International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:2, 2011

Study of Effect of Removal of Shiftrows and Mixcolumns Stages of AES and AES-KDS on their Encryption Quality and Hence Security

[1] Krishnamurthy G N, [2]V Ramaswamy

***Abstract*—**This paper demonstrates the results when either Shiftrows stage or Mixcolumns stage and when both the stages are omitted in the well known block cipher Advanced Encryption Standard(AES) and its modified version AES with Key Dependent S-box(AES-KDS), using avalanche criterion and other tests namely encryption quality, correlation coefficient, histogram analysis and key sensitivity tests.

***Keywords*—**Encryption, Decryption, Avalanche, key sensitivity.

I. Introduction

IN October 2000, after a four year effort to replace the ageing Data Encryption Standard (DES), National Institute for Standards and Technology announced the selection of Rijndael [1] as the proposed AES [1]-[3]. Here we will assume that readers are familiar with AES design. Details of modified version of AES namely AES-KDS are available in our paper [4]. In that paper we have suggested four different cases implementations of AES-KDS [4]. The encryption procedure of AES uses four stages namely Addroundkey, SubBytes, Shiftrows and Mixcolumns. AES-KDS has an extra stage Rotate_S-box. First we will study to see what happens to the performance of AES and AES-KDS if Shiftrows stage is omitted.

II. Effect of Removal of Shiftrows stage

We have taken 30000 pairs of plaintexts with each pair differing in only one bit. We have encrypted them using AES algorithm (without *Shiftrows* stage) and have compared these values with that of the encrypted samples of AES. We have counted the number times AES gives better avalanche [2], [3] number of times AES without Shiftrows stage gives better avalanche and number of times both give the same avalanche. Tabulation of results for rounds 2, 4, 6, 8 and 10 of AES and AES without *Shiftrows* stage algorithms for one bit change in plaintexts is shown in table I and that for AES and Case 3 of AES-KDS without *Shiftrows* stage using same plaintext samples is shown in table II.

The results show that AES algorithm gives better avalanche compared to AES without *Shiftrows* and Case 3 of AES-KDS without *Shiftrows* stage. We can also observe the little contribution by the stage *Rotate_S-box* of AES-KDS by observing the results for 2 rounds in table I and table II. Similar Avalanche results can be observed when *Mixcolums* stage is removed and also when both *Shiftrows* and *Mixcolums* stages are removed both for AES and for AES-KDS.

[1]Dr. Krishnamurthy G N, Dept. of Information Science & Engineering, Presently working as Registrar(Evaluation) at VTU, Belgaum, Karnataka on deputation basis deputed from BNM Institute of Technology, Bangalore, Karnataka, India krishnamurthy_gn@hotmail.com
[2]Dr. V Ramaswamy, Research Head, dept of Computer Science & Engineering, Mahaveer Jain College, Bangalore.

TABLE I AVALANCHE EFFECT FOR ONE BIT CHANGE IN PLAINTEXT

Number of rounds	Number of pairs of plaintext samples	Number of times AES algorithm gives better Avalanche	Number of times AES without Shiftrows gives better avalanche	Number of times AES and AES without Shiftrows stage give same Avalanche
2	30000	13903	13284	2813
4	30000	30000	0	0
6	30000	30000	0	0
8	30000	30000	0	0
10	30000	30000	0	0

TABLE II AVALANCHE EFFECT FOR ONE BIT CHANGE IN PLAINTEXT

Number of rounds	Number of pairs of plaintext samples	Number of times AES algorithm gives better Avalanche	Number of times AES-KDS without Shiftrows stage algorithm gives better avalanche	Number of times AES and AES-KDS without Shiftrows stage give same Avalanche
2	30000	30000	0	0
4	30000	30000	0	0
6	30000	30000	0	0
8	30000	30000	0	0
10	30000	30000	0	0

III. Encryption Quality Analysis

The quality of image encryption [6]-[10] may be determined as follows:
Let F and F' denote the original image (plainimage) and the encrypted image (cipherimage) respectively each of size M*N pixels with L grey levels. $F(x, y)$, $F'(x, y)$ ε {0,.., $L-1$} are the grey levels of the images F and F' at position (x, y) ($0 \le x \le M-1$, $0 \le y \le N-1$). Let $H_L(F)$ denote the number of occurrences of each grey level L in the original image (plainimage) F. Similarly, $H_L(F')$ denotes the number of occurrences of each grey level L in the encrypted image (cipherimage) F'. The encryption quality represents the average number of changes to each grey level L and is expressed mathematically as

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} \left| H_L(F') - H_L(F) \right|}{256}$$

For all tests we have used two images Birds.bmp and Ship.bmp both of size 512x512.

We now compare the quality of encryption of AES with that of AES without Shiftrows stage and with that of Case 3 of AES-KDS without Shiftrows stage using two images Ship.bmp and Birds.bmp and their corresponding encrypted images. The results are tabulated in tables III and IV.

TABLE III ENCRYPTION QUALITIES USING SHIP.BMP AS PLAINIMAGE

Number of Rounds r	Algorithm type		
	EQ for AES	EQ for AES without Shiftrows stage	EQ for AES-KDS without Shiftrows stage (Case 3)
2	866.757812	1015.625000	1015.625000
4	866.781250	1015.625000	1015.625000
6	863.656250	1015.625000	1015.625000
8	867.625000	1015.625000	1015.625000
10	862.859375	1015.625000	1015.625000

TABLE IV ENCRYPTION QUALITIES USING BIRDS.BMP AS PLAINIMAGE

Number of Rounds r	Algorithm type		
	EQ for AES	EQ for AES without Shiftrows stage	EQ for AES-KDS without Shiftrows stage (Case 3)
2	1400.585938	1413.687500	1470.945312
4	1386.945312	1437.015625	1445.835938
6	1402.367188	1441.304688	1445.968750
8	1384.312500	1389.234375	1415.437500
10	1396.031250	1426.445312	1415.109375

Even though the magnitudes of encryption quality for AES without Shiftrows stage are more than that of AES, their values differ very little for different rounds. This is a sign of poor encryption quality.

The above results show that modification done to the function does not degrade the quality of encryption.

IV. KEY SENSITIVITY TEST

We have conducted key sensitivity test on the image Birds.bmp for AES and AES without Shiftrows and AES-DS without Shiftrows using the 128 bit keys K1 and K2 as follows

K1 = ADF278565E262AD1F5DEC94A0BF25B27 (Hex)
K2 = ADF278565E262AD1F1DEC94A0BF25B27 (Hex)

For AES algorithm, the results are already shown in figure 1(figures 1A through F). The encrypted image (encrypted with K1) differs from the encrypted image (encrypted with K2) in 99.453354% of pixels.

This experiment is repeated for AES without Shiftrows, without Mixcolumns and without both. The encrypted image (encrypted with K1) differs from the encrypted image (encrypted with K2) by 24.836987%, 68.482422%, 24.773895% of pixels for AES without Shiftrows stage, AES without Mixcolums stage, and AES with both the stages removed respectively. These results show that Shiftrows stage is more sensitive to key change than Mixcolumns stage.

Encrypted images of Birds.bmp for AES without Shiftrows stage using keys K1 and K2 are shown in figures 2B and 2C, for that of AES without Mixcolums stage are shown in figures 3B and 3C, and for AES with both the stages removed are shown in figures 4B and 4C. From the figures we can observe the appearance of traces of original image which is an indication of poor encryption. This makes cryptanalysis very easy leading to the retrieval of original information without much difficulty. For removal of Shiftrows or Mixcolumns or both stages, when we tried to decrypt images encrypted with K1 and K2 using keys K2 and K1 respectively, decryption reveals much information about the original image. The results are shown in 2E and 2F for AES without Shiftrows stage, 3E and 3F for AES without Mixcolumns stage and for AES with both the stages removed the results are shown in 4E and 4F. The amount of information revealed for AES without Shiftrows stage is much more when compared to what is revealed for AES without Mixcolumns stage. So the contribution of Shiftrows stage is more to key sensitivity than Mixcolumns stage.

This experiment is repeated (Case 3 of modified AES-KDS). Percentages of number of pixels that differ from the image encrypted with K1 with that image encrypted with K2 for AES-KDS without Shiftrows stage, AES-KDS without Mixcolums stage, and AES-KDS with both the stages removed are 99.657234%, 99.929985%, 99.950760% respectively. Here percentage difference is huge compared to that of AES. This difference is computed based on the corresponding pixels in the encrypted images encrypted using keys K1 and K2. The additional stage Rotate_S-box has its own influence in mixing pixels. The textures visible in the encrypted images using AES reveal more information than that are visible in Case 3 of AES-KDS. These results show that Shiftrows stage is more sensitive to key change than Mixcolumns stage.

Encrypted images of Birds.bmp using AES-KDS without Shiftrows stage with keys K1 and K2 are respectively shown in figures 5B and 5C, for that of AES-KDS without Mixcolums stage are shown in 6B and 6C, and for AES-KDS with both the stages removed they are shown in 7B and 7C. For these three types, when we tried to decrypt images encrypted with K1 and K2 by using keys K2 and K1 respectively, decryption reveals much information about the original image. The results are shown in 5E and 5F for AES-KDS without Shiftrows stage, 6E and 6F AES-KDS without Mixcolumns stage and for AES with both the stages removed they are shown in 7E and 7F. The amount of information revealed for AES-KDS without Shiftrows stage is much more than what is revealed for AES without Mixcolumns stage. So the contribution of Shiftrows stage is more to the key sensitivity than Mixcolumns stage.

Fig. 1A Plainimage Birds.bmp

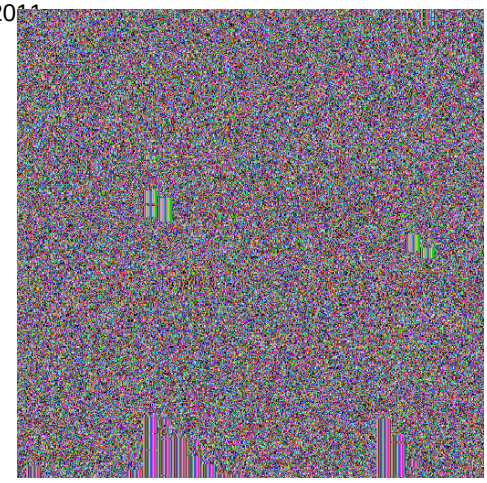


Fig. 1B Encrypted with Key K1

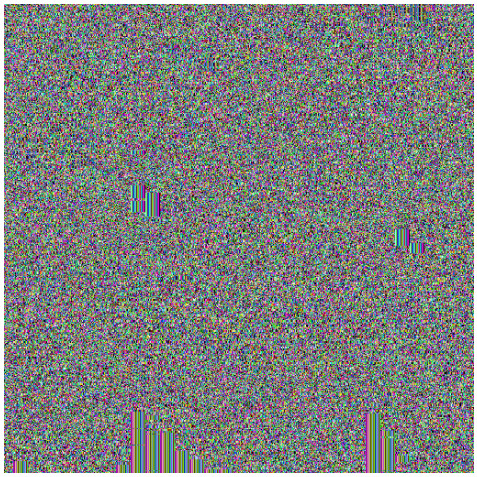


Fig. 1C Encrypted with Key K2

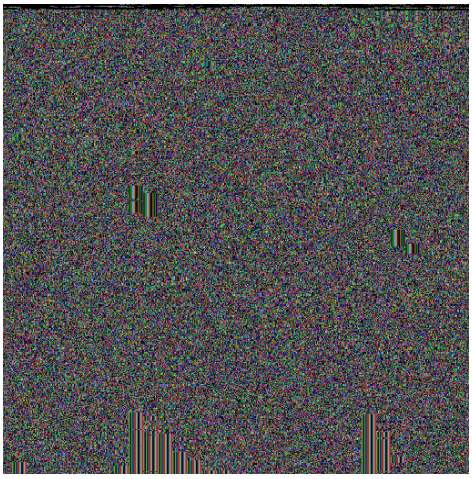


Fig. 1D Difference of Images in 1B & 1C

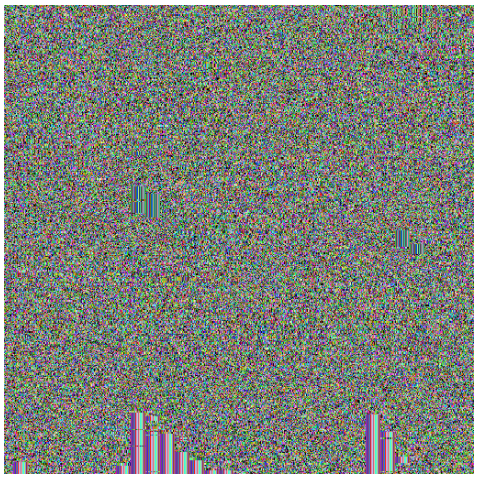


Fig. 1E Encrypted with Key K1 but Decrypted with K2

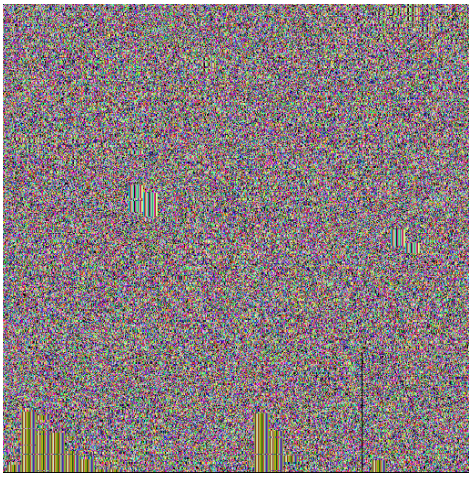


Fig. 1F Encrypted with Key K2 but Decrypted with K1

Fig. 1 Results of Key Sensitivity analysis for Original AES Algorithm

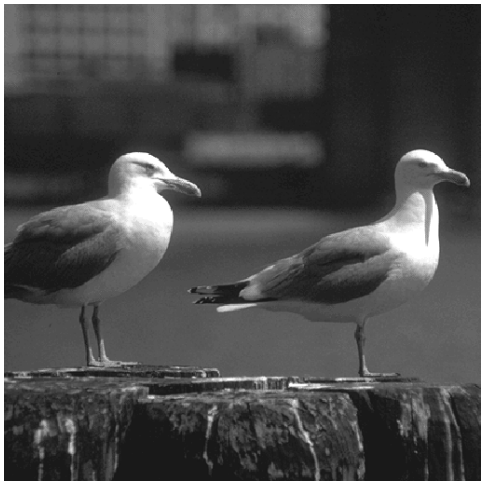
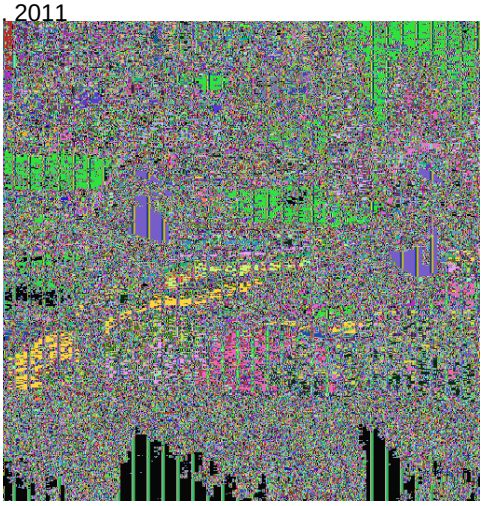


Fig. 2A Plainimage Birds.bmp



2B Encrypted with Key K1

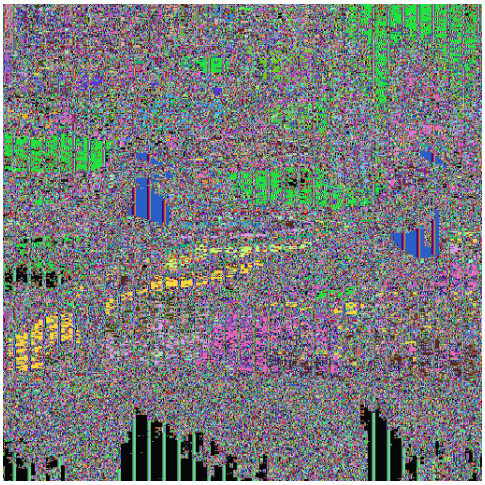


Fig. 2C Encrypted with Key K2

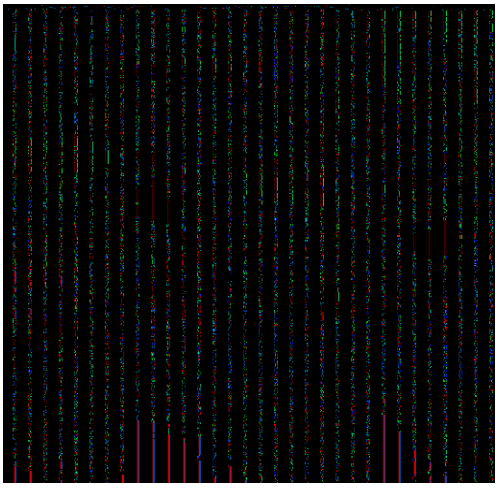


Fig. 2D Difference of Images in 2B & 2C

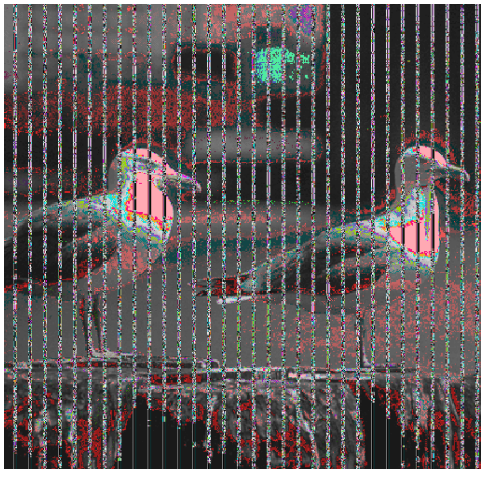


Fig. 2E Encrypted with Key K1 but Decrypted with K2

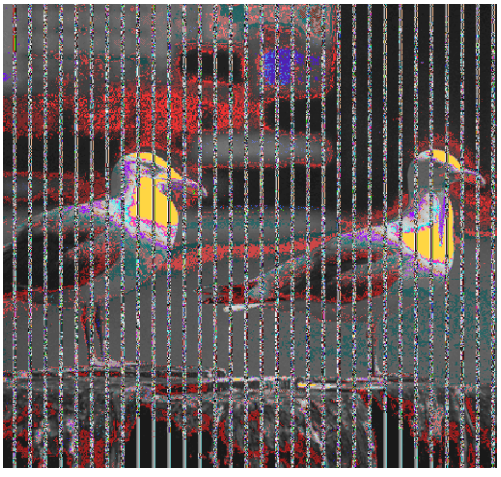


Fig. 2F Encrypted with Key K2 but Decrypted with K1

Fig. 2 Results of Key Sensitivity analysis for AES Algorithm without Shifttrows stage

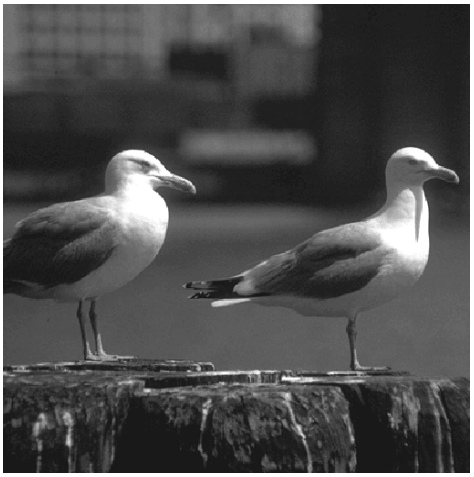


Fig. 3A Plainimage Birds.bmp

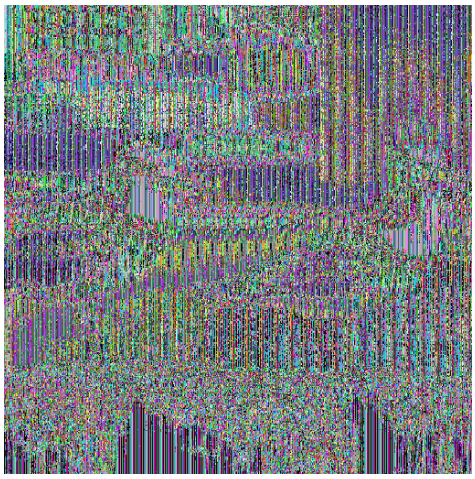


Fig. 3B Encrypted with Key K1

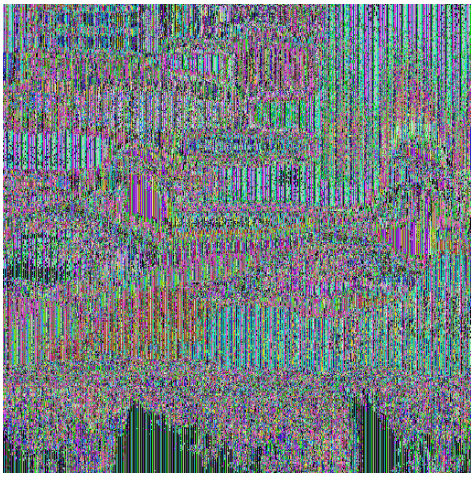


Fig. 3C Encrypted with Key K2

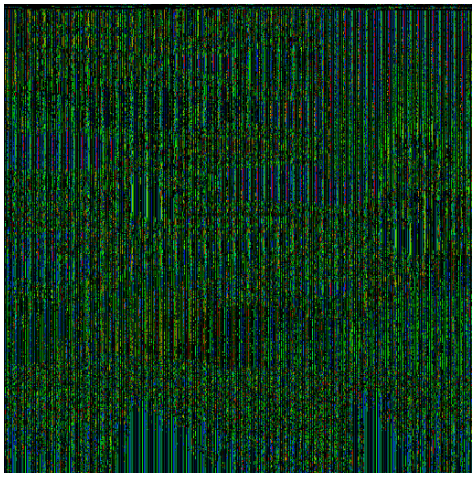


Fig. 3D Difference of Images in 3B & 3C

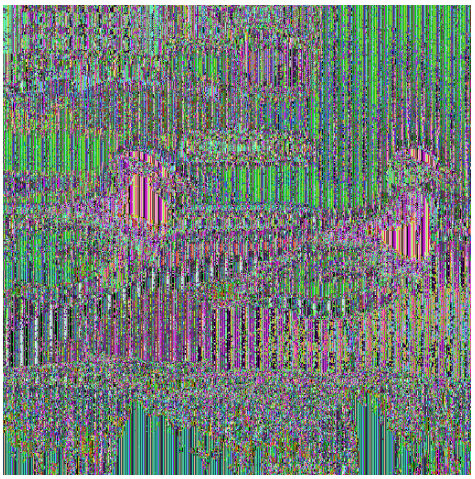


Fig. 3E Encrypted with Key K1 but Decrypted with K2

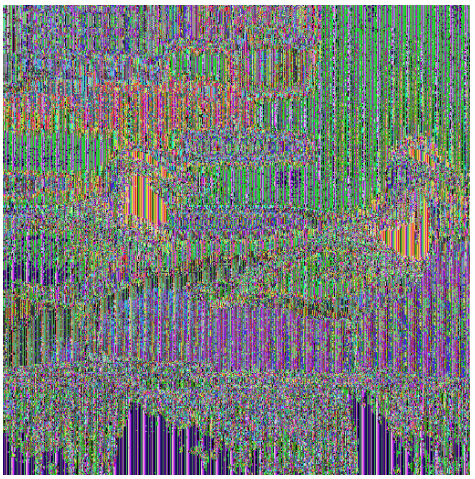


Fig. 3F Encrypted with Key K2 but Decrypted with K1

Fig. 3 Results of Key Sensitivity analysis for AES Algorithm without Mixcolumns stage

Fig. 4A Plainimage Birds.bmp

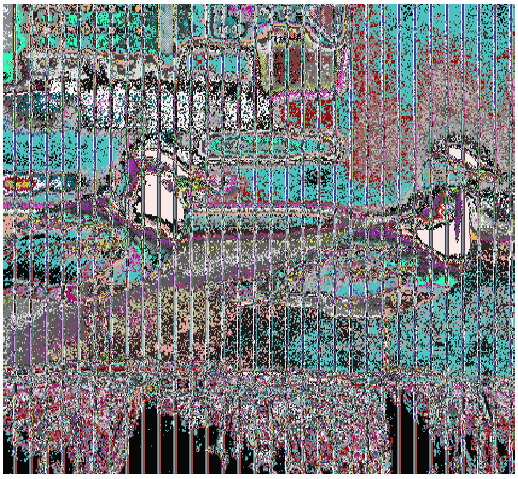


Fig. 4B Encrypted with Key K1

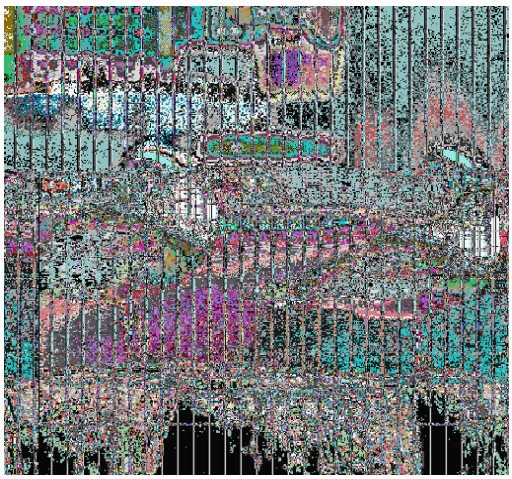


Fig. 4C Encrypted with Key K2

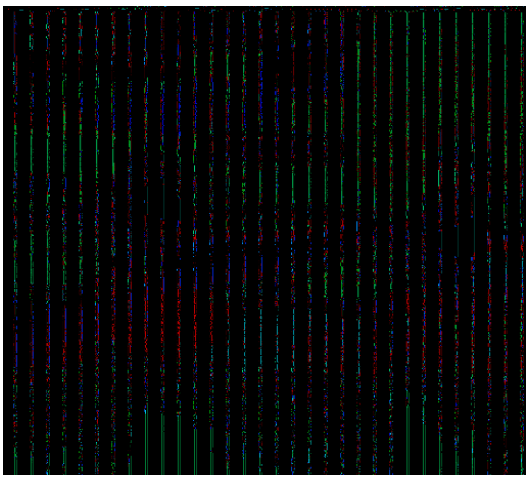


Fig. 4D Difference of Images in 4B & 4C

Fig. 4E Encrypted with Key K1 but Decrypted with K2

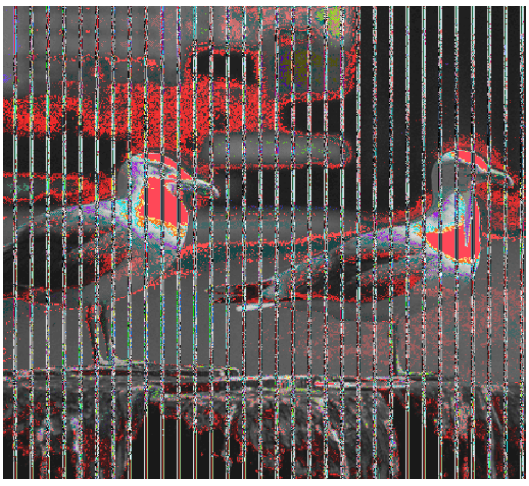


Fig. 4F Encrypted with Key K2 but Decrypted **with**

Fig. 4 Results of Key Sensitivity analysis for AES Algorithm without Shiftrows and Mixcolumns stages

Fig. 5A Plainimage Birds.bmp

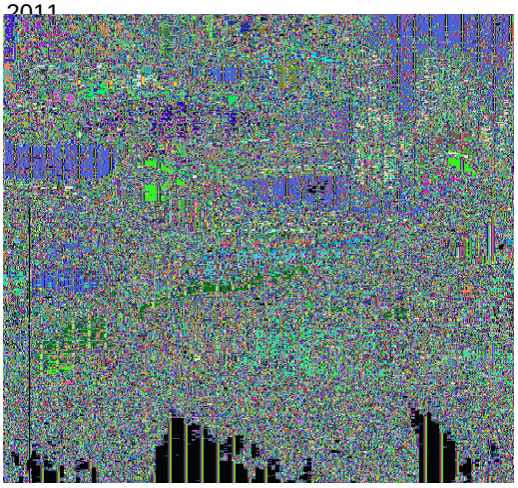


Fig. 5B Encrypted with Key K1

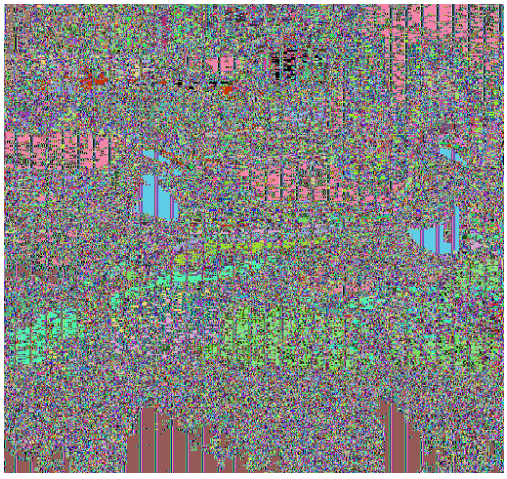


Fig. 5C Encrypted with Key K2

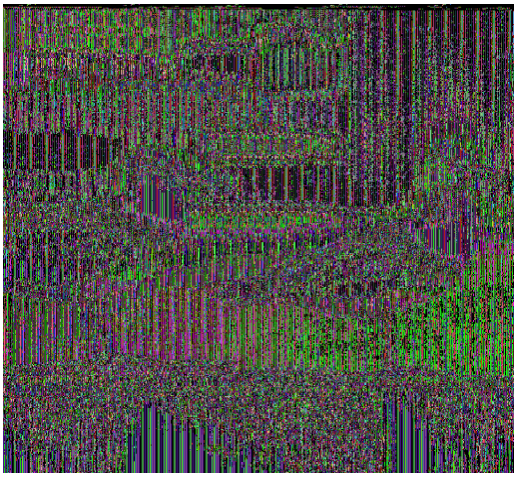


Fig. 5D Difference of Images in 5B & 5C

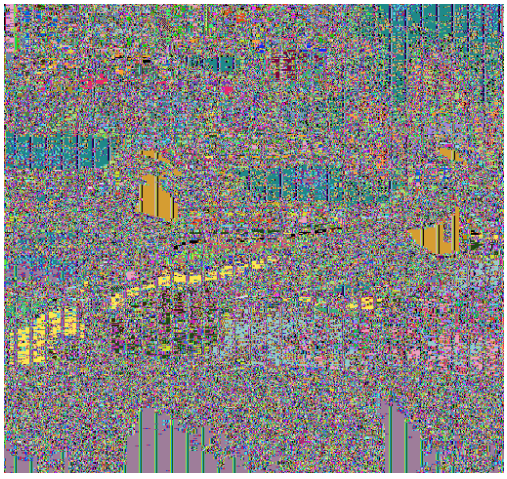


Fig. 5E Encrypted with Key K1 but Decrypted with K2

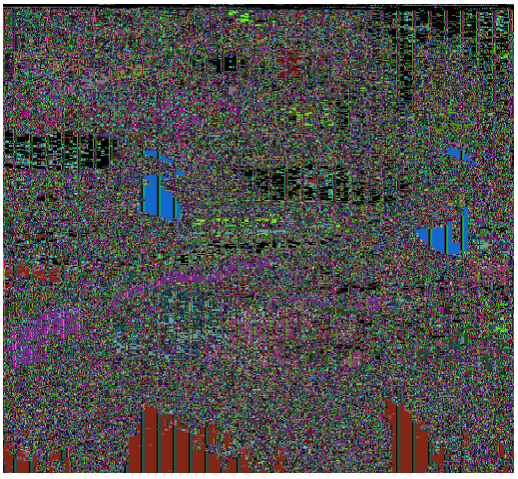


Fig. 5F Encrypted with Key K2 but Decrypted with K1

Fig. 5 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm Without Shiftrows stage

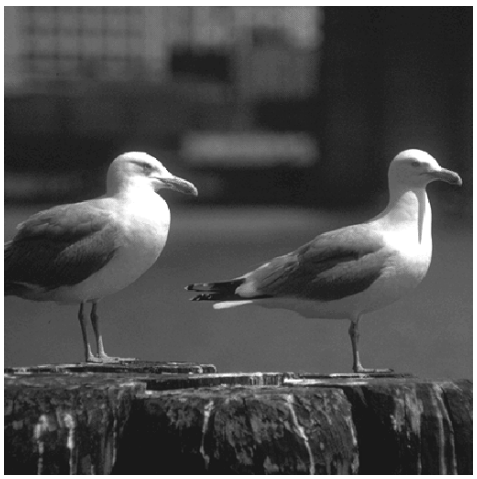


Fig. 6A Plainimage Birds.bmp

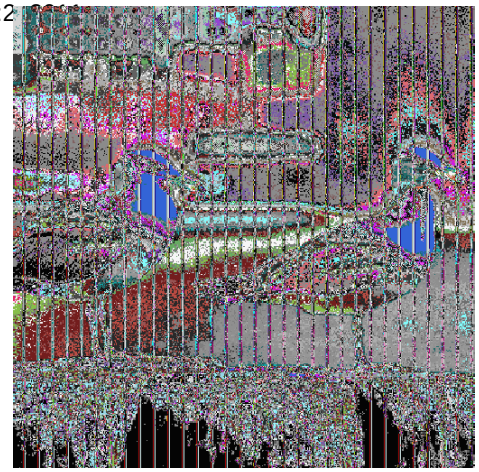


Fig. 6B Encrypted with Key K1

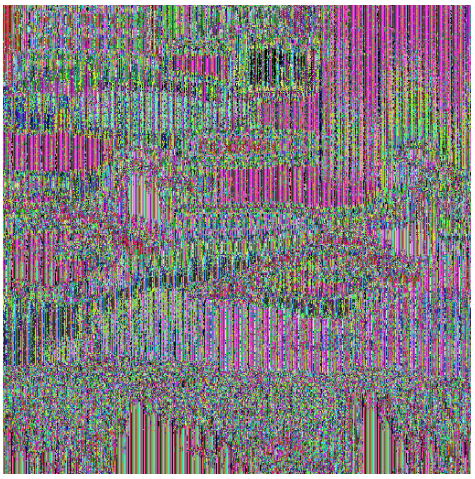


Fig. 6C Encrypted with Key K2

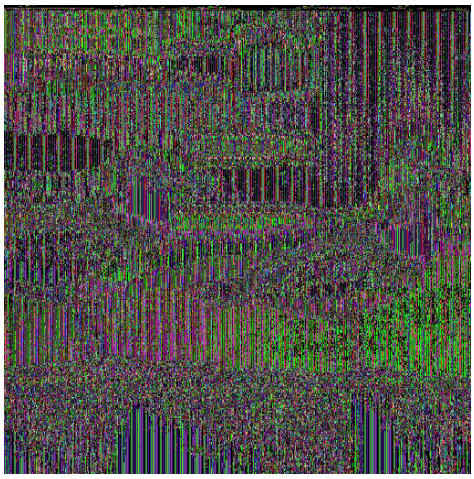


Fig. 6D Difference of Images in 6B & 6C

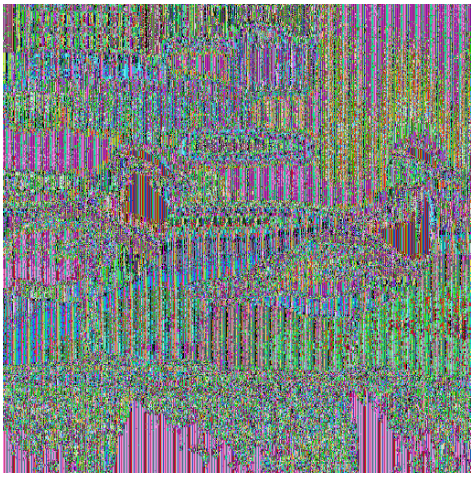


Fig. 6E Encrypted with Key K1 but Decrypted with K2

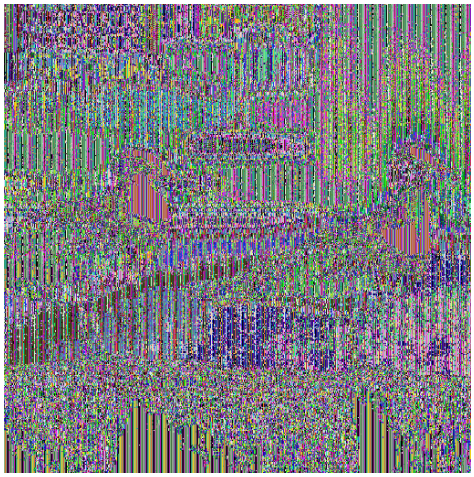


Fig. 6F Encrypted with Key K2 but Decrypted with K1

Fig. 6 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm without Mixcolumns stage

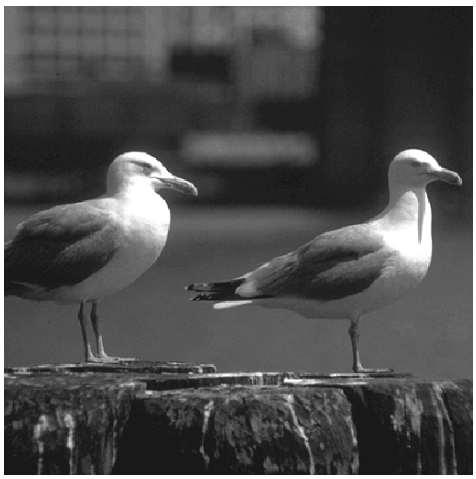


Fig. 7A Plainimage Birds.bmp

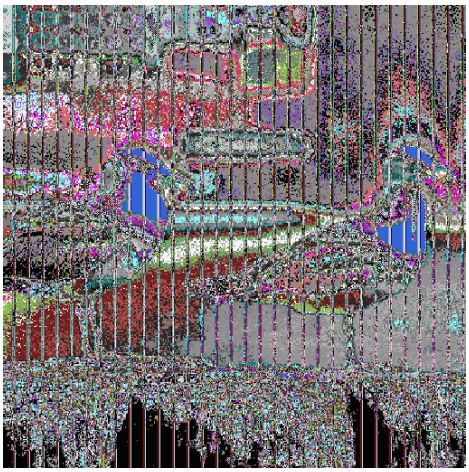


Fig. 7B Encrypted with Key K1

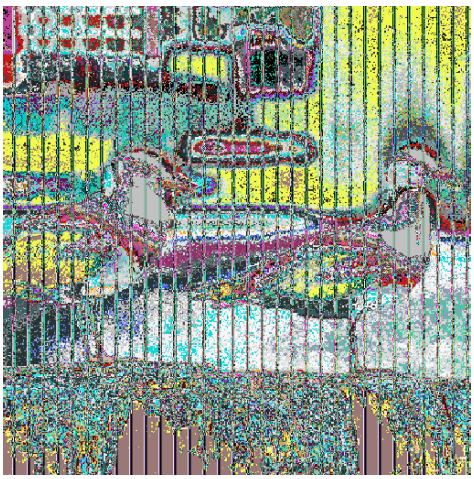


Fig. 7C Encrypted with Key K2

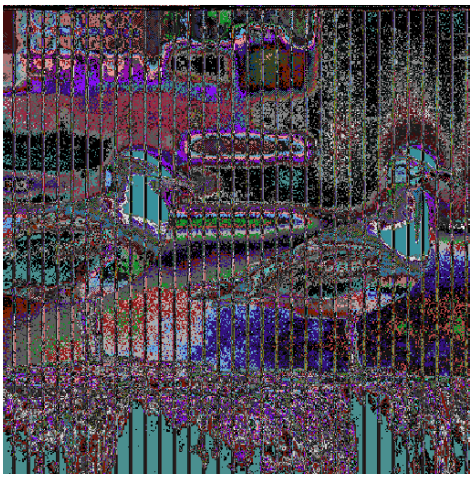


Fig. 7D Difference of Images in 7B & 7C

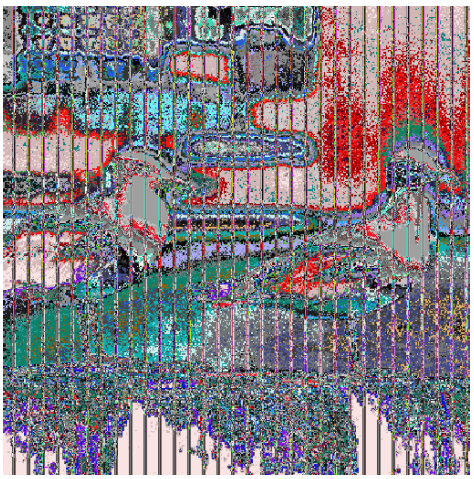


Fig. 7E Encrypted with Key K1 but Decrypted with K2

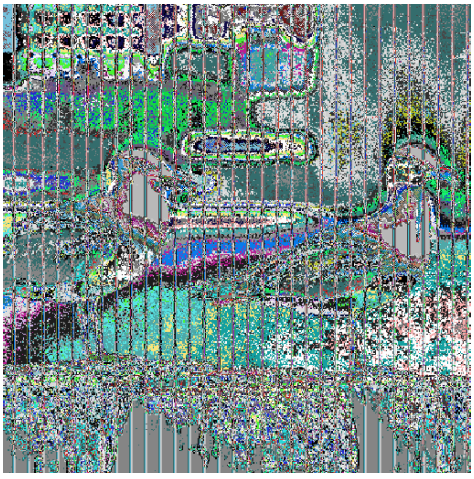


Fig. 7F Encrypted with Key K2 but Decrypted with K1

Fig. 7 Results of Key Sensitivity analysis for Case 3 of AES-KDS Algorithm without Shiftrows and Mixcolumns stages

V. Statistical Analysis

This is shown by a test on the histograms [6]-[10] of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

A. Histograms of Encrypted Images

We have selected Ship.bmp image as plainimage for histogram analysis. We have encrypted this image first by using AES without Shiftrows stage, then by using AES without Mixcolumns stage and finally by using AES with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Figure 8 shows the histogram for original image. Figures from 9 to 11 show histograms for encrypted images we just obtained. From figure 9B we can see that the histogram of the encrypted image (figure 9A) encrypted using AES without Shiftrows is fairly uniform and is significantly different from that of the original image. But the other two histograms (figures 10B and 11B) for encrypted images encrypted using AES without Mixcolumns and AES with both stages omitted, they are not uniform.

The percentages of number of pixels with a certain grey scale value range from 0 to 1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolums stage.

Similarly, we have encrypted plainimage (Ship.bmp) first by using AES-KDS (Case 3) without Shiftrows stage, then by using AES-KDS (Case 3) without Mixcolumns stage and finally by using AES-KDS (Case 3) with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Figures from 12 to 14 show histograms for encrypted images we just obtained. From figure 12B we can see that the histogram of the encrypted image (figure 12A) encrypted using case 3 of AES-KDS without Shiftrows is fairly uniform and is significantly different from that of the original image. But the other two histograms (figures 13B and 14B) for encrypted images encrypted using case 3 of AES-KDS without Mixcolumns and case 3 of AES-KDS with both stages omitted, they are not uniform.

The percentages of number of pixels with a certain grey scale value range from 0 to 1.1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolums stage.

The percentages of number of pixels with a certain grey scale value range from 0 to 1.1% and 0 to 1.8% respectively for the last two cases where as it is around 0.4% for the first case. This shows the importance of Mixcolums stage.

Fig. 8A Original Image (Ape.bmp)

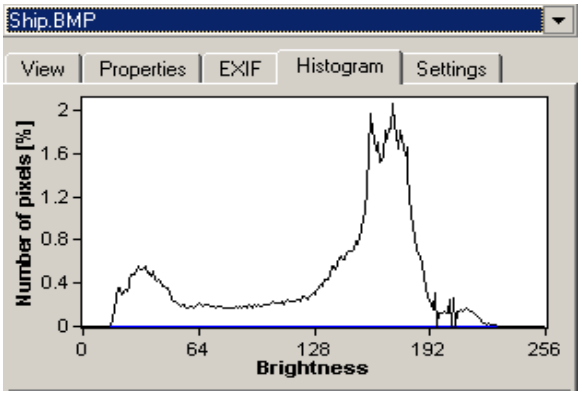


Fig. 8B Histogram for Original Image

Fig. 8 Histogram for Plainimage Ship.bmp

Fig. 9A Encrypted Image of Ship.bmp

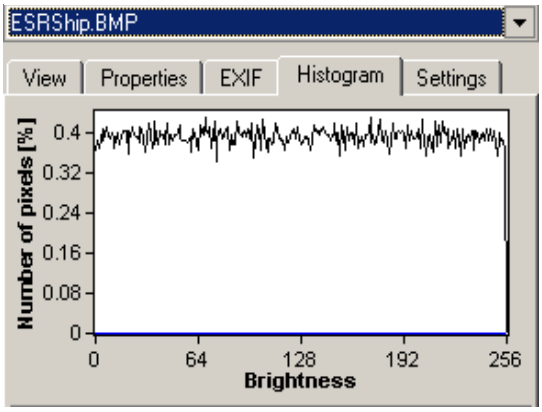


Fig. 9B Histogram of Encrypted Image

Fig. 9 Encrypted Image of Ship.bmp using of AES without Shiftrows and its Hitogram

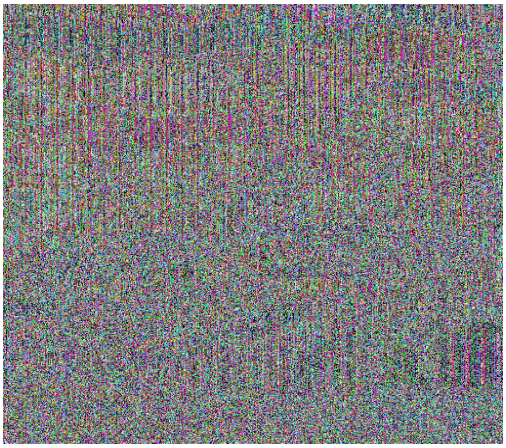


Fig. 10A Encrypted Image of Ship.bmp

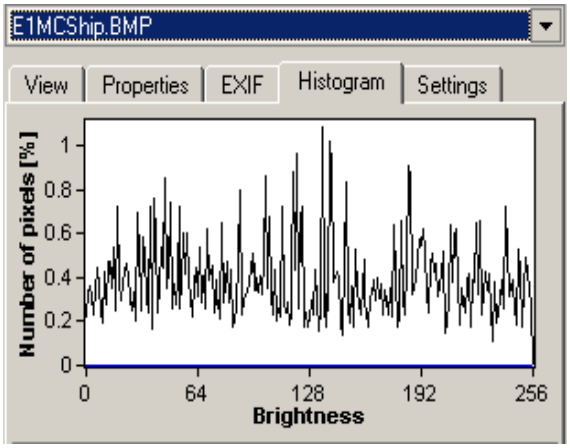


Fig. 10B Histogram of Encrypted Image

Fig. 10 Encrypted Image of Ship.bmp using of AES without Mixcolumns and its Hitogram

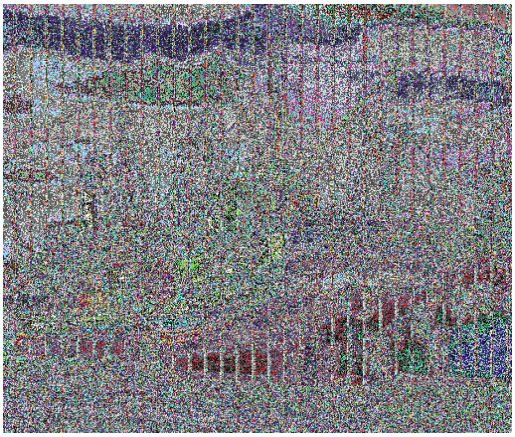


Fig. 11A Encrypted Image of Ship.bmp

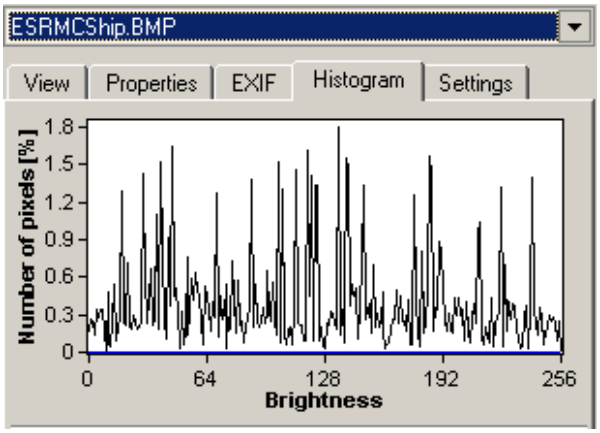


Fig. 11B Histogram of Encrypted Image

Fig. 11 Encrypted Image of Ship.bmp using of AES with bothShiftrows and Mixcolumns stages omitted and its Hitogram

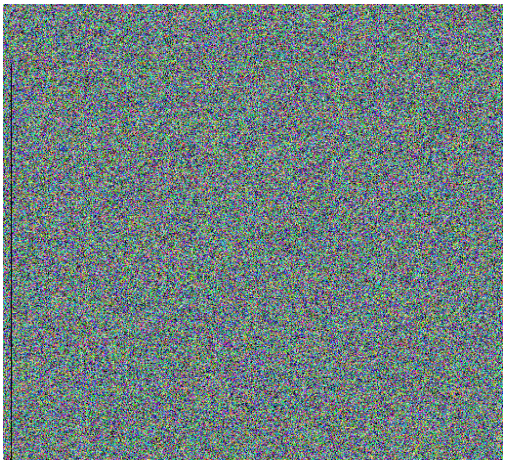


Fig. 12A Encrypted Image of Ship.bmp

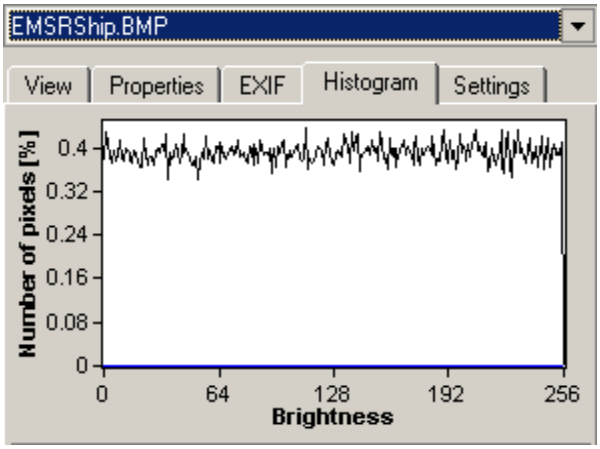


Fig. 12B Histogram of Encrypted Image

Fig. 12 Encrypted Image of Ship.bmp using Case 3 of AES-KDS without Shiftrows and its Hitogram

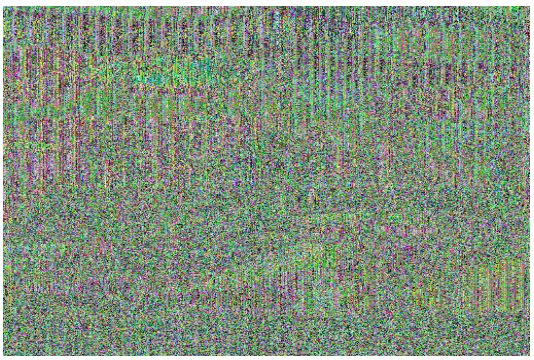


Fig. 13A Encrypted Image of Ship.bmp

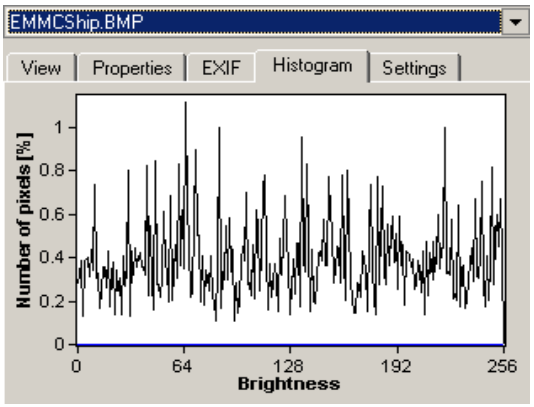


Fig. 13B Histogram of Encrypted Image

Fig. 13 Encrypted Image of Ship.bmp using Case 3 of AES-KDS without Mixcolumns and its Hitogram

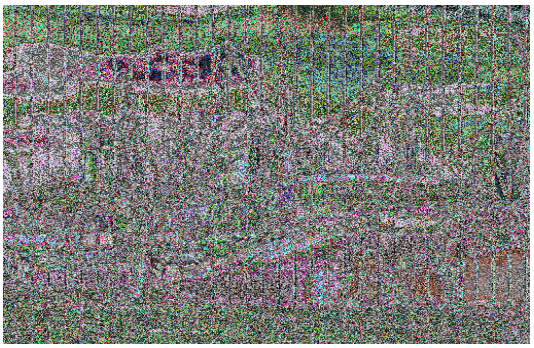


Fig. 14A Encrypted Image of Ship.bmp

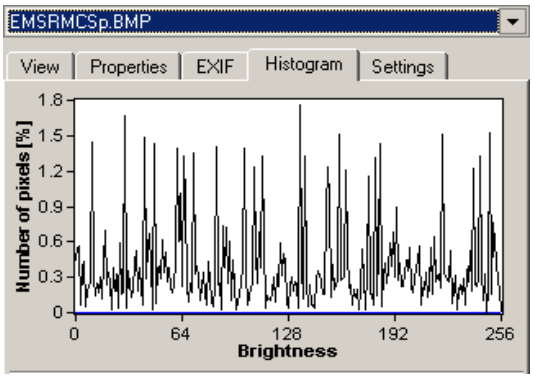


Fig. 14B Histogram of Encrypted Image

Fig. 14 Encrypted Image of Ship.bmp using Case 3 of AES-KDS with bothShiftrows and Mixcolumns stages omitted and its Hitogram

A. Correlation of Two Adjacent Pixels

To determine the correlation between horizontally adjacent pixels [6] - [10] in an image, the procedure is as follows:
First, randomly select N pairs of horizontally adjacent pixels from an image. