# Implementation of Modified AES as Image Encryption Scheme

**Heidilyn V. Gamido[1], Ariel M. Sison[2], Ruji P. Medina[3]**
[1,3]Technological Institute of the Philippines, Quezon City, Philippines
[2]Emilio Aguinaldo College, Manila Philippines

**Article Info**

***Article history:***

Received Jul 4, 2018
Revised Aug 23, 2018
Accepted Sep 6, 2018

***Keyword:***

AES
Entropy
Histogram
Image encryption
NPCR
UACI

**ABSTRACT**

Since images have bigger size than text, a faster encryption algorithm is needed to provide higher security in digital images. The paper presents a modified AES algorithm that address the requirement in image encryption. The modified algorithm used bit permutation in replacement of MixColumns to reduce the computational requirement of the algorithm in encrypting images. Results of the study show that the modified algorithm exhibited faster encryption and decryption time in images. The modified algorithm also achieved a good result in the key sensitivity analysis, histogram analysis, information entropy, the correlation coefficient of adjacent pixels, Number of Pixel Change Rate and Unified Average Change Intensity making the modified algorithm resistant to statistical and differential attack.

*Copyright © 2018 Institute of Advanced Engineering and Science.*
*All rights reserved.*

***Corresponding Author:***

Heidilyn V. Gamido,
Technological Institute of the Philippines,
Quezon City, Philippines.
Email: htvgamido@tsu.edu.ph

## 1. INTRODUCTION

In today’s multimedia technology, images are often used to communicate and convey meaningful information [1]. Securing images from unauthorized users is important and needed in the fields of medical processing, remote sensing, military, government documents, telecommunications and other similar fields [2]–[4].

The widespread usage of digital images on the internet requires a fast, reliable and robust security to store and transmit them over the network [5]. Image encryption is needed to enforce content access control, identity authentication and provide protection [6] of images by transforming the original content of the image into a texture-like or noise-like information that is hard to understand.

The use of encryption techniques provides a solution to the security issues in image and video processing. Asymmetric encryption algorithms are not suited for this type of application because asymmetric algorithms are much slower than symmetric techniques and require more computational processing power [7]. Symmetric encryption algorithms are already adequate when static media information like images [3] is to be secured.

Images have bigger file size compared to text and also are real-time data, a faster image encryption algorithm is necessary. AES is one of the naïve traditional algorithm used for multimedia storage and transmission of pixels. Using AES for encrypting images have drawbacks [8] because of its high computations and is slow when used for encrypting images [8]–[10].

One of the emerging challenges in image processing is that encryption techniques are often computationally expensive [6]. Unlike in text encryption, image encryption algorithm needs additional requirement because image data have properties like high redundancy, bulk capacity and high correlation between the pixels [11]. Therefore, having an efficient cryptographic algorithm is considered to be imperative, and a fast encryption algorithm is to be chosen to provide higher security in digital images [12].

The paper presents an implementation of the modified AES algorithm [13] as an image encryption scheme. The modified algorithm used bit permutation in replacement of the MixColumns Transformation to achieve faster encryption time in images. The modified algorithm had high key sensitivity and achieved a low correlation value between adjacent pixels. The result also shows a negligible value of predictability making it resistant to statistical and differential attack.

## 2. REVIEW OF RELATED LITERATURE

Encrypting images can be performed either in full or partial image encryption procedure under the spatial, frequency or hybrid domain [3]. A full encryption algorithm encrypts the whole image rather than just a selected or important part. While spatial domain deals with the image as it is, where the pixel values of image change concerning a scene. The implementation of the modified algorithm is under the full image encryption procedure in the spatial domain.

The paper of [14] presents a framework to evaluate image encryption schemes. Aside from visual inspection, parameters like correlation coefficient, information entropy, number of pixel change rate, and unified average change rate are used to evaluate image encryption schemes. These parameters were used in this study to evaluate the performance of the modified algorithm.

