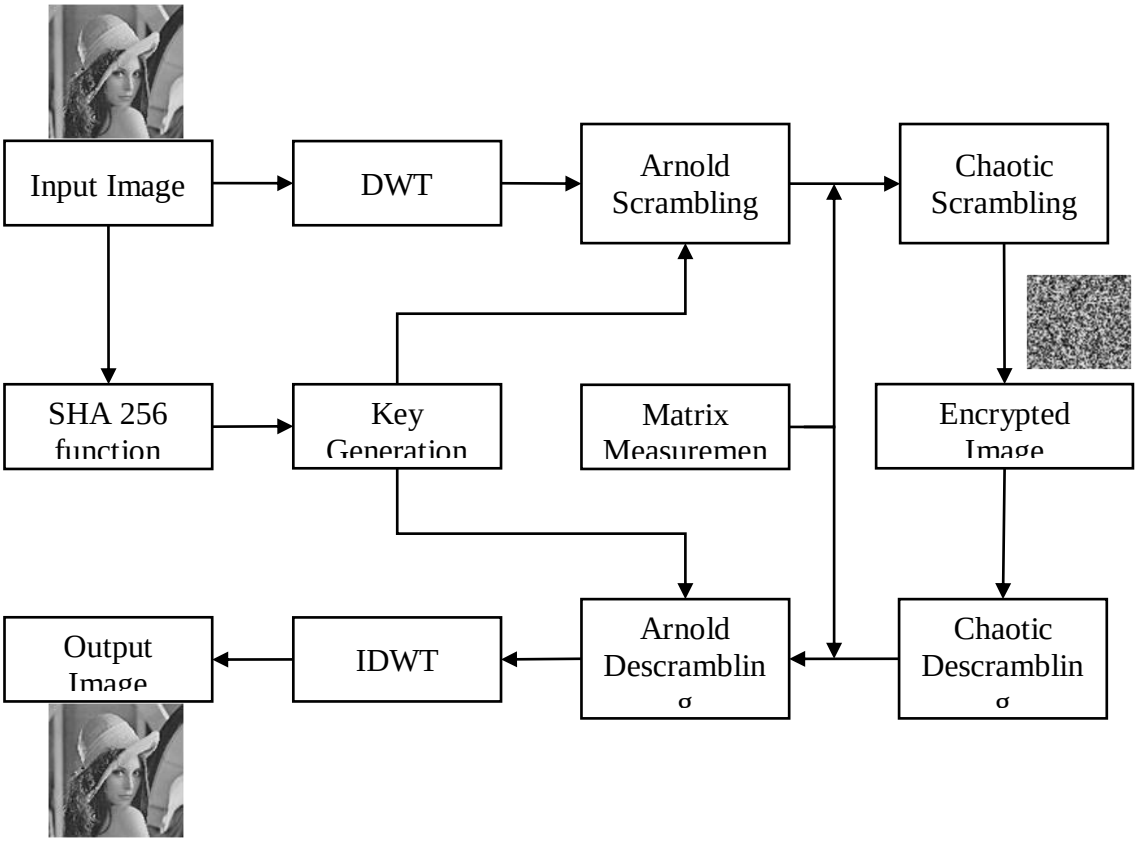
Also [4], on the base of this system, a new chaos-based random variety generator (RNG) is developed and value of the designed RNG in an encryption system is shown over NIST 800-22 randomness tests. S-Box era set of rules is designed, and the overall performance assessments of S-Box are found out. By the usage of the designed RNG and S-Box era algorithms, the brand new hybrid image encryption algorithm primarily based on AES (CS-AES) is evolved. Image encryption packages are carried out for comparison with different encryption algorithms inside the literature to show its security stage and performance

The Increase of virtual media transfer made the modification of the photograph very easy. So one principal trouble of proprietorship is raised, as copying and transferring are very tender practices. Here this paper has to resolve proprietorship hassle by embedding the digital information with encryption. In this work, embedding of records is executed making use of the LZW algorithm. Then robustness is supplied by using the use of the AES algorithm. Finally through the use of spatial approach, embedding of digital records is carried out in encrypted picture. Experiment is completed on actual dataset photo. Evaluation parameter values show that proposed paintings has maintained the SNR and PSNR values with excessive robustness of the facts.

