Image Encryption and Analysis using Dynamic AES

*

1st Amandeep Singh
Department of Computer Science
Baba Farid College
Bathinda, India
amanharar@gmail.com

2nd Praveen Agarwal
Department of Mathematics
Anand International College of Engineering
Jaipur, India
goyal.praveen2011@gmail.com

3rd Mehar Chand
Department of Mathematics
Baba Farid College
Bathinda, India
mehar.jallandhra@gmail.com

***Abstract*—AES (Advanced Encryption Algorithm) is a block cipher, which is world wide implemented for encryption of data. It has been accepted as a standard for data security since 2001. AES is a substitution and permutation cipher, which provides confusion by using substitution box (S-Box) in the algorithm. The main drawback of AES is that it uses static S-Box throughout algorithm, which compromise the security of AES and may be exposed to different algebraic attacks. So to overcome this problem new Dynamic AES algorithm developed by key dependent dynamic S-Box using dynamic irreducible polynomial and affine constant. The analysis is done on gray scale and colour images. Both the images are encrypted and decrypted by using standard AES and Dynamic AES. Quality of algorithm and the level of security is analyzed based on the parameters like Image Histogram Analysis, Adjacent Pixel Correlation Analysis, Image Entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Encryption Quality.**

***Index Terms*—AES, Dynamic AES, NPCR, UACI, Encryption Quality, Image Entropy**

I. Introduction

Advanced encryption standard (AES) is one of the widely used symmetric encryption algorithm. It is an encryption standard adopted by the US government. AES was developed by Joan and Vincent Rijmen. AES uses the Rijndael block cipher. AES encrypts a 128 bit fixed size block at once. To encrypt 128 bit size block AES uses variable key sizes like 128 bit, 192 bit and 256 bit to attain different level of security. AES works on different encryption rounds dependent upon key size like 10 round encryption for 128 bit key size [1], 12 rounds encryption for 192 bit key bits [2] and 14 round encryption for 256 bit key size [3]. Each round has 4 different processing steps except the last round, which has 3 steps. These 4 steps consists of byte substitution, shift row operation, mix column operation and add round key operation. For encryption these 4 steps are used in each round and for decryption the inverse of these steps are used these are inverse substitution byte, inverse shift row, inverse mix column and inverse add round key. All the steps are explain briefly as under. The AES is shown in Fig. 1.

- *The Byte Substitution Transformation :* Byte substitution is a non-linear substitution layer of AES. It consists of 16×16 matrix consists elements ranging 0 to 255, which provides confusion properties. This matrix is calculated by taking multiplicative inverse in GF(2^8). In encryption process Byte substitution is applied on 4×4 initial stage matrix and an intermediate matrix is calculated then an affine transformation is done in intermediate matrix to calculate the next state matrix. In decryption inverse byte substitution matrix and inverse affine transformation process is applied.
- *The Shift Row Transformation :* A Shift row is a linear diffusion layer that operates on individual rows in a 4×4 state matrix. In encryption left circular shifts are done on each row of the state matrix except first row. One, two and three left shifts are done on 2nd, 3rd and 4th row of the state matrix respectively. In decryption process inverse shift row operation is used in which the circular shifts are done in right direction.
- *The Mix Column Transformation :* In mix column operation a fixed matrix column matrix is multiplied in GF(2^8) to the state matrix. In which all the bytes of state matrix are treated as polynomials. In decryption process inverse mix column matrix is used.
- *Add Round Key:* In add round key the bytes of state matrix and XORed with bytes of the round key. In encryption on each round a round key is generated from initial key this process is called key expansion schedule. This schedule is used in reverse order in decryption process.

II. Related Work

In recent years many researches developed various approaches to make AES dynamic by introducing Dynamic S-Boxes.

Krishnamurthy et al. they used S-Box rotation and added it as an extra stage in existing AES algorithm to make S-Box dynamic. They also generated 3 stages of algorithm in which the S-Boxs are rotated on the basis of a fixed key value, partial key values and whole key values to enhance security [4]. *Piotr Mroczkowski* The algorithm based on chancing S-Boxes. To make it possible pseudorandom sequences was used to generate identical S-Boxes for data encryption and decryption [5]. *Abd-ElGhafar et al.* they used RC4 algorithm to generate key dependent S-Boxes. In this algorithm S-Box values are dependent on input key [6]. *Kazlauskas et al.* they analyzed the

ISBN: 978-1-7281-1482-8/19/$31.00 ©2019 IEEE

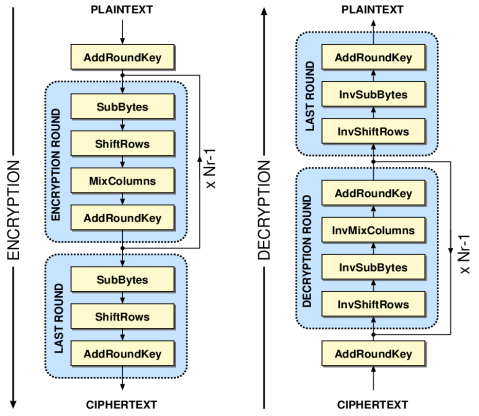


Fig. 1: AES Algorithm

AES algorithm, S-boxes, linear and differential cryptanalysis and proposed key-dependent S-Boxs and inverse S-Boxes [7]. *Ghada Zaibi et al.* they used one-dimensional chaotic maps to generate key dependent dynamic S-Boxes [8]. *Jie Cui et al.* they modified affine transformation of AES algorithm. The results improved affine transformation period, iterative period and distance to SAC [9]. *Anna Grocholewska-Czurylo* they used random irreducible polynomial to construct 8×8 dynamic S-Boxes [10]. *Julia Juremi et al.* they modified key expansion module of AES algorithm to generate dynamic S-boxes [11]. *Razi Hosseinkhani et al.* they used cipher key to generate dynamic S-Boxes [12]. *Oleksandr Kazymyrov et al.* they used gradient descent method for improving nonlinear vectorial Boolean functions in AES algorithm [13]. *Mona Dara et al.* they used cipher key and chaotic logistic maps to generate AES S-Boxes [14]. *Eman Mohammed Mahmoud et al.* they used PN Sequence generator and LFSR (Linear Feedback Shift Register) to generate dynamic S-Boxes [15]. *Sliman Arrag et al.* they enhanced S-Box complexity by using nonlinear transformation algorithm. Further they also modified Key expansion schedule and used S-Box lookup table to make S-Box dynamic [16]. *Fatma Ahmed et al.* they generated S-Boxes by using dynamic key MDS matrix (SDK-AES) and used as S-boxes bank for randomly selecting S-Boxes in algorithm [17]. *Adi Narayana Reddy K et. al* they used secrete value to the static index to shift the S-Box to a secrete location. To enhance further security they used random number generator to generate sub keys in key expansion module of algorithm [18]. *Kazlauskas et al.* they generated a key dependent S-Boxes by modifying existing AES algorithm and they further claim that the new generated algorithm is faster [19]. *Balajee Maram et al.* they generated key dependent S-Boxes by using Pseudo-Random generator. They further claimed that their algorithm generates S-Boxes faster than other available algorithms [20]. *Shishir Katiyar et al.* they generated dynamic S-Boxes by using one dimensional logistic maps [21]. *Tianyong Ao et al.* they made affine transformation key dependent to generate dynamic S-Boxes for their algorithm [22].

In above mentioned work some authors have used their proposed algorithms to analysis images.

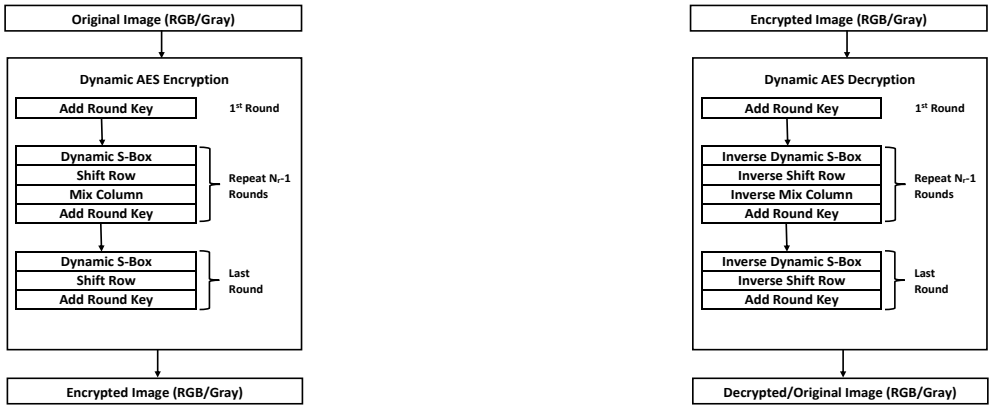
Krishnamurthy et al. they used gray scale image of size (0-255). They encrypted and decrypted image using their algorithm. The image quality their algorithm got 128.773438 as compared to AES i.e. 128.109375. The correlation factor they got 0.032304 as compared to AES i.e. 0.048484 [4]. *Abd-ElGhafar et al.* they did hectogram analysis of bit map picture image by using their algorithm AES-RC4 and compared with standard AES and found that both the encrypted image hectogram are identical and shows uniform pixel distribution [6]. *Ghada Zaibi et al.* they used gray scale image for analysis by using their algorithm and found that both AES and their algorithm gave uniform pixel distribution in hectogram analysis [8]. *Eman Mohammed Mahmoud et al.* used moon.tif file and did hectogram analysis of encryption both by their AES-128 key dependent algorithm and AES. Both hectograms showed randomness of pixels and showed significant difference from original image hectogram [15]. *Shrija Somaraj et al.* they used bit plain algorithm to analysis image. They used Cameraman.tif image of size 256×256 pixels. The hectogram analysis shows good randomness in pixels. Correlation coefficient of encrypted image shows values 0.0456, -0.0568 and -0.0202 for horizontal, vertical and diagonal pixels correlation. Encryption quality (EQ) for encrypted image is 290.0156. UACI and NPCR values of encrypted image shows values 17.5430 and 97.7814 respectively [25]. *Unal avusoglu et al.* they used chaos based S-Box algorithm for image analysis. They used Crowd.jpg image of size 256×256. They obtained NPCR values 99.60672 for chaos algorithm and 99.63245 for AES, UACI values 31.24768 for chaos algorithm 31.8723631 for AES, Information entropy 7.95454 for chaos algorithm and 7.95912 for AES. Encryption quality values 296.7574 for chaos and 358.4217 for AES [24].

III. Proposed Dynamic AES Algorithm

In existing work researchers have given good contribution in making AES dynamic by introducing dynamic S-Boxes. Further in this work we developed a new Dynamic AES in which we not only make S-Boxes key dependent but also dependent on dynamic irreducible polynomial and affine constant [23].

The proposed Dynamic Key Dependent S-Box algorithm is a permutation of existing AES S-Box. The Dynamic AES algorithm is dependent on three parameters i.e. key values, irreducible polynomial and affine constant.

- **Key** The construction of S-Box is dependent on key values. S-Box is highly sensitive to key values, if there is a single bit of key change then all values of S-Box will be permuted.
- **Irreducible Polynomial** In existing AES only one irreducible polynomial is used to generate S-Box. But there are other irreducible polynomials which may be used to construct S-Boxes. In Dynamic AES we used all possible irreducible polynomials in random way to generate dynamic S-Boxes.



(a) Encryption Algorithm

(b) Decryption Algorithm

Fig. 2: Dynamic AES

- **Affine Constant** In existing AES only one affine constant i.e. 63 is used to generate S-Box. But there are total 256 affine constants, which may be used to construct S-Boxes. In Dynamic AES we used all possible affine constants in random way to generate dynamic S-Boxes.

By using above methodology we developed Dynamic AES algorithm generates dynamic S-Boxes, which are highly sensitive to these three inputs. By using this methodology the algorithm is capable to generate 256! dynamic S-Boxes. Dynamic AES for encryption of gray scale and colour images is shown in Fig. 2.

IV. Image Analysis with AES and Dynamic AES

Here, we are implementing new developed Dynamic AES to encrypt and decrypt a gray scale as well as colour scale image. The performance of the same compared with the standard AES on the basis of parameters like Histogram Analysis, Adjacent Pixel Correlation Analysis, Image Entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Encryption Quality. In this test we are using a gray scale image 'Secenry.jpg' and a colour scale image 'colours.bmp'. Fig. 3a shows the original gray scale image, Fig. 3b shows the encrypted version of gray scale image with standard AES and Fig. 3c shows the encrypted version of gray image with Dynamic AES. Both encrypted images do not give any information of original image.

Similarly Fig. 6a shows the original colour scale image, Fig. 6b shows the encrypted version of colour scale image with standard AES and Fig. 6c shows the encrypted version of colour image with Dynamic AES

A. Histogram Analysis:

The histogram graph shows the number of pixels in an image at different intensity values. For a good encryption, the distribution of pixels of an encrypted image should be uniform or balanced. For this analysis gray scale and colour images are encrypted by both standard AES and Dynamic AES. The histograms are shown in Fig. 4 and Fig. 7. In the histogram analysis of original gray scale image in Fig. 4a and colour scale image in Fig. 7a one can analyze that the pixel distribution is not uniform or unbalanced. The histograms of encrypted gray scale image and color image by standard AES are shown in Fig. 4b and Fig. 7b respectively. The histograms of encrypted gray scale image and color image by Dynamic AES are shown in Fig. 4c and Fig. 7c respectively. The analysis of these histograms shows that the pixels distribution in both encrypted images by standard AES and Dynamic AES are uniform or balanced. Both the algorithms performed well in encrypting gray scale and color images.

B. Adjacent Pixel Correlation Analysis:

Correlation is a relationship of two adjacent pixel values in an image [25], [27]. If there is a liner relationship among the pixels of an image then there is a close correlation among the pixels on the other hand if there is non-liner relationship among the pixels then there is less correlation among the pixels. To analyze the correlation factor in original and encrypted images, we consider the horizontal, vertical and diagonal adjacent pixel correlation. Correlation coefficient of an image is calculated through Equation 1 to Equation 5, where a and b are adjacent pixel values, N is the number of chosen pixel pairs.

$$cc = \frac{cov(a,b)}{\sigma a \times \sigma b} \tag{1}$$

$$where\ \sigma\ a = \sqrt{var(a)} \tag{2}$$

$$\sigma\ b = \sqrt{var(b)} \tag{3}$$

$$var(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))^2 \tag{4}$$

$$cor(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i - E(a))(b_i - E(b)) \quad (5)$$

Fig. 5a shows the correlation histogram of original gray scale image, Fig. 5b Shows the correlation histogram of encrypted image by standard AES and Fig. 5c shows the correlation histogram of encrypted gray scale image by Dynamic AES. Similarly Fig. 8a shows the correlation histogram of original colour scale image, Fig. 8b Shows the correlation histogram of encrypted colour image by standard AES and Fig. 8c shows the correlation histogram of encrypted colour image by Dynamic AES. The analysis of horizontal, vertical and diagonal adjacent pixel correlation shows close correlation among the pixels of both original gray scale and colour images whereas less correlation among the encrypted images. So both algorithms are very close in terms of pixel correlation analysis. The same is shown in Table I.

TABLE I: Correlation Coefficient Analysis

Image Type	Original Image			Encrypted Image					
				AES			Dynamic AES		
	Horizontal	*Vertical*	*Diagonal*	*Horizontal*	*Vertical*	*Diagonal*	*Horizontal*	*Vertical*	*Diagonal*
Gray Scale Image	0.9248	0.8848	0.8582	-0.00216	0.00318	-0.00172	0.00263	0.00236	-0.00013
RGB Image	0.9908	0.9891	0.9768	-0.00105	0.00216	0.00164	-0.00097	-0.00022	-0.00169

C. Information Entropy Analysis:

Used to check the complexity of an encrypted data where encrypted data must be complex therefore it should not provide any clue of original data. Information entropy is calculated by Equation 6.

$$En(y) = -\sum_{i=1}^{N}(p_i(y))^2(\log_2 p_i(y)))^2 \quad (6)$$

The entropy value should be closer to value 8 [24], [29]. If the value is closer to 8 the quality of encrypted data is higher. Entropy information of gray scale image and colour image encrypted by standard AES and Dynamic AES are shown in Table II. The results are close to 8, which shows the higher encryption complexity.

D. NPCR and UACI Analysis:

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are the methods to analyze the resistance of encrypted data against various differential attacks [24], [26]. These are used to check that how small changes in original image will effect encryption. These methods compares original image and encrypted image data and find that how much they are different from each other. To attain good encryption there should be big change in original image and encrypted image data to resist various differential attacks. NPCR score are calculated with Equation 7 and Equation 8.

$$NPCR(X,Y) = \left(\sum_{p,q} D(p,q)/N\right)100\% \quad (7)$$

$$D(p,q) = \begin{cases} 1 \; if X(p,q) \neq Y(p,q) \\ 0 \; if X(p,q) = Y(p,q) \end{cases} \quad (8)$$

To calculate NPCR score consider two images, whose corresponding original image and encrypted image, be denoted by X and Y. A bipolar array, D with the same size as image X and Y. Then, $D(p,q)$ is determined by $X(p,q)$ and $Y(p,q)$. For example if $X(p,q) = Y(p,q)$ then $D(p,q) = 0$; otherwise, $D(p,q) = 1$. The optimal value of NPCR is 99.61% [25], [28]. UACI defines the average density between two image in Equation 9. $X(p,q)$ and $Y(p,q)$ represent the previous and following pixels, N represents total pixel number, L represents the bit number that describes the pixel of the image. The NPCR and UACI score of gray scale and colour image are shown in Table II. So both the standard AES and Dynamic AES has good NPCR and UACI scores.

$$UACI(X,Y) = \frac{1}{N}\left(\sum_{p,q}\frac{(|X(p,q) - Y(p,q)|)}{2^L - 1}\right)100\% \quad (9)$$

E. Encryption Quality:

Encryption quality of an encrypted image is calculated by comparing the pixels of encrypted and original image [24], [25]. The encryption quality is higher if the change in pixel values of encrypted image and original image is higher. The EQ is calculated with Equation 10. In this equation PI is original image and CI is encrypted image.

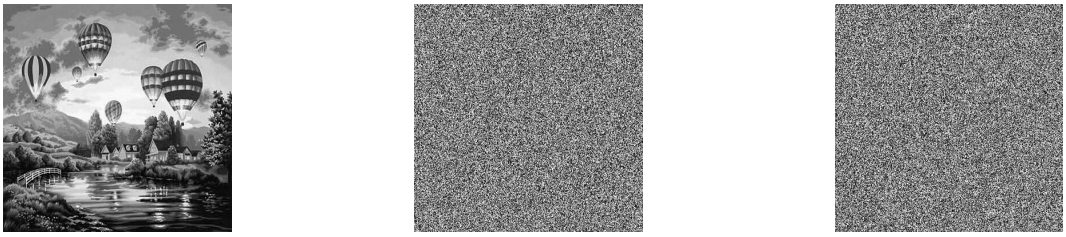
$$EncryptionQuality = \frac{\sum_{L=0}^{255}|H_L(CI) - H_L(PI)|}{256} \quad (10)$$

TABLE II: Image Encryption Quality Analysis:

Algorithm	Image Type	Entropy	NPCR	UACI	EQ
AES	*Gray Scale*	7.99938	99.62225	35.23801	428.8594
	RGB	7.99937	99.62185	35.20152	642.3984
Dynamic AES	*Gray Scale*	7.99985	99.61677	32.21847	434.9531
	RGB	7.99938	99.60502	35.15426	637.7422

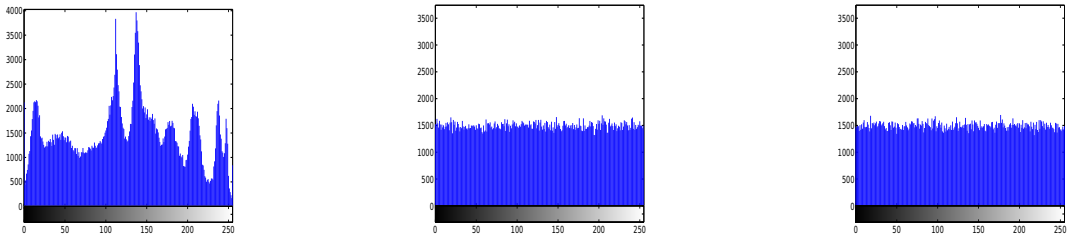
V. Conclusion

We introduced algorithm which generates dynamic key dependent S-Boxes with dynamic irreducible polynomial and affine constant. New Dynamic AES and standard AES algorithms are used to encrypt and decrypt colour and gray scale images. It is observed that both algorithms performed well in terms of histogram analysis, adjacent correlation coefficient analysis, encryption quality, information entropy, NPCR and UACI tests. In adjacent correlation coefficient analysis Dynamic AES performed well as compared to standard AES.



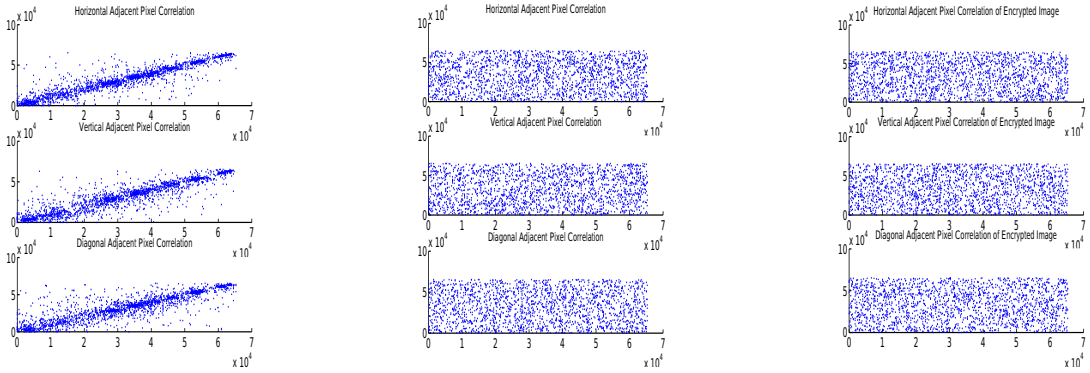
(a) Orignial Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 3: Gray Scale Image Encryption Decryption



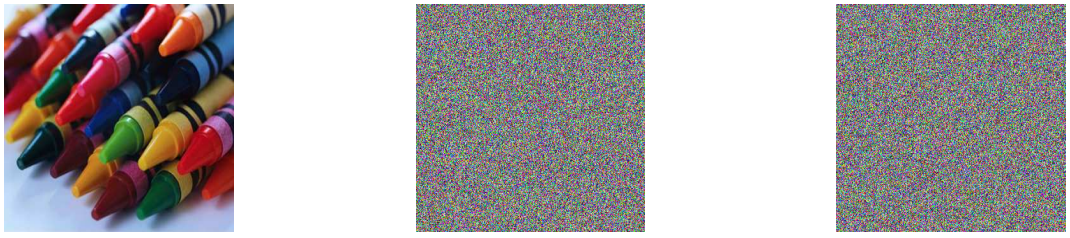
(a) Original Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 4: Histogram Analysis of Gray Scale Image



(a) Original Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 5: Horizontal, Vertical and Diagonal Correlation Analysis of Gray Scale Image



(a) Orignial Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 6: Colour Image Encryption Decryption

REFERENCES

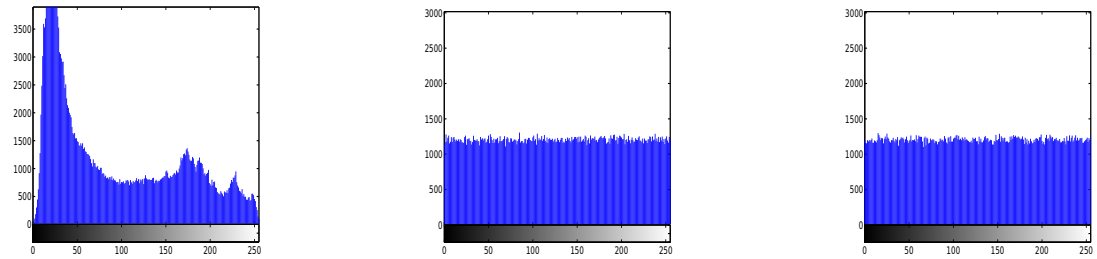
[1] J. Daemen and V. Rijmen, "The Design of Rijndael: AES The Advanced Encryption Standard," *Springer-Verlag*. 2002.

[2] J. Daemen and V. Rijmen, "The block cipher Rijindael," *In*: Proceedings of the Third International Conference on smart card Research and Applications. *CARDIS98*. vol. 1820, pp. 277-284, 2000.

[3] Federal Information Processing Standards Publications (FIPS 197), Advanced Encryption Standard (AES), 26 Nov. 2001.

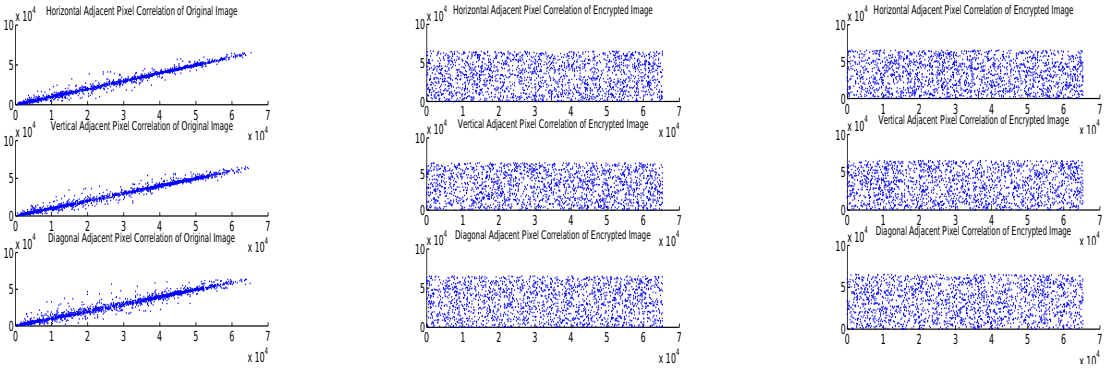
[4] G.N. Krishnamurthy and V. Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box," *International Journal of Computer Science and Network Security*, vol. 8, pp. 388-398, 2008.

[5] M. Piotr, "Generating Pseudorandom S-Boxes a Method of Improving the Security of Cryptosystems Based on Block Ciphers," *Journal of*



(a) Original Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 7: Histogram Analysis of Colour Image



(a) Original Image (b) Encrypted by AES (c) Encrypted by Dyn. AES

Fig. 8: Horizontal, Vertical and Diagonal Correlation Analysis of Colour Image

Telecommunications and Information Technology, 2009.

[6] A. ElGhafar, A. Rohiem, A. Diaa and F. Mohammed, "Generation of AES Key Dependent S-Boxes using RC4 Algorithm," *13th International Conference on Aerospace Sciences Aviation Technology*, *ASAT- 13*, 2009, pp. 26-28.

[7] K. Kazys and K. Jaunius, "Key-Dependent S-Box Generation in AES Block Cipher System," *INFORMATICA*, 2009, pp. 23-34.

[8] Z. Ghada, K. Abdennaceur, P. Fabrice and F. Daniele, "On Dynamic chaotic S-BOX," *IEEE*, 2009.

[9] J. Cui, L. Huang, H. Zhong, C. Chang and W. Yang, "An Improved AES S-Box and Its Performance Analysis," *International Journal of Innovative Computing, Information and Control*, 2011.

[10] G. Anna, "Cryptographic properties of modified AES-like S-boxes," *Annales UMCS Informatica AI XI*, 2011; **2**, 37-48.

[11] J. Julia, M. Ramlan, S. Salasiah and R. Jazrin, "Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key,", *IJCSDF*, vol. 3, pp. 183-188, 2012.

[12] R. Hosseinkhani and H. Haj Seyyed Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System", *IJCSS*, vol. 6, pp. 19-28, 2012.

[13] O. Kazymyrov, V. Kazymyrova and R. Oliynykov, "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent,"*IACR Cryptology*, 2013.

[14] M. Dara and K. Manochehri, "A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key," *World Applied Sciences Journal*, vol. 28, pp. 2003-2009, 2013.

[15] E. Mohammed Mahmoud , A. Abd El Hafez, A. Talaat and A. Zekry, "Dynamic AES-128 with key-dependent s-box," *International Journal of Engineering Research and Applications*, vol. 3, 1662-1670, 2013.

[16] S. Arrag, A. Hamdoun, A. Tragha and S. Eddine Khamlich, "Implementation Of Stronger AES By Using Dynamic S-Box Dependent Of Master Key," *Journal of Theoretical and Applied Information Technology*. 2013.

[17] F. Ahmed and D. Elkamchouchi, "Strongest AES with S-Boxes Bank and Dynamic Key MDS Matrix (SDK-AES)," *International Journal of Computer and Communication Engineering*, 2013.

[18] K. Adi Narayana Reddy and B. Vishnuvardhan, "Secure Linear Transformation Based Cryptosystem using Dynamic Byte Substitution," *International Journal of Security*, 2014.

[19] K. Kazys, V. Gytis and S. Robertas, "An Algorithm for Key-Dependent S-Box Generation in Block Cipher System," *INFORMATICA*, vol. 26, pp. 51-65, 2015.

[20] K. Balajee Maram and J.M. Gnanasekar, "Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output," *TEM Journal*. 2016.

[21] S. Katiyar and N. Jeyanthi, "Pure Dynamic S-box Construction," *International Journal of Computers*, 2016.

[22] A. Tianyong, R. Jinli, D. Kui, and Z. Xuecheng, "Construction of High Quality Key-dependent S-Box," *IAENG International Journal of Computer Science*, 2017.

[23] P. Agarwal, A. Singh and A. Kilicman, "Development of Key Dependent Dynamic S-Boxes with Dynamic Irreducible Polynomial and Affine Constant," *Advances in Mechanical Engineering*, 2018.

[24] C. Unal, K. Sezgin, P. Ihsan and Z. Ahmet, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons and Fractals*, vol. 95, pp. 92-101, 2017.

[25] S. Shrija and H. Mohammed Ali, "Performance and Security Analysis for Image Encryption using Key Image," *Indian Journal of Science and Technology*, 2015.

[26] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J Cryptology*, vol. 4, pp. 3-72, 1991.

[27] N.K. Pareek, V. Patidar and K.K. Sud, "Image encryption using chaotic logistic map," *Image Vis Comput*, vol. 24, pp. 926-934, 2006.

[28] Y. Wang, K.W. Wong, X. Liao, T. Xiang and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons Fractals*, vol. 41, pp. 1773-1783, 2009.

[29] C.E. Shannon, "Communication theory of secrecy systems," *Bell Syst Tech J*, vol. 28, pp. 656-715, 2006.