Similar studies of modification of AES algorithms were presented for image encryption. Some of the studies are the following:

The reduction of the number of rounds of AES to only one round is introduced to address the high computational load of the AES algorithms, and a new S-box was proposed in the research of [15] to encrypt greyscale high definition images. The reduction to only one round showed a significant decreased in the encryption time of the algorithm by 1/10 and reduced the ROM used by 256 bytes. However, several studies [16]–[18] show that a round-reduction in AES is likely to affect the security level of the algorithm.

An AES modification by adjusting the ShiftRows transformation was introduced by[19]. The basis of shifting of rows is from the value in the state ([0][0]) whether the value of the state is odd or even. The result shows that the proposed transformation gives better encryption time because it does not have any additional operations.

Modifications in both ShiftRows and MixColumns were also presented [20]. The direction of shifting in ShiftRows modification is also about checking the value of the state ([0][0]). The modification in MixColumns includes a matrix transformation of the final state from ShiftRows before applying the MixColumn process. The modification shows that the modification resulted in lesser computational time.

The paper of [21] proposed image encryption based on shifted row and columns of the image. Before the encryption of images, a shifting process is introduced to divide the plaintext image into blocks with 3x3 pixels. These blocks are used to further shift it through the rows and the columns within the image using a shifted table processed by the hash algorithm. The result shows that the algorithm produces a significant difference in small change in the original image

The paper of [22] proposed an image based encryption technique by shuffling the RGB pixel values of the image. The shuffling of values on pixel-based only interchange the RGB values of the image and do not create a new pixel value for the encrypted image unlike with a bit-permutation technique.

The proposed image encryption of [23] is also based on pixel modification. The proposed pixel modification is an exchange between the most significant bits and the least significant bits. The result of the study shows that the density of the histogram image of the plain image is greater than the density of the encrypted image. The correlation coefficient in horizontal direction of the plain and encrypted image are the same which means that the two images are the same in horizontal direction [14].

## 3. PROPOSED METHOD

Figure 1 shows the modified AES algorithm using bit permutation as presented in the study of [13]. The result in the paper shows that the use of bit permutation instead of MixColumns makes the modified AES algorithm suited for encrypting digital images because of increased efficiency and throughput due to reduced execution time and CPU usage. Bit permutation has no complex mathematical operationbut only involves shifting of the position of bits of every state [13]. The proposed modified AES algorithm takes 128-bit data length as input and 128 key length which has ten rounds of transformation and used AES-CBC mode in encrypting images.

Figure 2 shows the conceptual framework for image encryption. The original image is taken as an input, taking its height and width and its RGB component. The proposed method is done in full image encryption using the proposedalgorithm. The secret key is used during the encryption and decryption process.

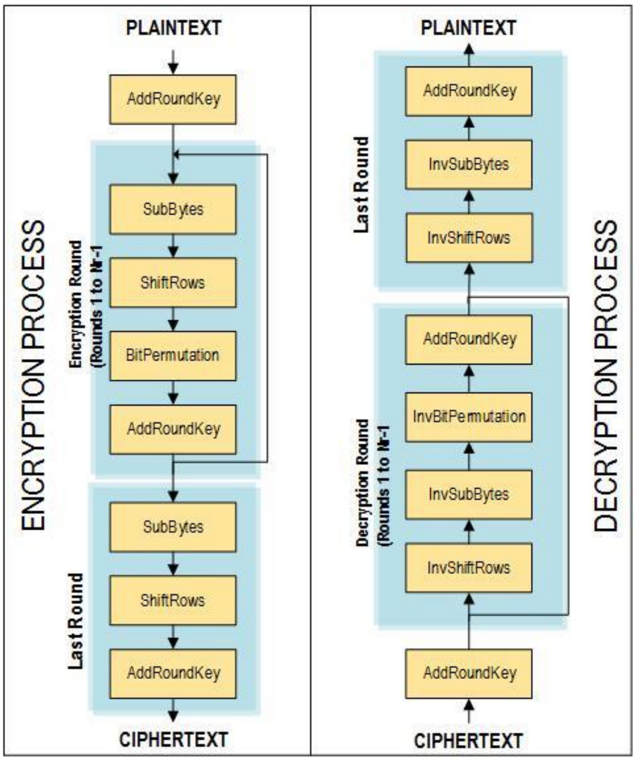


Figure 1. Modified AES algorithm

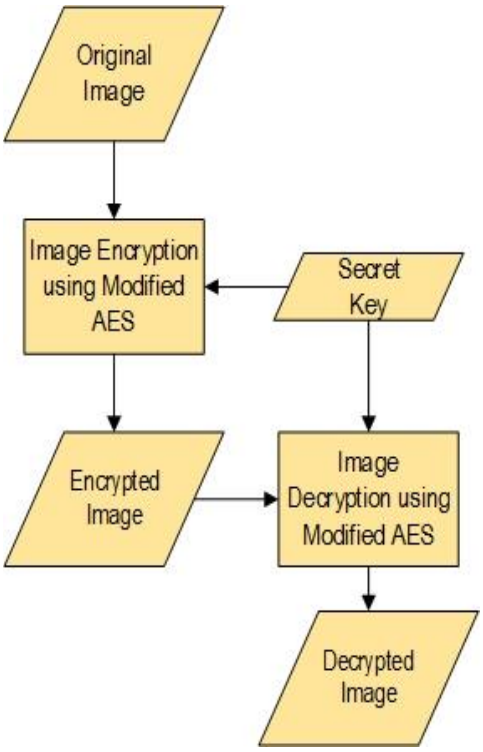

Original Image
Image Encryption using Modified AES
Secret Key
Encrypted Image
Image Decryption using Modified AES
Decrypted Image

Figure 2. Conceptual framework for image encryption

The steps for encrypting and decrypting digital image are as follows:

### 3.1. Image Encryption Phase

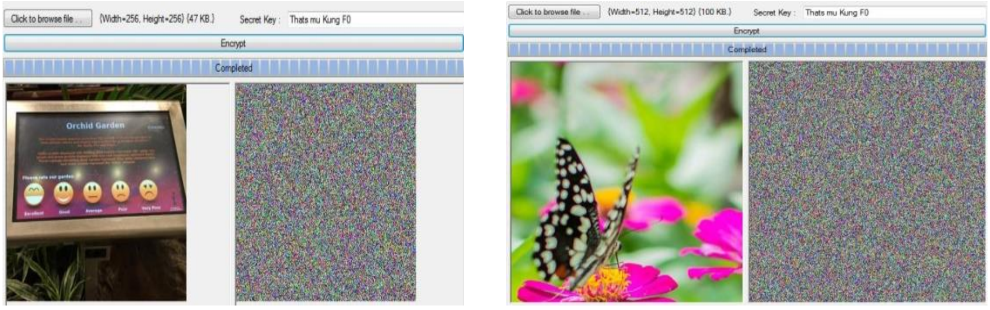
a. Get the height (M) and width (N) of the plaintext image (I);
b. For each pixel in I, get RGB components (Ir, Ig, Ib)
c. Concatenate the value of Ir, Ig, Ib of all pixels
d. Group concatenated string by 32 to complete the 128-bit data length
e. Encrypt concatenated value using Modified AES algorithm in CBC mode
f. Divide the length of the encrypted string by 6
g. For each value in new length of the encrypted string, get RGB (Er, Eg, Eb) component
h. For each M and N, map RGB component (Er, Eg, Eb)

### 3.2. Image Decryption Phase

a. Get the height (M) and width (N) of the encrypted image (E);
b. For each pixel in E, get RGB component (Er, Eg, Eb)
c. Concatenate value of Er, Eg, Eb of all pixels
d. Group concatenated string by 32 to complete the 128-bit data length
e. Decrypt concatenated value using Modified AES algorithm in CBC mode
f. Divide the length of the decrypted string by 6
g. For each value in new length of the decrypted string, get RGB (Ir, Ig, Ib) component
h. For each M and N, map RGB component (Ir, Ig, Ib)

## 4. RESULTS AND DISCUSSION

The encryption algorithm in images was simulated using Microsoft .NET framework, and the generated encrypted images were evaluated using the functions in Matlab (R2017a). The evaluation of the encrypted image is on the encryption and decryption time, key sensitivity analysis, histogram analysis, correlation coefficient, information entropy, NPCR, and UACI.



{Width=256, Height=256} {47 KB.} Secret Key : Thats mu Kung F0

{Width=512, Height=512} {100 KB.} Secret Key : Thats mu Kung F0

Figure 3. Encrypted images of original images

Figure 3 above shows the equivalent encrypted image of the original images where the original image is transformed into a noise-like image making it difficult to understand.

### 4.1. Encryption and Decryption Time

Encryption Time refers to the amount it takes to process the plaintext image to its equivalent encrypted image while Decryption Time refers to the amount it takes to convert back the encrypted image to the plaintext image. Results in Table 1 and 2 show that the modified AES encrypts the image faster than the standard AES. A faster encryption algorithm for images is needed to provide better security of digital images.

Table 1. Encryption Time Result

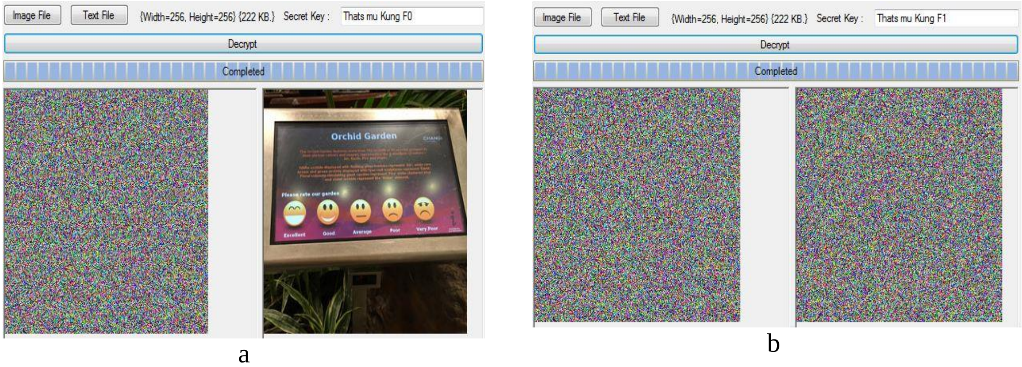
| File | Image Size | Size on Disk (KB) before Encryption | Size on Disk (KB) after Encryption | Encryption Time of AES (ms) | Encryption Time of Modified AES (ms) |
|---|---|---|---|---|---|
| Smiley | 256x256 | 47 | 222 | 13141 | 12322 |
| Butterfly | 512x512 | 100 | 887 | 103008 | 98288 |

Table 2. Decryption Time Result

| File | Image Size | Size on Disk (KB) before decryption | Size on Disk (KB) after decryption | Decryption Time of AES (ms) | Decryption Time of Modified AES (ms) |
|---|---|---|---|---|---|
| Smiley | 256x256 | 222 | 47 | 11211 | 10517 |
| Butterfly | 512x512 | 887 | 100 | 88309 | 83766 |

### 4.2. Key Sensitivity Analysis

A good encryption algorithm should be highly sensitive to changes in the secret key [4]. A minor change in the secret key during decryption process results in a completely different decrypted image. Figure 4a shows the decrypted image using the correct secret key while Figure 4b shows a wrong decrypted image using a changed value in the secret key. The result shows that the algorithm produces a high sensitivity in small changes in the secret key.



{Width=256, Height=256} {222 KB.} Secret Key : Thats mu Kung F0

{Width=256, Height=256} {222 KB.} Secret Key : Thats mu Kung F1

a

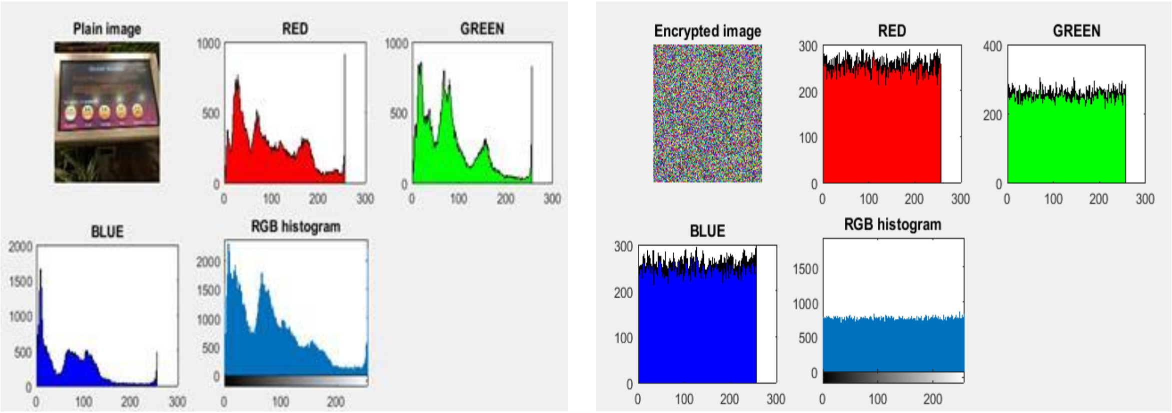
b

Figure 4. Key sensitivity analysis result

### 4.3. Histogram Analysis

The histogram is a graphical representation that shows the distribution of pixels in the image at every different intensity value. For an encryption algorithm to be resistant to statistical attack, it must have a histogram that is entirely different from the plain image and has a uniform distribution of values [24], [25].

Figure 5a-5b show that the histogram of the plaintext image Smiley is completely different from the encrypted image. The encrypted image has a uniformly distributed histogram which means that a little information about the data is known. The result of the analysis of the histogram shows that the modified algorithm is resistant to statistical attack.



(a) (b)

Figure 5. Histogram analysis result of (a) Plain image (b) Encrypted image smiley

### 4.4. Correlation Coefficient

Correlation Coefficient computes the degree of similarity between adjacent pixels. A correlation coefficient that is very low or very close to zero means that the plain and encrypted images are completely different. A correlation coefficient equal to one means that both images are identical and are in perfect correlation and that the encryption process fails because the encrypted image is same as the plaintext image [14].

A randomly selected 3000 adjacent pairs of pixels in horizontal and vertical direction in the plain and encrypted image were used to compute for the correlation coefficient. Below shows the formula for the computation of correlation coefficient [14, 21, 26, 27].

$$Correlation\ Coefficient = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2} \cdot \sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \tag{1}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{2}$$

where x and y are the values of two pixels of the plaintext and encrypted images and N is the number of selected adjacent pixels. Table 3 shows that the modified AES algorithm has achieved a lower correlation coefficient than the standard AES for the two images. The value means that the plain and the encrypted image are entirely different from each other and are uncorrelated both in horizontal and vertical directions. Figure 6 shows the distribution of two pixels in horizontal and vertical direction in the original image and its equivalent encrypted image using the modified algorithm.

Table 3. Correlation Coefficient Result

| File | Plaintext image | | Encrypted image using AES | | Encrypted image using modified AES | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Horizontal | Vertical | Horizontal | Vertical |
| Smiley | 0.9721 | 0.9486 | 0.0231 | 0.0059 | -0.0119 | -0.0322 |
| Butterfly | 0.9865 | 0.9880 | -0.0245 | 0.0014 | -0.0028 | -0.0265 |

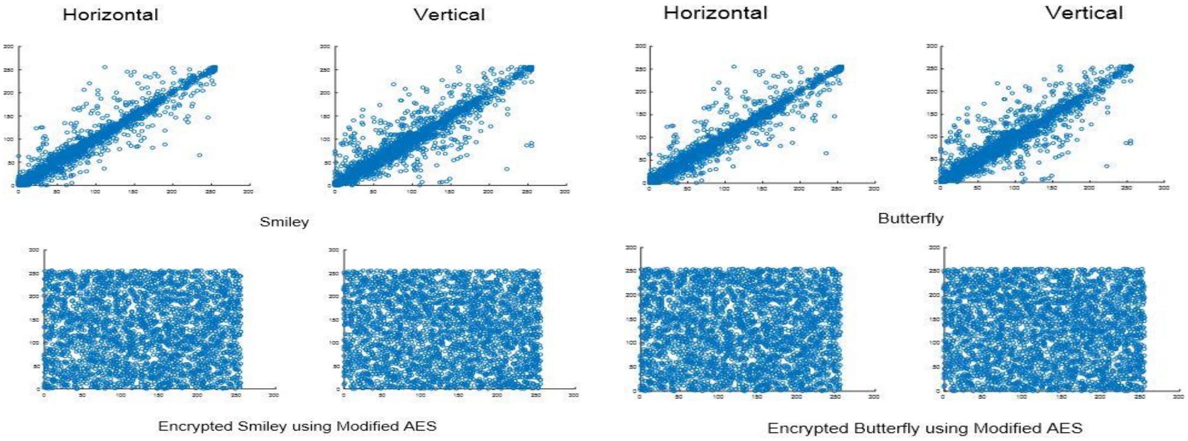


Figure 6. Distribution of pixels in horizontal and vertical direction

### 4.5. Information Entropy

Information Entropy is vital in analyzing the encryption algorithm because it is used to depict the randomness of data [28] and is used to show the degree of uncertainties in a communication system [14]. When messages are encrypted, the value of the entropy should be approximated to 8. An entropy value that is less than 8 means a certain degree of predictability exists. The information entropy H(m) of a message is calculated as [14, 21, 28]:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 \frac{1}{p(m_i)} \tag{3}$$

Where $p(m_i)$ is the propability of $m_i$

The result in Table 4 shows that the modified AES has a very close value to the ideal value of 8, which implies that the modified AES has a negligible value of predictability and introduces randomness to the encrypted image and a comparable performance with the standard.

Table 4. Information Entropy Result

| File | AES | Modified AES |
|---|---|---|
| Smiley | 7.9990 | 7.9991 |
| Flower | 7.9998 | 7.9998 |

### 4.6. NPCR and UACI

The NPCR and UACI are factors to demonstrate that the modified encryption algorithm can strongly resist differential attack [29] [30]. A higher value of these two factors means a better encryption algorithm [14].

*Number of Pixel Change Rate (NPCR)* - NPCR refers to a test to measure the avalanche effect in image encryption. It refers to the number of pixel difference between encrypted images C1 and C2, where C1 is the encrypted image of original image and C2 is the encrypted image with one (1) pixel change.

*Unified Average Change Intensity (UACI)* - UACI indicates the average intensity of differences between the plain image and the encrypted image.

The computation of NPCR and UACI is[30]:

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{MxN} \times 100\% \tag{4}$$

Where: $D(i,j) = \begin{cases} 0, if\ C1(i,j) = C2(i,j) \\ 1, if\ C1(i,j) \neq C2(i,j) \end{cases}$

$$UACI = \frac{1}{M\ x\ N}\left[\sum \frac{C1(i,j) - C2(i,j)}{255}\right] \times 100\% \tag{5}$$

Table 5. Plaintext Sensitivity

| File | AES | | Modified AES | |
|---|---|---|---|---|
| | NPCR | UACI | NPCR | UACI |
| Smiley | 99.47 | 33.38 | 99.48 | 34.50 |
| Flower | 99.47 | 33.43 | 99.49 | 33.40 |

Table 6. Key Sensitivity

| File | AES | | Modified AES | |
|---|---|---|---|---|
| | NPCR | UACI | NPCR | UACI |
| Smiley | 99.59 | 33.42 | 99.63 | 33.45 |
| Flower | 99.61 | 33.43 | 99.62 | 33.47 |

The ideal value of NPCR and UACI is 99.61% and 33.46% respectively [31].The result in Table 5 and 6 show that themodified algorithm has high sensitivity to small changes because the value of the NPCR and UACI are closer to their ideal value than the standard AES. It shows that the modified algorithm also hasstrong diffusion mechanism and strongly resists differential attack.

## 5. CONCLUSION

The paper presented an implementation of the proposed modified AES as an image encryption scheme to address the requirement in encrypting images. Comparison with the standard AES is carried out concerning encryption time, key sensitivity analysis, histogram analysis, the correlation coefficient of adjacent pixels, information entropy, NPCR, and UACI. The experimental result showed that the modified algorithm produced an entirely different encrypted image and that there is a significant difference in the encrypted image whenever there is a small change in the plaintext image. The result also showed that the modified algorithm is faster than AES, has a comparable value of predictability with the standard and is resistant to statistical and differential attacks making it suitable for image encryption. In the future, the implementation of the modified AES algorithm in partial image encryption can be considered and a comparison of the modified algorithm with other image encryption algorithms.

## REFERENCES

[1] A. Kumar and A. Agrawal, “Image Encryption by 128 Bit Encryption Technique”, *Int. Conf. Syst. Model. Adv. Res. Trends*, pp. 106–108, 2015.

[2] P.K. Das, P. Kumar, and M. Sreenivasulu, “Image Cryptography : A Survey towards its Growth”, *Adv. Electron. Electr. Eng. Res. India Publ.*, vol. 4, no. 2, pp. 179–184, 2014.

[3] M. Khan and T. Shah, “A Literature Review on Image Encryption Techniques”, *3D Res.*, vol. 5, no. 4, p. 29, Dec. 2014.

[4] Q. Zhang and A. Qunding, “Digital image encryption based on Advanced Encryption Standard(AES) algorithm”, *5th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC 2015*, pp. 1218–1221, 2015.

[5] D. Saravanan, “Secured Image Transformation using Disorganized Chart Pattern Technique”, *Pak . J . Biotechnol . Vol . 13 Spec. issue II ( Int. Conf. Eng. Technol. Syst.*, vol. 13, no. Ii, pp. 135–137, 2016.

[6] W. Puech, Z. Erkin, M. Barni, S. Rane, and R.L. Lagendijk, “Emerging cryptographic challenges in image and video processing”, in *2012 19th IEEE International Conference on Image Processing*, 2012, pp. 2629–2632.

[7] A. Jain and D. Bhatnagar, “A Comparative Study of Symmetric Key Encryption Algorithms”, *IJCSN Int. J. Comput. Sci. Netw.*, vol. 3, no. 5, pp. 2277–5420, 2014.

[8] S. Anwarul and S. Agarwal, “Image enciphering using modified AES with secure key transmission”, *Commun. Comput. Syst. - Prasad al.*, pp. 137–142, 2016.

[9] A. Abdulgader, M. Ismail, N. Zainal, and T. Idbeaa, “Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption”, *J. Theor. Appl. Inf. Technol.*, vol. 71, no. 1, pp. 1–12, 2015.

[10] S. MT and E. Nurpeti, “Performance of Chaos-Based Encryption Algorithm for Digital Image”, *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 12, no. 3, p. 675, 2014.

[11] H. Patwa and A.D. Arya, “Review on Block Based Transformation Image Encryption Techniques”, *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 3, pp. 1994–1995, 2015.

[12] K. Patel and S. Belani, “Image encryption using different techniques: A review”, *Int. J. Emerg. Technol. Adv. Eng.*, vol. 1, no. 1, pp. 30–34, 2011.

[13] H.V. Gamido, A.M. Sison, and R.P. Medina, “Modified AES for Text and Image Encryption”, *Indones. J. Electr. Engiineering Comput. Sci.*, vol. 11, no. 3, 2018.

[14] J. Ahmad and F. Ahmed, “Efficiency analysis and security evaluation of image encryption schemes”, *Int. J. Video Image Process. Netw. Secur.*, vol. 12, no. 04, pp. 18–30, 2012.

[15] S.M. Wadi and N. Zainal, “Rapid Encryption Method based on AES Algorithm for Grey Scale HD Image Encryption”, *Procedia Technol.*, vol. 11, no. Iceei, pp. 51–56, 2013.

[16] K. Bae, S. Moon, D. Choi, Y. Choi, D.S. Choi, and J. Ha, “Differential fault analysis on AES by round reduction”, in *2011 6th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 2011, pp. 607–612.

[17] C. Bouillaguet, P. Derbez, and P.A. Fouque, “Automatic Search of Attacks on Round-Reduced AES and Applications”, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6841 LNCS, 2011, pp. 169–187.

[18] A.P. Mirbaha, J.M. Dutertre, and A. Tria, “Differential analysis of Round-Reduced AES faulty ciphertexts”, in *2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, 2013, pp. 204–211.

[19] S.H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, “A New Modified Version of Advanced Encryption Standard Based Algorithm”, *Int. Conf. Electron. Inf. Eng. (ICEIE 2010)*, vol. 1, no. Iceie, pp. 141–145, 2010.

[20] H. Kaur and R. Mehla, “Image Encryption Using AES with Modified Transformation”, *Int. J. Sci. Res.*, vol. 3, no. 7, pp. 360–363, 2014.

[21] A.B. Abugharsa, A.S. Hasan Basari, and H. Almangush, “A New Image Encryption Approach using Block-Based on Shifted Algorithm”, *Int. J. Comput. Sci. Netw. Secur.*, vol. 11, no. 12, pp. 123–130, 2011.

[22] Q. Kester, “A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling”, *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 2, no. 2, pp. 848–854, 2013.

[23] K. Agung, Fatmawati, and H. Suprajitno, “Image encryption based on pixel bit modification”, *J. Phys. Conf. Ser.*, vol. 1008, p. 012016, Apr. 2018.

[24] E. Setyaningsih and C. Iswahyudi, “Image Encryption on Mobile Phone Using Super Encryption Algorithm”, *TELKOMNIKA Indones. J. Electr. Eng.*, vol. 10, no. 4, pp. 835–843, 2012.

[25] Y. Jain, R. Bansal, G. Sharma, B. Kumar, and S. Gupta, “Image Encryption Schemes : A Complete Survey”, *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 9, no. 7, pp. 157–192, 2016.

[26] S. Mondal, “Data security-modified AES algorithm and its applications”, *ACM SIGARCH Comput. Archit. News*, vol. 42, no. 2, pp. 1–8, 2014.

[27] X. Zhang and X. Wang, “Multiple-image encryption algorithm based on mixed image element and permutation”, *Opt. Lasers Eng.*, vol. 92, no. December 2016, pp. 6–16, 2017.

[28] M. Ahmad, H.D. Alsharari, and M. Nizam, “Security Improvement of an Image Encryption Based on mPixel-Chaotic-Shuffle and Pixel-Chaotic-Diffusion”, *CoRR*, vol. abs/1403.6, 2014.

[29] M.A. El-wahed, S. Mesbah, and A. Shoukry, “Efficiency and Security of Some Image Encryption Algorithms”, *Proc. World Congr. Eng.*, vol. I, pp. 4–7, 2008.

[30] Y. Wu, S. Member, J.P. Noonan, and L. Member, “NPCR and UACI Randomness Tests for Image Encryption”, *Cyber Journals Multidiscip. Journals Sci. Technol. J. Sel. Areas Telecommun.*, no. APRIL 2011, pp. 31–38, 2011.

[31] X. Tong, Y. Liu, M. Zhang, H. Xu, and Z. Wang, “An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps”, *Entropy*, vol. 17, no. 1, pp. 181–196, 2015.