The SM4 [5] and [6] block cipher set of rules utilized in IEEE 802.11i widespread is launched with the aid of the China National Cryptographic Authority and is one of the maximum important symmetric cryptographic algorithms in China. However, whether in the round encryption or key enlargement phase of the SM4 algorithm, a big variety of bit operations at the registers (e.G., circular shifting) are required. These operations are not effective to encryption in situations with huge-scale records. In traditional implementations of SM4, distinct operands are assigned to exceptional words and are processed serially, that could bring redundant operations inside the manner of encryption and decryption. Bit-slice generation locations the equal bit of multiple operands into one word, which allows bit-degree operations in parallel. Bit-slice is certainly a single training parallel processing technology for records, hence it may be expanded through the CPU's multimedia

commands. In this paper, we recommend a fast implementation of the SM4 set of rules using bit-slice techniques. The test proves that the Bit-slice based SM4 is extra green than the original version. It increases the encryption and decryption speed of the message by means of a median of eighty%–one hundred twenty%, in comparison with the original technique.

BLOCK DIAGRAM



Energy limitation is another important problem in WBANs, because the battery power is limited and the replacement is inconvenient. Each sensor uses limited energy to maximize its own life. Sensors are worn on the body or implanted in the skin in WBANs. For those sensors implanted in the skin, battery replacement and charging need to be completed by surgery. Energy harvesting is one solution, allowing the sensor to self-charge. Other approaches to save energy include improving routing protocols or reducing data transmission size.

In recent years, compressive sensing (CS) has been applied in wireless body area networks and image encryption. Due to the implementations of encryption and compression simultaneously, CS has attracted extensive attention. Some schemes of image encryption were presented based on compressive sensing. Zhang et al. reviewed compressive sensing in the field of information security applications, including image, audio and video security, cloud computing security and 5G security. One disadvantage of compressive sensing is that it cannot resist the chosen plaintext attack because of the lack of a diffusion mechanism.

III. PROPOSED SYSTEM

Adaptiveness is a key problem in wi-fi body region networks. The kinds of alerts are distinct, which includes ECG, EEG. And the sizes of indicators also are special.

Compressive sensing (CS) can be carried out to WBANs to degree alerts. According to the rule of thumb of matrix multiplication in CS, the column variety have to equal to the sign period. To reduce the dimensions of the size matrix, many workscentered on reducing the row wide variety of the measurement matrix. Besides, dividing the alerts into blocks is every other approach to lessen the matrix size. However, these methods need to layout a specific size matrix for a particular size. In the proposed scheme, semi-tensor compressing sensing (STP-CS) is used to lessen the row and column numbers of the dimension matrix concurrently, and it may measure various sizes via using the identical dimension matrix.

In order to solve the above issues, consisting of adaptiveness, energy and protection troubles in wireless frame region networks, a bendy and comfortable information transmission gadget is proposed on this task. The proposed scheme consists of semi-tensor compressive sensing, hash characteristic, Arnold scrambling, and chaotic scrambling (SC-HAC). Semi-tensor product compressive sensing (STP-CS) was proposed, which validated spark, coherence, and the restrained isometry assets (RIP) theoretically. In our scheme, taking image statistics as an example, we examine the transmission effect of information encryption in frame vicinity networks. The simple photo conducts a sparse transformation, then uses Arnold scrambling and semitensor compressive sensing.

A. PROPOSED SCHEME

The information of our scheme (SC-HAC) are supplied on this segment. We provide the important thing generation system, which makes use of the SHA-256 hash function. We introduce the encryption and compression technique, which includes Arnold scrambling, semi-tensor compressive sensing, and chaotic scrambling. The decryption and decompression technique is provided. We examine the performance of our scheme.

B. KEY GENERATION

The SHA-2 series includes the hash capabilities SHA-256, and SHA-512. Out of these, SHA-256 is the maximum broadly used. For the SHA-256 hash characteristic, the period of the input is bigoted, and the length of the output is 256 bits. In this project, a plain picture is used as the enter, and the output of the hash function is dealt with as the important thing.

C. IMAGE ENCRYPTION

The model of semi-tensor product compressive sensing (STP-CS) is given in proposed block diagram, which shows the process of semi-tensor compressive sensing. In this model, the parameters α, β can be preset, a chaotic measurement matrix with size m × n, the compression ratio is CR = m/n, and the measurement matrix is generated by the Logistic chaotic sequence. The chaotic measurement matrix satisfies the restricted isometry property (RIP), which can guarantee exact recovery from compressive sensing. This project the initial value of Logistic system is k4, and the parameter of Logistic system is 4. Then we sample the Logistic sequence. The initial sampling position is arbitrary. For convenience, it is set as 1. In order to reduce the correlation of the Logistic sequence, the sampling interval is set as 4 empirically.

The proposed block diagram shows the whole flow chart of our encryption and decryption algorithms in SC-HAC. The encryption process is presented as follows:

Step 1: According to the plain image P1, the keys k1, k2 and k3 can be calculated.

Step 2: The plain image is P1, whose size is p × q. The discrete wavelet transform (DWT) is performed to get P2, whose size is still the same as that of P1. DWT can only be performed on a square matrix.

Step 3: Arnold scrambling is performed on P2 to get P3 whose size is p × q. The parameters are k1, k2, k3, where k1 is Arnold scrambling number, and k2 and k3 are Arnold scrambling parameters.

Step 4: P3 is considered as x. performing a semi-tensor compressive sensing

measurement, y can be obtained. y is denoted as P4 whose size is mp/n × q, and P4 is the result of compression and encryption.

Step 5: Logistic chaotic scrambling is an application of Logistic chaotic system. First, we get the Logistic chaotic sequence w according to specific chaotic parameters. Then, we put the sequence w in ascending order to get the sequence v. The position of each element in the sequence v appearing in the original sequence w is denoted as the index sequence θ.

D. IMAGE DECRYPTION

Decryption is the inverse process of encryption. In proposed block diagram, the sender should transmit some data to the receiver for the decryption. They are k1 (Arnold scrambling number), k2 (Arnold scrambling parameter), k3 (Arnold scrambling parameter), k4 (the initial values of the measurement matrix), k5 (the initial values of the auxiliary matrix), k6 (the initial values of the scrambling sequence) and the cipher image P5. Our scheme transmits only a few constants, which greatly reduces the transmission overhead.

The decryption process is presented as follows. Firstly, we use the key k6 to generate the Logistic chaotic scrambling matrix. Secondly, the cipher image is multiplied by the inverse matrix of the scrambling matrix. Thirdly, we perform semitensor compressive sensing reconstruction algorithm by using OMP algorithm. Finally, we can restore the original image by Arnold recovery and the inverse discrete wavelet transforms (IDWT). The proposed algorithm has the sensitivity to the decryption process. It means that the scheme prevents adversaries from decrypting the transmitted data with a key similar to the encryption key.

The algorithm proposed in this paper can resist the chosen plaintext attack and the known plaintext attack. We add Logistic chaotic scrambling to improve the diffusion process. SHA256 hash function is associated with the plain image, and it is used to generate the key parameters for the Arnold scrambling. Different plain images will have different hash function values, and hash values are all different even if the original image is changed with one pixel.

IV. EXPERIMENTAL RESULTS

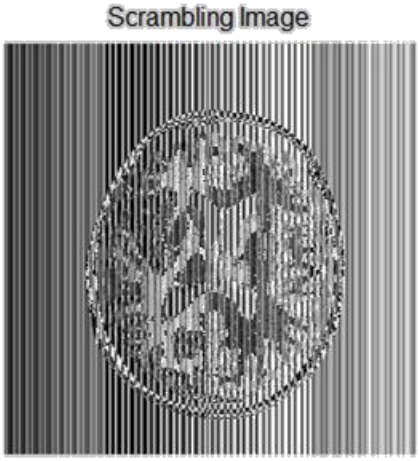
To demonstrate the robustness of proposed SMIE-SIS, Output Figs. show several simulation results of binary, grayscale and color images using proposed SMIE-SIS with different (k, n)-sharing matrices. As shown in Figs. all the secret shares are noise-like image, protecting from information leakage. And the k can be set to 3, 4, 5, and other any number users want to use. Most importantly, with enough number of shares, the original image will be reconstructed with any data loss. When only less than k shares are available, the reconstructed images are noise-like. These demonstrate SMIE-SIS is able to achieve lossless secret sharing for different types of original images.

In this project, conduct a series of simulation experiments. Experimental conditions include the simulation platform MATLAB R2014a, CPU 2.40GHz, RAM Memory 4GB, and 64-bit Microsoft Windows Operating System. We set the initial values are all positive integers. In the chaotic system, the initial values of the measurement matrix, the auxiliary matrix and the scrambling sequence are respectively. The initial values of the chaotic system should be in the range of (0, 1). Three different initial values are to generate

three different sequences. The reconstruction algorithm is the OMP algorithm.

A. INPUT

Six images with different contents like the Lena and MRI brain images with a resolution of 256 × 256, 512 × 512 pixels are chosen to be the embedded images. This set of images is representative since it includes synthetic images with a uniform background and natural images with a complex structure.



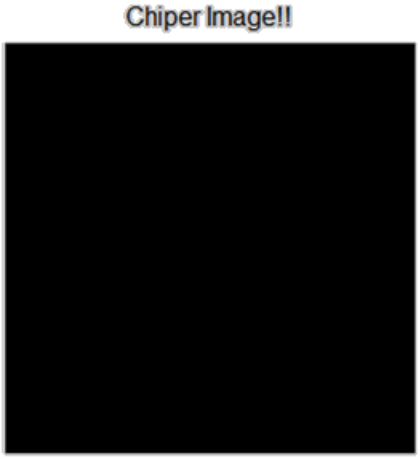
B. PERFORMANCE METRICS

The proposed as well as other encode and decodes introduce distortions to the embedded image since data bits are carried by the modules via customized modulation schemes. To evaluate such distortions, employ the structural similarity (SSIM) metric.

However, the multi-scale structural similarity (MS-SSIM) metric is employed in our experiment to cater for different viewing conditions, such as different resolutions and physical sizes, which are important for barcodes with different capacities. The metric ranges from 0 to 1. A higher score indicates higher similarity between the original and processed images, and therefore less distortion are incurred by the picture embedding process.

Structural Similarity Index Measuring

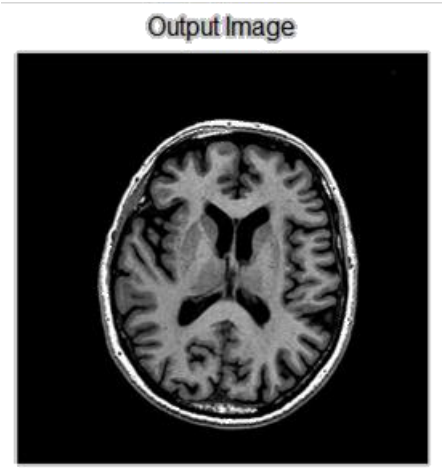
The structural similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index is a full reference metric; in other words, the measuring of image quality based on an initial uncompressed or distortion-free image as reference.



SSIM is a perception-based model that considers image degradation as perceived change in structural information, while also incorporating important perceptual phenomena, including both luminance masking and contrast masking terms. Structural information is the idea that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. Luminance masking is a phenomenon whereby image distortions (in this context) tend to be less visible in bright regions, while contrast masking is a phenomenon whereby distortions become less visible where there is significant activity or "texture" in the image.

Multiscale Structural Similarity Index

A more advanced form of SSIM, called Multiscale SSIM is conducted over multiple scales through a process of multiple stages of sub-sampling, reminiscent of multiscale processing in the early vision system. The performance of both SSIM and Multiscale SSIM is very high in regards to correlations to human judgments, as measured on widely used public image quality databases, including the live Image Quality Database and the TID Database. Most competitive image quality models are some form or variation of the SSIM concept.



V. CONCLUSION

The paper proposes a flexible and relaxed data transmission system based totally on semi-tensor compressive sensing in Wi-Fi body region networks. The plain photo conducts DWT, then this image is converted through Arnold scrambling. The scrambled photo makes use of semi-tensor compressive sensing to compression and encryption, and Logistic chaotic scrambling is used to generate the cipher photo. The proposed scheme is bendy and it is able to be used to measure the snap shots with distinctive sizes without adjusting the scale of the dimension matrix, at the same time as other methods ought to change the scale of the measurement matrix to healthy the apparent picture. Because the dimension matrix is generated by way of the chaotic gadget, the transmission cost is greatly decreased by means of most effective transmitting numerous constants. In addition, the SHA-256 hash function resists the selected plaintext assault, and additionally compensates for the dangers of compressive sensing. By experimental simulations, we analyze the performance of the proposed encryption scheme from numerous perspectives. It can resist the brute force assault, the statistical assault, the regarded plaintext attack and the selected plaintext attack.

FUTURE WORK

In future enhancement of this project has to improve authentication. Recovered image size should be the same for other algorithms also. Also the noise level should be decreased. Also extend further, Cryptography is used to encrypt an image which when separately viewed reveals no information about the secret image. The medical data was hidden within the QR image. Then QR image can be hidden within secret image. A text is written and hidden inside an image. Adaptive modulation method is used for this purpose. Now the image is splited into shares. Each share is embedded using XOR method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work.

REFERENCES

[1] K. Li, G. Cheng, S. Bu, and X. You, ‘‘Rotation-insensitive and contextaugmented object detection in remote sensing images,’’ IEEE Trans. Geosci. Remote Sens., vol. 56, no. 4, pp. 2337–2348, Apr. 2018

[2] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, ‘‘A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation,’’ IEEE Access, vol. 6, no. 3, pp. 77740–77753, 2018

[3] M. Umar, B. L. Rhoads, and J. A. Greenberg, ‘‘Use of multispectral satellite remote sensing to assess mixing of suspended sediment downstream of large river confluences,’’ J. Hydrol., vol. 556, pp. 325–338, Jan. 2018.

[4] U. Çavuşoglu, S. Kaçar, A. Zengin, and I. Pehlivan, ‘‘A novel hybrid ˇ encryption algorithm based on chaos and S-AES algorithm,’’ Nonlinear Dyn., vol. 92, no. 4, pp. 1745–1759, 2018

[5] A. K. Joshi and S. Sharma, ‘‘Reversible data hiding by utilizing AES encryption and LZW compression,’’ in Proc. Int. Conf. Recent Adv. Comput. Commun. Singapore: Springer, 2018, pp. 73–81.

[6] J. Zhang, M. Ma, and P. Wang, ‘‘Fast implementation for SM4 cipher algorithm based on bit-slice technology,’’ in Proc. Int. Conf. Smart Comput. Commun. Cham, Switzerland: Springer, 2018, pp. 104–113.

[7] M. Gharib, Z. Moradlou, M. A. Doostari, and A. Movaghar, ‘‘Fully distributed ECC-based key management for mobile ad hoc networks,’’ Comput. Netw., vol. 113, pp. 269–283, Feb. 2017.

[8] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, ‘‘An elliptic curve cryptography based lightweight authentication scheme for smart grid communication,’’ Future Generat. Comput. Syst., vol. 81, pp. 557–565, Apr. 2018.

[9] S. Qiu, G. Xu, H. Ahmad, and L. Wang, ‘‘A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems,’’ IEEE Access, vol. 6, pp. 7452–7463, 2018.

[10] L. Teng, X. Wang, and J. Meng, ‘‘A chaotic color image encryption using integrated bit-level permutation,’’ Multimedia Tools Appl., vol. 77, no. 3, pp. 6883–6896, 2018.

