Mehran University Research Journal of Engineering & Technology
Vol. 37, No. 4, 645-654 October 2018
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.1804.16

Efficient Advanced Encryption Standard for Securing Cognitive Radio Networks

MARIA SAHER*, ASJAD AMIN*, IMRAN ALI QURESHI**, MUHAMMAD ALI QURESHI*, AND MUHAMMAD MOAZZAM JAWAID***

RECEIVED ON 07.12.2017 ACCEPTED ON 12.02.2018

ABSTRACT

During the last decade, the CR (Cognitive Radio) came into view as a major wireless technology to resolve the issue of spectrum secrecy and efficient spectrum utilization. However, due to unlicensed (secondary) users, there are various security threats to the CRN (Cognitive Radio Networks). Some malicious users may access the CRN and mislead the secondary users to vacate the occupied channel, which may stop the communication. In this work, we propose a new cryptographic-based algorithm, CR-AES (Cognitive Radio-Advanced Encryption Standard), inspired by the traditional AES to secure the CRN. The data of the primary and secondary users is encrypted at the transmitter and decrypted at the receiver. Unlike the conventional AES, we introduce the data-dependent key-generation and shift-rows process. We also reduce the rounds of AES from 10-6 to improve the computational efficiency without compromising the overall security. The experimental results demonstrate the effectiveness of the proposed CR-AES in terms of better security, reliability, and computational efficiency.

Key Words: Cognitive Radio Networks, Cryptography, Advanced Encryption Standard.

1. INTRODUCTION

The demand for radio spectrum is increasing with the emergence of new wireless technologies and related applications such as ad-hoc networks, the internet of things, next generation networks, etc. The CR technology, which utilizes the concept of frequency reuse, has the potential to meet the demands of future technologies. The CR is the spectrum defined radio in which both licensed (primary) and unlicensed (secondary) users are present. In CRN, the secondary user continuously senses the spectrum for white spaces (unused spectrum) and switches to the vacant slot. On the arrival of the primary user, the secondary user has to vacate the occupied slot and switch to another vacant space (hole). In this way, the problem of scarce spectrum resources is efficiently resolved [1]. However, the security of CRN is affected by numerous threats that arise due to sharing of spectrum between primary and secondary users. These threats may cause the DoS (Denial of Services), bandwidth wastage, data modification, connection loss, and interference for the primary users in CRN. To overcome these problems, the security of the CRN is needed [2].

Authors E-Mail: (mariasaher@gmail.com, asjad.amin@iub.edu.pk, imran.qureshi@faculty.muet.edu.pk, ali.qureshi@iub.edu.pk, moazzam.jawaid@faculty.muet.edu.pk)
* University College of Engineering & Technology, The Islamia University of Bahawalpur, Bahawalpur.
** Department of Telecommunication Engineering, Mehran University of Engineering & Technology, Jamshoro.
*** Department of Computer Systems Engineering, Mehran University of Engineering & Technology, Jamshoro.

This is an open access article published by Mehran University Research Journal of Engineering and Technology, Jamshoro under the CC by 4.0 International License.

In literature, many security techniques have been proposed to make CRN more secure against such attacks. These techniques include location verification-based approaches [3-4], Frequency-based approaches [5-6], Cooperative spectrum sensing-based approaches [7-8], Surveillance-based approaches [9], Relay selection techniques [10], Belief propagation-based approaches [11-12], SAP (Signal Activity Pattern) based approaches [13], the sub-carrier shifting-based approach [14], Physical layer-based approaches [15-16], and the cryptographic-based approaches [17-22]. The AES, a cryptographic technique, has shown promising results in securing the CRN as compared to other techniques. The reference signal of the primary user is encrypted at the transmitter and decrypted at the receiver side using AES. In this work, we propose a new cryptographic-based approach, CR-AES, inspired by the conventional AES. The proposed technique enhances the security by linking the key generation and shift-rows step with the user data. The proposed algorithm also reduces the computational efficiency by reducing the rounds of AES without compromising the overall security of system.

2. ADVANCED ENCRYPTION STANDARD

The AES, proposed by Daemen and Rijmen [20], has shown superior performance over other cryptographic algorithms for different applications. The AES takes 128-bits block size and performs encryption and decryption in N rounds (N=10,12,14) using key of size 128, 192, and 256 bits. Each round performs four operations on the input block: (i) Substitute bytes, (ii) Shift rows, (iii) Mix columns, and (iv) Add round key. Fig. 1 shows the block diagram of AES encryption and decryption process. The process takes 16-bytes of user data as input. These bytes are arranged in a matrix of 4×4. The AES algorithm starts by generating 44 words (176 bytes) linear array using four-word (16 bytes) input key. Each AES round (10 rounds) utilizes four words from the linear array. Next, we discuss each block of the key-generation process and AES round:

2.1 AES Key Generation

The key expansion step generates 44 different key words from the 4-word input key. The process is iterative and generates one key word in every iteration. The key expansion algorithm is:

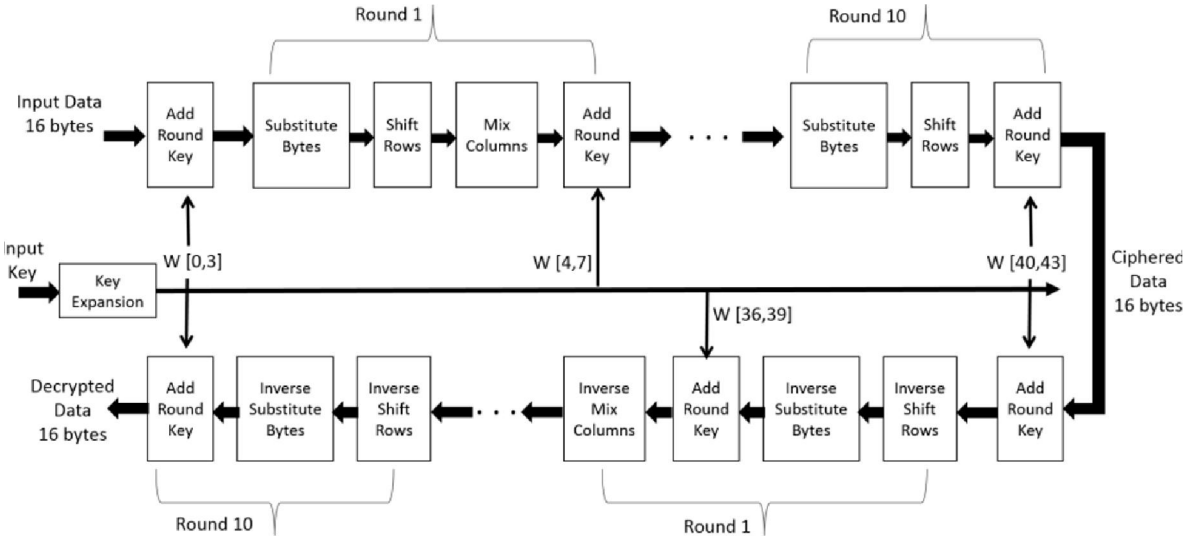

FIG. 1. BLOCK DIAGRAM OF AES

(i) Execute circular left shift of one-byte on the input word. The input word [A0,A1,A2,A3] is changed into [A1,A2,A3,A0] (Ai = ith byte).

(ii) Perform byte substitution by using S-box on each byte.

(iii) XOR the result of step 2 with Rcon (Round constant) [i/4]. The Rcon is different for each round. The values of round constant proposed in the original work [20] are shown in **Table 1**. More details on the key generation process are given in [20].

2.2 Add Round Key

During the encryption process, add round key block takes 128 bits of data as input and bitwise XOR it with 128 bit key. The process remains same during the decryption (but with reverse key order).

2.3 Substitute Bytes Transformation

In this step, a simple table, S-box, containing 16×16 bytes covering all 256 8-bit values is used to substitute the input byte with a value from the S-box. The rightmost 4 bits of the input byte are used as column address and the leftmost 4 bits used as row address. The substitute byte is then selected using these columns and row addresses.

2.4 Shift Rows Transformations

In shift row transformation, a left circular byte shift is performed. The first row of data (4 bytes) is not shifted. The second, third, and fourth row are shifted by one, two, and three bytes respectively. The process remains the same during decryption except the shift process is performed right.

2.5 Mix Columns Transformation

The mix column transformation uses arithmetic over Galois Field GF(2^8). Each byte of a column is transformed into a new value that is a function of all four bytes in that column. The inverse transformation is used for decryption process.

2.6 Limitations of AES in CRN

The conventional AES has shown promising results in many applications including CRN. However, there are few factors, listed below, that affects the performance of the AES in CRN.

(i) The process of key-generation in AES is public. It is possible for intruders to hack the 128 bits input key and generate 44 words key set.

(ii) Similarly, the process of shift rows is also public which reduces the overall security of network.

(iii) The AES process is time consuming and therefore, not suitable for real-time communications.

3. COGNITIVE RADIO-ADVANCED ENCRYPTION STANDARD

To overcome the limitations of traditional AES in CRN, we propose a new cryptography-based algorithm CR-AES. Following are the main highlights:

TABLE 1. ROUND CONSTANT (RCON) VALUES

i	1	2	3	4	5	6	7	8	9	10
Rcon[i]	01000000	02000000	04000000	08000000	10000000	20000000	40000000	80000000	1b000000	36000000

(i) In CR-AES, we introduce a new data-dependent key-expansion algorithm to enhance the security of CRN. The CRN becomes more secure as the public key-generation algorithm is replaced by the proposed data-dependent key generation algorithm.

(ii) We also introduce a new method for shift rows using information from previous data-byte. This keeps the network safe from the attackers.

(iii) We also reduce the rounds from 10-6 to increase the computational efficiency. Fig. 2 shows the process of encryption and decryption in CR-AES.

The CR-AES takes 16-bytes of user data as input. These bytes are arranged in 4×4 matrix. The proposed algorithm has six rounds where each round consists of four transformations: Substitute bytes, shift rows, mix columns, and Add Round Key. The reduction in rounds provides more computational efficiency as compared to the AES.

3.1 New Key Generation Process

The CR-AES key expansion takes four-word (16-bytes) key as input and creates a linear array of 28 words (112 bytes). This is enough to provide four-word key for every round (6 rounds) of encryption process. The proposed key-expansion process has the following steps:

(1) XOR the first word of input key with the previous data.

(2) Execute circular left shift of one-byte on the input word.

(3) Perform byte substitution by using S-box on each byte.

(4) XOR the result of step 3 with round constant, Rcon [i/4].

3.2 New Shift Rows Transformation

In CR-AES, we propose a new shift row transformation where the input data rows are shifted (left circular shift)

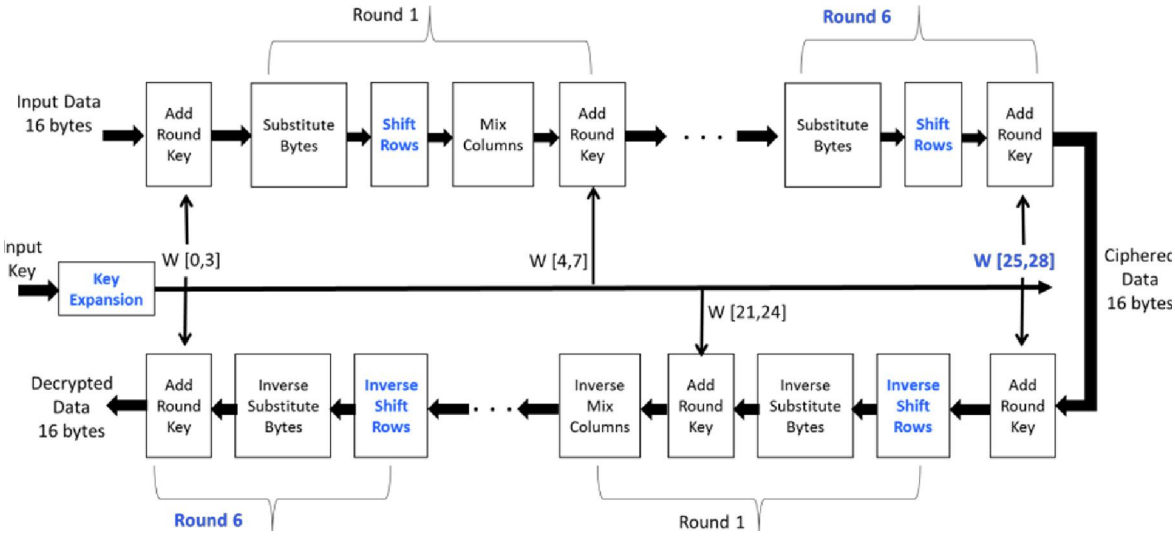

FIG. 2. BLOCK DIAGRAM OF CR-AES (NEW CONTRIBUTIONS HIGHLIGHTED IN BLUE)

according to an 8-bit shift vector which contains the last byte of previous data. The 1st row is shifted according to the value of first 2 bits, 2nd row according to the next 2 bits, and so on. The process is same during decryption except shift process is performed right.

The data is encrypted in six rounds using 28 words key. The decryption process is similar to the encryption process with reverse key order.

4. EXPERIMENTAL RESULTS

The performance of the proposed CR-AES is evaluated using the histograms and correlation (statistical test). For images, the histogram provides the distribution of pixel values/intensities. For our experiments, we have selected nine test images (i) Cameraman, (ii) House, (iii) Pepper, (iv) Building, (v) House-2, (vi) Doll, (vii) Raccoon, (viii) Parrot, and (ix) MRI-Skull. The selected images cover a variety of textures and pixel distributions and include most of the image categories used in real transmission. The images are encrypted using CR-AES and transmitted over the CRN. The received image is then decrypted at the destination node. In Figs. 3-5, we show the original and encrypted images, their histograms, and decrypted images. We observe that the frequency distribution of original images is not uniform. This type of data is prone to various security threats. The distributions of encrypted images are uniform and it is very difficult to extract any information from these images. The proposed CR-AES secures the transmitted data from the intruders. The original images are recovered at the receiver side using the CR-AES decryption.

The correlation shows the linear relationship of the two pixel values of the image. The correlation can be negative (similar but out of phase), zero (no similarity), or positive (similar and in phase). Here, we measure the correlation in horizontal, vertical, and diagonal directions. We take the average of the correlation between neighboring pixels in horizontal, vertical, and diagonal directions. The correlation of neighboring pixels in the original image is strong as compared to the encrypted images. For our test images, without CR-AES, we found the correlation values are in the range 0.80-0.95 as shown in Table 2. The values are close to 1 which shows high correlation in the data. Such data is prone to security attacks. The correlation values for encrypted images are less than 0.0299, which show almost no little correlation in data. The reduction in correlation, therefore, proves the effectiveness of the proposed algorithm.

5. CONCLUSION

In this work, we presented a cryptographic-based security technique for CRN. The proposed CR-AES overcome the limitations of traditional AES in CRN. The CR-AES enhances the security of CRN using a new data-dependent key-expansion process and a shift-rows method by using the information from previous data byte. The proposed technique also improves the overall computational efficiency by reducing the rounds from 10-6 for encryption and decryption without compromising the security of CRN. The experimental results show the superior performance of our proposed CR-AES in CRN. The histogram of the encrypted image is uniform and does not provide any information about the data. Also, the correlation is very low in the encrypted images which make the data robust in insecure channels.

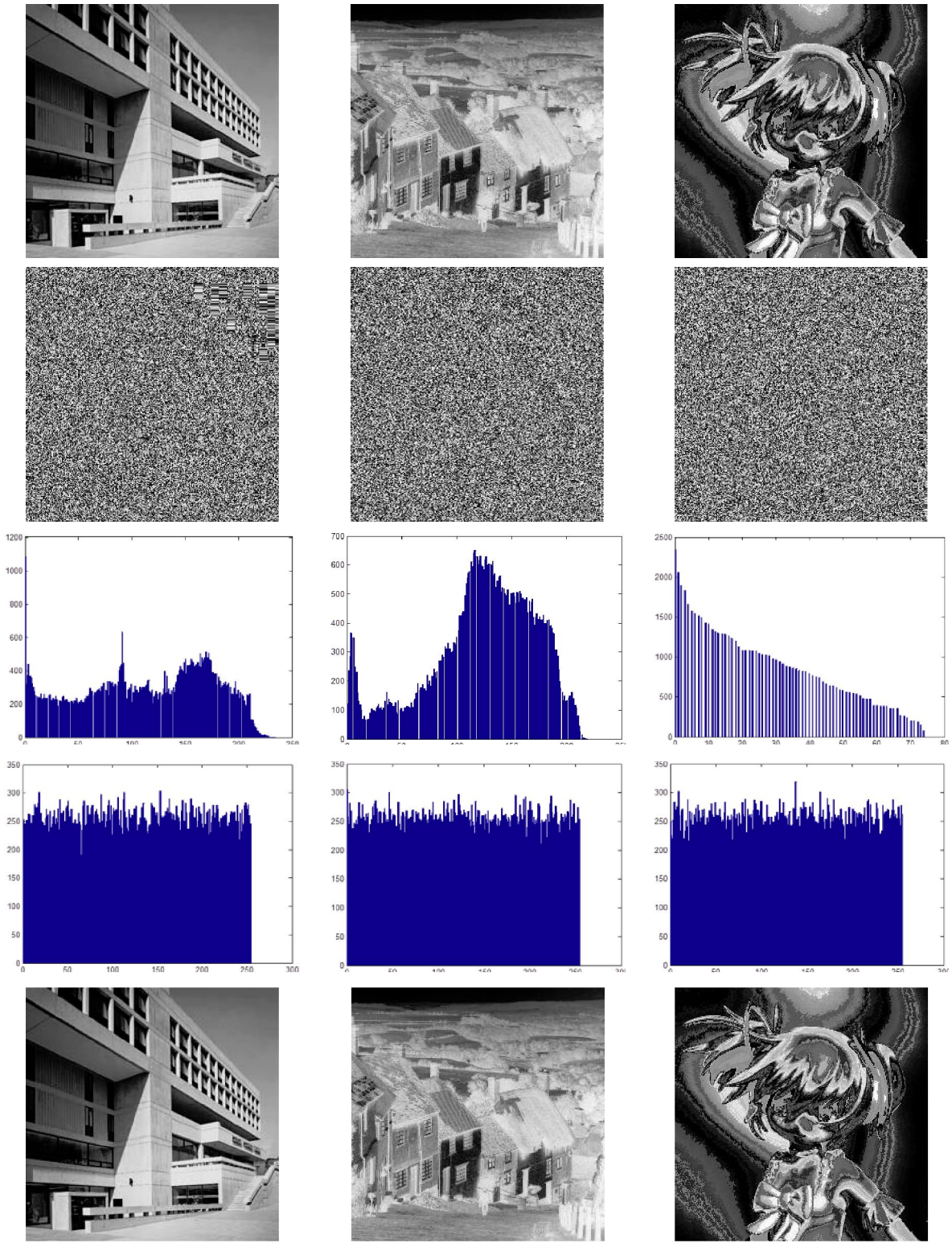

FIG. 3. ROW-1: ORIGINAL IMAGES: (I) CAMERAMAN (II) HOUSE-1 (III) PEPPER, ROW-2: ENCRYPTED IMAGES, ROW-3: HISTOGRAMS OF ORIGINAL IMAGES, ROW-4: HISTOGRAMS OF ENCRYPTED IMAGES, ROW-5: DECRYPTED IMAGES

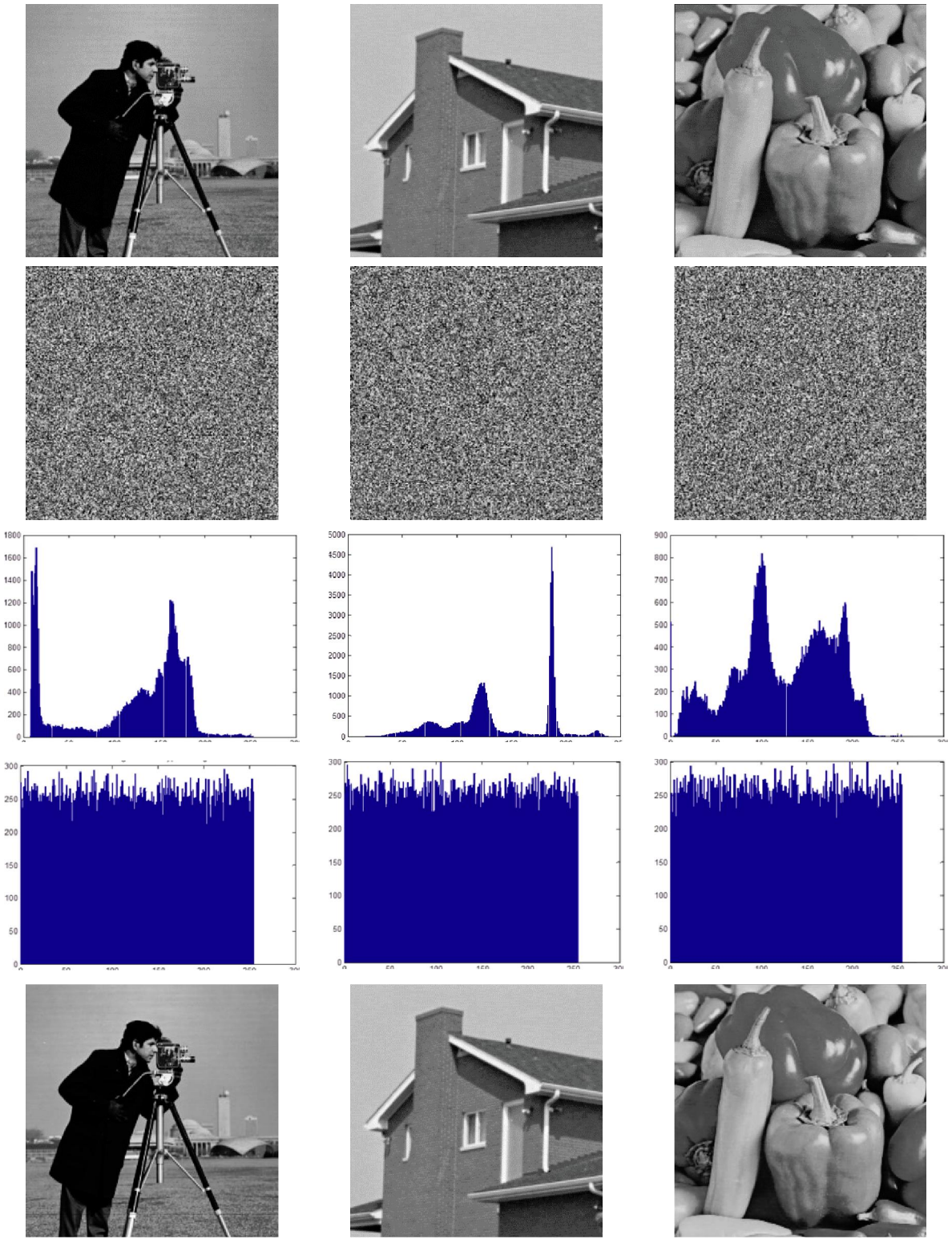

FIG. 4. ROW-1: ORIGINAL IMAGES: (I) BUILDING (II) HOUSE-2 (III) DOLL, ROW-2: ENCRYPTED IMAGES, ROW-3: HISTOGRAMS OF ORIGINAL IMAGES, ROW-4: HISTOGRAMS OF ENCRYPTED IMAGES, ROW-5: DECRYPTED IMAGES

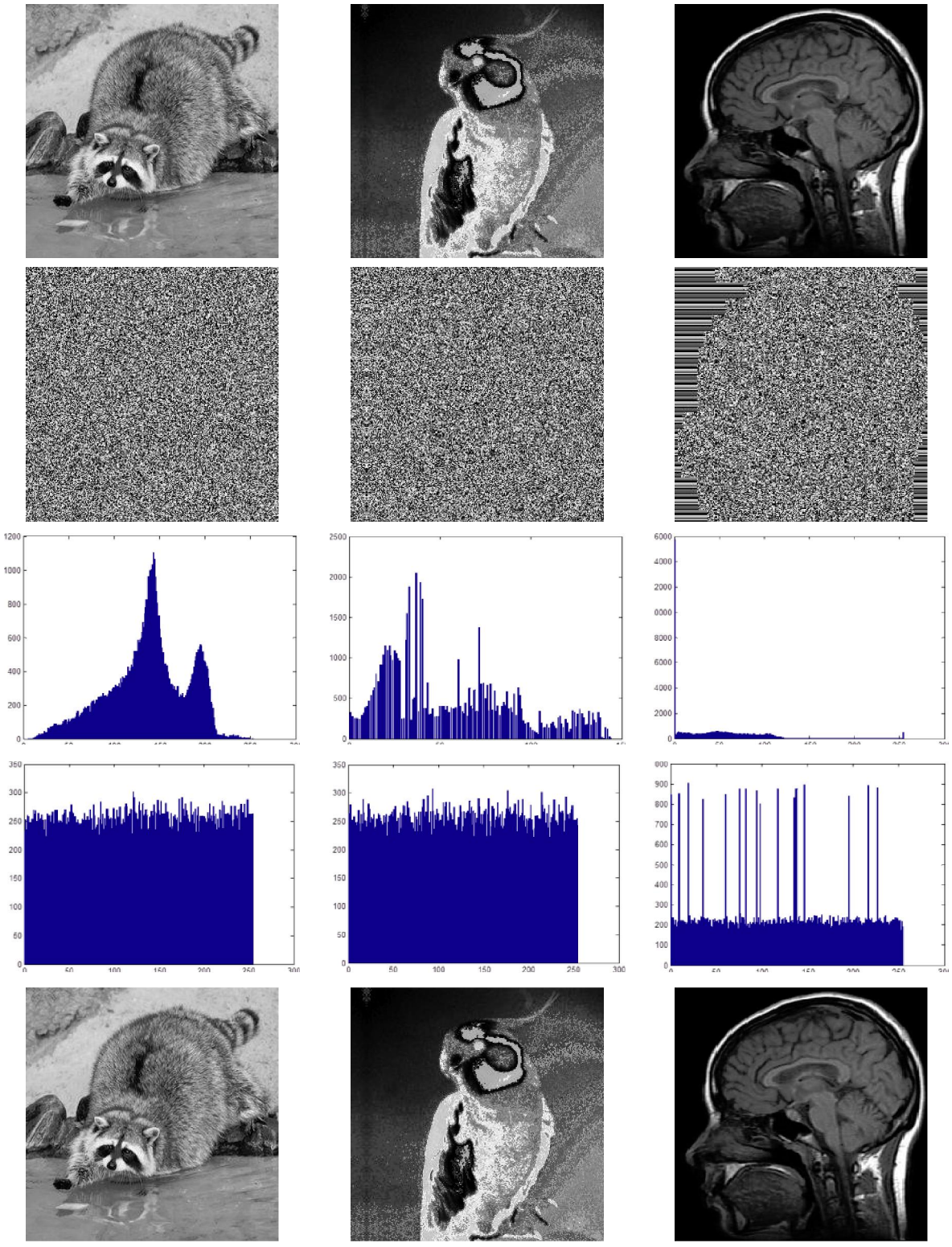

FIG. 5. ROW-1: ORIGINAL IMAGES: (I) RACCOON (II) PARROT (III) MRI SKULL, ROW-2: ENCRYPTED IMAGES, ROW-3: HISTOGRAMS OF ORIGINAL IMAGES, ROW-4: HISTOGRAMS OF ENCRYPTED IMAGES, ROW-5: DECRYPTED IMAGES

TABLE 2. CORRELATION VALUES FOR THE ORIGINAL AND ENCRYPTED IMAGES SHOWN IN FIGS. 3-5

Image	Correlation Original Image	Correlation Encrypted Image
Cameraman	0.9231	0.0104
House-1	0.9497	0.0022
Pepper	0.9253	0.0064
Building	0.9204	0.0299
House-2	0.9193	0.0087
Doll	0.8085	0.0141
Raccoon	0.8983	0.0025
Parrot	0.8655	0.0053
MRI-Skull	0.9376	0.1894

ACKNOWLEDGEMENT

The authors are thankful to the University College of Engineering & Technology, The Islamia University of Bahawalpur, Pakistan, and Mehran University of Engineering & Technology, Jamshoro, Pakistan, for providing well adequate research facilities.

REFERENCES

[1] Zhao, Q., and Sadler, B.M., "A Survey of Dynamic Spectrum Access", IEEE Signal Processing Magazine, Volume 24, No. 3, pp. 79-89, 2007.

[2] Chen, Z., Cooklev, T., Chen, C., and Pomalaza-R´aez, C., "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks", IEEE 28th International Conference on Performance Computing and Communications, pp. 208-215, 2009.

[3] Yu, R., Zhang, Y., Liu, Y., Gjessing, S., and Guizani, M., "Securing Cognitive Radio Networks Against Primary User Emulation Attacks", IEEE Network, Volume 29, No. 4, pp. 68-74, 2015.

[4] Chen, R., Park, J.-M., and Reed, J.H., "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks", IEEE Journal on Selected Areas in Communications, Volume 26, No. 1, 2008.

[5] Rehman, S.U., Sowerby, K.W., and Coghill, C., "Radio-Frequency Fingerprinting for Mitigating Primary User Emulation Attack in Low-End Cognitive Radios", IET Communications, Volume 8, No. 8, pp. 1274-1284, 2014.

[6] Pu, D., and Wyglinski, A.M., "Primary User Emulation Detection Using Frequency Domain Action Recognition", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 791-796, 2011.

[7] Saber, M.J., and Sadough, S.M.S., "Multiband Cooperative Spectrum Sensing for Cognitive Radio in the Presence of Malicious Users", IEEE Communications Letters, Volume 20, No. 2, pp. 404-407, 2016.

[8] Chen, C., Cheng, H., and Yao, Y.D., "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack", IEEE Transactions on Wireless Communications, Volume 10, No. 7, pp. 2135-2141, 2011.

[9] Nguyen-Thanh, N., Ciblat, P., Pham, A.T., and Nguyen, V.-T., "Surveillance Strategies Against Primary User Emulation Attack in Cognitive Radio Networks", IEEE Transactions on Wireless Communications, Volume 14, No. 9, pp. 4981-4993, 2015.

[10] Zou, Y., Champagne, B., Zhu, W.-P., and Hanzo, L., "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems", IEEE Transactions on Communications, Volume 63, No. 1, pp. 215-228, 2015.

[11] Maric, S., Reisenfeld, S., and Goratti, L., "A Single Iteration Belief Propagation Algorithm to Minimize the Effects of Primary User Emulation Attacks", International Symposium on Intelligent Signal Processing and Communication Systems, pp. 1-6, 2016.

[12] Yuan, Z., Niyato, D., Li, H., and Han, Z., "Defense Against Primary User Emulation Attacks Using Belief Propagation of Location Information in Cognitive Radio Networks", IEEE Wireless Communications and Networking Conference, pp. 599-604, 2011.

[13] Xin, C., and Song, M., "Detection of PUEAttacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE Transactions on Mobile Computing, Volume 13, No. 5, pp. 1022-1034, 2014.

[14] Lu, H., Zhang, L., Jiang, M., and Wu, Z., "High-Security Chaotic Cognitive Radio System with Subcarrier Shifting", IEEE Communications Letters, Volume 19, No. 10, pp. 1726-1729, 2015.

[15] Le, T.N., Chin, W.L., and Kao, W.C., "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks", IEEE Communications Letters, Volume 19, No. 5, pp. 799-802, 2015.

[16] Elkashlan, M., Wang, L., Duong, T. Q., Karagiannidis, G. K., and Nallanathan, A., "On the Security of Cognitive Radio Networks", IEEE Transactions on Vehicular Technology, Volume 64, No. 8, pp. 3790-3795, 2015.

[17] Liu, Y., Ning, P., and Dai, H., "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures", IEEE Symposium on Security and Privacy, pp. 286-301, 2010.

[18] Harini, S.V., and Aruna, T., "A Mitigation Strategy for Primary User Emulation Attacks in Cognitive Radio Networks", 10th International Conference on Intelligent Systems and Control, pp. 1-5, 2016.

[19] Alahmadi, A., Abdelhakim, M., Ren, J., and Li, T., "Mitigating Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", IEEE Global Communications Conference, pp. 3229-3234, 2013.

[20] Daemen, J., and Rijmen, V., "The Design of Rijndael: AES-The Advanced Encryption Standard", Springer Science & Business Media, 2013.

[21] Aswini, K., and Begum, S.A., "Implementation of AES and RSA for Cognitive Radio Networks", International Journal of Applied Sciences, Engineering and Management, Volume 6, No. 1, pp. 61-64, January, 2017.

[22] Alahmadi, A., Abdelhakim, M., and Ren, J., "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", IEEE Transactions on Information Forensics and Security, Volume 9, No. 5, pp. 772-781, May, 2014.