Asian Journal of Information Technology 15 (7): 1243-1248, 2016
ISSN: 1682-3915

Realization of AES with Cellular Automata Based S-Box For High-Speed Image Encyrption

[1]K.J. Jegadish Kumar, [1]S. Joseph Gladwin, [2]V. Karthick and [1]V. Vaithianathan
[1]Department of ECE, SSN College of Engineering, Kalavakkam, Tamil Nadu, India
[2]Fine Tuning RF Specialist, Gurgaon, Haryana, India

Abstract: Information security is a major issue in the field of communication systems to avert an intruder who attack the network or steal the information. Researchers are still active in designing various cryptographic algorithms to support resource constrained computing systems. Modern wireless communication channel streams multimedia information like high-quality videos, color still images, audios and requires high-speed microprocessor for fast processing and secure transmission over insecure channels. Consequently, design of high-speed processing security algorithm emerged to give solutions to Wireless Multimedia Sensor Network. Hence, this study discusses a fast image encryption by AES modified with reversible cellular automata based S-Box.

Key words: Cryptography, reversible cellular automata, image encryption, security analysis, WMSNs

INTRODUCTION

New era of computing and communication technologies are initiated to handle different types of handy devices for portable applications. These portable devices must hold portability and affordability factors on memory storage, power backup and high speed microprocessors. Regardless of the type of devices used, secured communication is a major requirement for every consumer using these devices. Advanced Encryption Standard (AES) is a standard non-feistal iterated block cipher that is most common and widely used encryption scheme in major communication standards (Daemen and Rijmen, 2002). Large code size, memory usage and computational time consumption are the major setback in the traditional AES (Cazorla *et al*., 2013). Recent trend of self-organized Wireless Sensor Network (WSN) is used to transmit multimedia information like video, still images, audio through the network called Wireless Multimedia Sensor Network (WMSN) (Misra *et al*., 2008; Gurses and Akan, 2005) . Conventional wireless sensor nodes are limited in microprocessor speed and inadequate to process the multimedia information efficiently turns out to be a challenging issue. Hence, this study discusses the image encryption using theory of cellular automata.

A Cellular Automaton (CA) is a finite array of cells in Field F_2. The cell states are updated in discrete time steps t and defined by its original state and the state of the cells surrounding it. Mathematically, a cell is defined by C = ({0,1}, f) where 'f' is a mapping function $f : \{0,1\}^n \rightarrow \{0,1\}$, where 'f' is a local transition function and 'n' is the number of cells. The CA updates the given data bit stream with specific to local transition f on each iteration (Sarkar, 2000; Nandi *et al*., 1994; Wolfram, 1986). One-dimensional CA is the two state elementary automata called "cell" array in a single row of length 'n' and its state changes when locally interacted at discrete time step't'. The state of the ith cell at time (t+1) depends on the states of (I-1)th, ith, (I+1)th cells at time 't'. Two-dimensional CA is a two state elementary array of cells with 'm' rows and 'n' columns. Each cell state is updated relatively to a local updating rule at discrete time steps.

Typical related works are: a novel scheme AES is proposed in the study (Li and Liu, 2013) for color image encryption, which is based on the two-dimensional (2-D) Henon and Chebyshev chaotic map. This study shows the modified encryption algorithm has better resistance to differential cryptanalysis. However, the researcher missed to state the computation time of the image encryption process. In the study (EI-Badawy *et al*., 2010), a new chaos AES algorithm is proposed in which the affine transformation S-Box is replaced with S-Box based on the chaos. In this study, Kun *et al*. (2009) two chaos systems are used to generate two sequences, one is used as key and the other is used to control the times of the row-shift.

The timing and security analyses of the chaos based AES algorithms are missing in the studys (Li and Liu, 2013; EI-Badawy *et al*., 2010; Kun *et al*., 2009). In this

Corresponding Author: K.J. Jegadish Kumar, Department of ECE, SSN College of Engineering, Kalavakkam, Tamil Nadu, India

study, AES constructed with Reversible Cellular Automata (RCA) based S-Box and is presented as lightweight encryption scheme to suit resource constrained computing applications. This modified AES block cipher counters the latency glitches in Advanced Encryption Standard (AES) without compromising the security level.

MATERIALS AND METHODS

Algorithm description: The Advanced Encryption Standard (AES) is the standard symmetric key block cipher endorsed by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) 197.The original Rijndael specification is iterative round based ciphers which support 128 bits data block and key sizes of 128, 192 and 256 bits. The modified AES specification is identical to the original with the block size of 128 bits and retains the option of key size of 128, 192 or 256 bits. The use of larger key sizes increases the cryptographic strength of the cipher but requires that a greater number of processing rounds be performed. The number of rounds will be 10, 12 and 14 depending on the key size of 128, 192 and 256, respectively.

For both the forward and inverse cipher, the AES algorithm uses a round function that is composed of four different byte-oriented transformations: subbytes transformation, add roundkey transformation, shift rows transformation, mix columns transformation. The detailed description of aes algorithms can be found in the literatures (Daemen and Rijmen, 2002).

Proposed RCA based S-Box: Reversible Cellular Automata (RCA) is defined as the high order CA in which the future (C_x^{t+1}) states of the grid of cells (C) are calculated using the present (C_x^t) and past (C_x^{t-1}) configuration of the cells (Kumar *et al*., 2011; Hand, 2005; Seredynski *et al*., 2004). Generally, second order CA is used to construct local transition rule function. A second order local transition rule function is defined as:

$$C_x^{t+1} = f(C_x^t, C_x^{t-1}) \tag{1}$$

The proposed S-Box design is based on Reversible Cellular Automata (RCA) function. The RCA based S-Box is constructed through the following manner: First, generate a constant matrix with the initial constant value as {63H}. Then, apply the RCA function based on the rule to the constant matrix and the state matrix (input to the S-Box). The RCA approach is depicted in matrix form as follow:

$$\begin{pmatrix} n_{0,0} & n_{0,1} & n_{0,2} & n_{0,3} \\ n_{1,0} & n_{1,1} & n_{1,2} & n_{1,3} \\ n_{2,0} & n_{2,1} & n_{2,2} & n_{2,3} \\ n_{3,0} & n_{3,1} & n_{3,2} & n_{3,3} \end{pmatrix} = f \left(\begin{bmatrix} m_{0,0} & m_{0,1} & m_{0,2} & m_{0,3} \\ m_{1,0} & m_{1,1} & m_{1,2} & m_{1,3} \\ m_{2,0} & m_{2,1} & m_{2,2} & m_{2,3} \\ m_{3,0} & m_{3,1} & m_{3,2} & m_{3,3} \end{bmatrix}, \begin{bmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{bmatrix} \right) \tag{2}$$

Where:

$\hat{m}$ = Input state matrix to S-Box with values in hexadecimal

$\hat{n}$ = Output state matrix of S-Box with values in hexadecimal

$\hat{c}$ = Constant matrix in Hex with values in hexadecimal, f-RCA function

The RCA function for Rule-30 is mathematically defined (Tripathy and Nandi, 2009) as:

$$n_i(t) = [c_i(t) \vee c_{i+1}(t) \oplus c_{i-1}(t)] \oplus m_i(t) \tag{3}$$

The RCA function for Rule-45 is mathematically defined (Tripathy and Nandi, 2009) as:

$$n_i(t) = [c_i(t) \bullet c_{i+1}(t) \oplus c_{i-1}(t) \oplus c_{i+1}(t) \oplus 1] \oplus m_i(t) \tag{4}$$

The RCA function for Rule-229 is mathematically defined as:

$$n_i(t) = [c_{i-1}(t) \bullet c_i(t) \bullet c_{i+1}(t) \oplus c_{i-1}(t) \bullet c_i(t) \oplus c_{i-1}(t) \oplus c_{i+1}(t) \oplus 1] \oplus m_i(t) \tag{5}$$

Where, the symbols $\bullet, \vee, \oplus$ represents AND, OR, XOR operation, respectively.

Algorithm to construct the constant matrix:

- Step 1: Consider the initial constant value as {63} H
- Step 2: Apply one bit cyclic left shift to the initial constant

- Step 3: Store the resulting constant in column wise and again apply the cyclic left shift to the new constant
- Step 4: Repeat step 1-3 until the 4×4 constant matrix is generated

The resultant constant matrix generated is given as:

$$\begin{bmatrix} 63 & 36 & 63 & 36 \\ C6 & 6C & C6 & 6C \\ 8D & D8 & 8D & D8 \\ 1B & B1 & 1B & B1 \end{bmatrix}$$

RESULTS AND DISUSSION

Application and analyses of proposed aes with RCA S-Box: MATLAB 7.12 (R2011) tool is used to prove the functionality of image encryption and decryption process. Colour image is chosen as plaintext of size 128-bit and are encrypted using key length of 128-bit using the proposed encryption scheme traditional AES. In addition, traditional AES algorithm is implemented to have comparative analysis with the proposed AES with RCA based S-Box. The simple image encryption process is shown in Fig. 1.

Histogram of image: The chaotic behavior of the 1-D cellular automata is highly complex and makes the statistical relationship between plaintext and ciphertext complex. The histogram of both original image and encrypted image is shown in Table 1. The histogram of encrypted image is well-distributed and completely different from the original image. Thus, the attacker cannot retrieve the key even if he has obtained some statistical relationship between the encrypted and original image.

Computational time analysis: The time taken for encryption and decryption of AES using both the LUT S-Box and RCA S-Box are measured and some manual calculations are done to find the required number of CPU cycles. For standard AES:

Average time taken for a
single ineration $(t_i) = 1.275$ sec
CPU clock frequency = 2.4 GHz

Then the CPU clock time is:

$$t_{clk} = \frac{1}{2.4\times10^{9}} = 0.4166 \text{ ns}$$

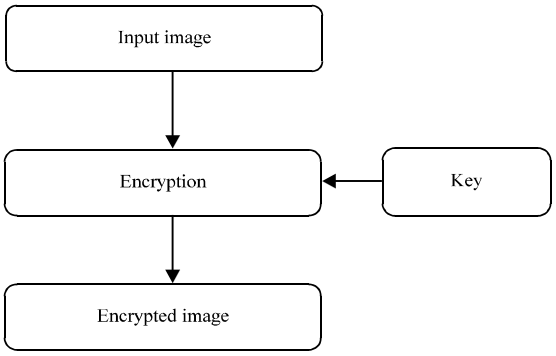
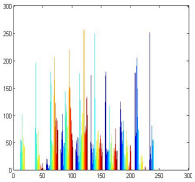
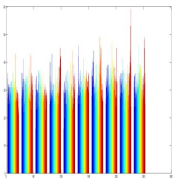
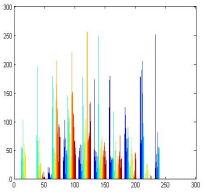
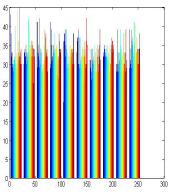


Fig. 1: Process of image encryption

Table 1: Histogram of the original image and encrypted image of the proposed encryption scheme and implemented traditional AES

	Histogram	
Parameters	Original image	Encrypted image
Colour Image: Lena (256×256)		
AES with RCA S-Box		
Traditional AES		

The number of CPU cycles required per iteration:

$$\frac{t_i}{t_{clk}} = \frac{1.275}{0.4166\times10^{-9}}$$

For RCA S-Box implemented AES:

Average time taken for
a single ineration $(t_i) = 0.203$ sec
CPU clock frequency = 2.4 GHz

Then, the CPU clock time is:

$$t_{clk} = \frac{1}{2.4\times10^{9}} = 0.4166 \text{ ns}$$

The number of CPU cycles required per iteration:

$$\frac{t_i}{t_{clk}} = \frac{0.203}{0.4166\times10^{-9}} = 0.487\times10^{9} \text{ clock cycles}$$

From the computational time analysis, it is apparent that the proposed RCA S-Box implemented AES algorithm requires 93.34 % less number of clock cycles per iteration. Hence, the proposed AES with RCA Based S-Box is time optimized than the standard AES.

Security analyses of the proposed encryption scheme

PSNR analysis: Peak Signal to Noise Ratio (PSNR) is a measure of quality of reconstruction which is an approximation to human perception. In other words, PSNR is most commonly used to measure the quality of reconstruction of lossy compression codec (e.g., for image compression). In this case, PSNR is measured to represent the quality of encrypted image. The PSNR is calculated using the given Eq. 6:

$$PSNR = 10\,Log\left[\frac{m\times n\times 255^{2}}{\sum_{i=1}^{m}\sum_{j=1}^{n}\left[M(i,j)-M(i,j)\right]^{2}}\right] \quad (6)$$

The PSNR value tabulated in Table 2 is computed between original and the encrypted image for both the proposed encryption scheme and traditional AES. If the PSNR value is high means quality of encryption is poor, low means the quality of encryption is good.

Statistical characteristics analysis: Statistical correlation is a measure that states strength of linear relationship between two random variables (Li and Liu, 2013). Let 'x' and 'y' are two random variables, each consisting of n elements, correlation coefficient of the two random variables is calculated by Eq. 7:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (7)$$

Where:

$$cov(x,y) = \frac{1}{n}\sum_{n=1}^{n}\left[x_i - E(x)\right]\left[y_i - E(y)\right]$$

Table 2: Comparison of peak signal to noise ratio

Algorithm	PSNR (dB)
Traditional AES	8.0159
AES with RCA S-Box	8.2638

Table 3: Correlation coefficient of the original image and the encrypted image of different algorithm

Algorithm	Horizontal correlation coefficient	Vertical correlation coefficient	Diagonal correlation coefficient
Original image	0.9423	0.960500	0.885600
Encrypted image			
AES with RCA S-Box	0.003613	0.006376	0.004115
Traditional AES	0.007964	0.072856	0.002364
AES Chaos algorithm Li and Liu (2013)	0.005080	0.000050	0.001699
AES Chaos algorithm El-Badawy *et al.* (2010)	0.007539	0.012878	0.004914
AES Chaos algorithm Kun *et al.* (2009)	0.011718	0.002639	0.001069

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}\left[x_i - E(x)\right]^{2},$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i$$

To determine the correlation of pixels in the encrypted image, the correlation coefficient is calculated between two horizontally neighboring pixels [f(x, y) and f(x, y+ 1)], two vertically neighboring pixels [f(x, y) and f(x+1, y)] and two diagonally neighboring pixel [f(x, y) and f(x+1, y+1)] by selecting 1000 pairs of neighboring pixels in each direction (vertical, horizontal and diagonal), each for original image and encrypted image. In any natural-image, neighboring pixels have a strong linear relationship. It is characterized by a high correlation coefficient (close to +1 or -1). Table 3 shows that it is true that the correlation coefficient in the original image is close to 1 and the correlation coefficient between original and encrypted image is close to zero.

The correlation of the horizontal direction is shown in Fig. 2a is the original image and Fig. 2b is the encrypted image. The correlation between the adjacent pixels in the encrypted image is almost low compared to the original image. Hence, the proposed encryption scheme has a strong ability of anti-statistical characteristic analysis.

Differential cryptanalysis: The basic requirement in all image encryption schemes is that the encrypted image should be greatly different from its original appearance (Sarkar, 2000). To test this influence, number of pixels change rate (NPCRRGB) using Eq. 8 is measured and the unified average changing intensity (UACIRGB) for the encrypted images is measured using Eq. 9 (Sarkar, 2000).

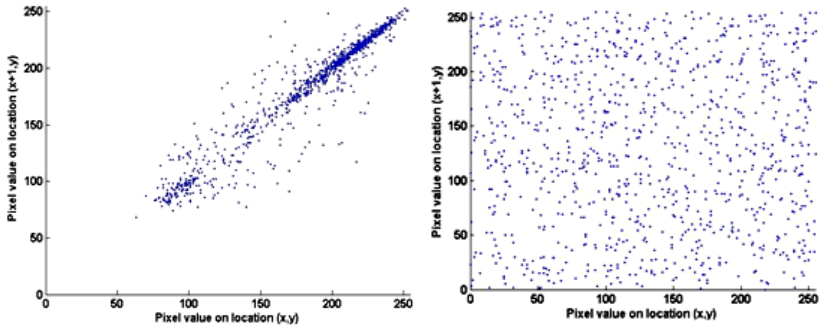


Fig. 2: Correlation of horizontal pixels in: a) Original image and b) Encrypted image

Table 4: $NPCR_{RGB}$ and $UACI_{RGB}$ values of different algorithms

Algorithms	AES with RCA S-Box	Traditional AES	AES Chaos algorithm Li and Liu (2013)	AES Chaos algorithm El-Badawy *et al.* (2010)	AES Chaos algorithm Kun *et al.* (2009)
$NPCR_{RGB}$	0.99738	0.99436	0.99683	0.99607	0.0003814
$UACI_{RGB}$	0.33674	0.33154	0.33464	0.33463	0.0000457

The definition of $NPCR_{RGB}$ is:

$$NPCR_{RGB} = \frac{\sum_{i,j} D_{RGB}(i,j)}{W \times H} \times 100 \quad (8)$$

The definition of $UACI_{RGB}$ is:

$$UACI_{RGB} = \frac{1}{W \times H}\left[\frac{\sum i,j \left| C_{RGB}(i,j) - C'_{RGB}(i,j) \right|}{255}\right] \times 100 \quad (9)$$

Where:

'W' = The width of the encrypted image
'H' = The height of the encrypted image
C_{RGB} and C_{RGB} = Two encrypted images are used which are different by only one pixel

A2-D array D which is also same size as C_{RGB} (i,j) and C_{RGB} (i,j). If $C_{RGB}(i,j) = C_{RGB}(i,j)$, then $D_{RGB}(i,j) = 0$ otherwise $D_{RGB}(i,j) = 1$ (Sarkar, 2000). For high resistance to differential attack in ideal cipher systems, the computed $NPCR_{RGB}$ and $UACI_{RGB}$ values should be high enough. To test the proposed encryption scheme each color component is encrypted first. Then one similar pixel in each component is taken randomly and shuffled. The modified component is encrypted again using the same key so as to generate the new modified encrypted component. The calculated $NPCR_{RGB}$ and $UACI_{RGB}$ the proposed AES with RCA S-Box and implemented traditional AES is shown in Table 4.

Obviously from the simulation results, the proposed encryption scheme offers better performance as the computed $NPCR_{RGB}$ = 0.99738 and $UACI_{RGB}$ = 0.33674. This shows the proposed encryption scheme can well resist the known-plaintext and the chosen-plaintext attacks.

CONCLUSION

In this study, a lightweight AES using RCA based S-Box is proposed to ensure fast and secure image encryption compared to traditional AES. The simulation results gives suitable study of PSNR, correlation coefficient and differential cryptanalysis to indicate the nature of the proposed AES with RCA S-box is more efficient and practically secure. So, it can be concluded that this proposed scheme is particularly suitable for wireless multimedia sensor networks as it offers high speed of computations with adequate level of security.

ACKNOWLEDGEMENTS

This research is supported by Research Foundation of SSN Institution.

REFERENCES

Cazorla, M., K. Marquet and M. Minier, 2013. Survey and benchmark of lightweight block ciphers for wireless sensor networks. Proceedings of the 2013 International Conference on IEEE Security and Cryptography (SECRYPT), July 29-31, 2013, IEEE, Reykjavik, Iceland, pp: 1-6.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES-The Advanced Encryption Standard. Springer, New York, USA., ISBN-13: 9783540425809, Pages: 238.

El-Badawy, E.S.A.M., A. Mokhtar, W.A. El-Masry and A.E.D.S. Hafez, 2010. A new chaos advanced encryption standard (AES) algorithm for data security. Proceedings of the International Conference on Signals and Electronic Systems (ICSES), September 7-10, 2010, IEEE, Gliwice, Poland, ISBN: 978-1-4244-5307-8, pp: 405-408.

Gurses, E. and O.B. Akan, 2005. Multimedia communication in wireless sensor networks. Ann. Telecommun., 60: 799-827.

Hand, C., 2005. Simple cellular automata on a spreadsheet. Comput. Higher Educ. Econ. Rev., Vol. 17,

Kumar, K.J., K.C.K. Reddy and S. Salivahanan, 2011. Novel and Efficient cellular automata based symmetric key encryption algorithm for wireless sensor networks. Intl. J. Comput. Appl., 23: 30-37.

Kun, Y., Z. Han and L. Zhaohui, 2009. An improved AES algorithm based on chaos. Proceedings of the International Conference on Multimedia Information Networking and Security MINES'09, November 18-20, 2009, IEEE., Hubei, Chinese, ISBN: 978-0-7695-3843-3, pp: 326-329.

Li, J. and H. Liu, 2013. Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map. IET Inform. Secur., 7: 265-270.

Misra, S., M. Reisslein and G. Xue, 2008. A survey of multimedia streaming in wireless sensor networks. IEEE Commun. Surv. Tutorials, 10: 18-39.

Nandi, S., B.K. Kar and P. Pal Chaudhuri, 1994. Theory and applications of cellular automata in cryptography. IEEE Trans. Comput., 43: 1346-1357.

Sarkar, P., 2000. A brief history of cellular automata. ACM Comput. Surv., 32: 80-107.

Seredynski, M., K. Pienkosz and P. Bouvry, 2004. Reversible cellular automata based encryption. In: Network and Parallel Computing Proceedings. Hai, J., R. Guang, Z.X. Gao and C. Hao (Eds.). Springer, Berlin, Heidelberg, Germany, ISBN: 978-3-540-23388-6, pp: 411-418.

Tripathy, S. and S. Nandi, 2009. Lightweight cellular automata-based symmetric-key encryption. I. J. Netw. Secur., 8: 243-252.

Wolfram, S., 1986. Cryptography with cellular automata. Proceedings of the Advances in Cryptology, August 18-22, 1986, Springer-Verlag, Santa Barbara, CA., USA., pp: 429-432.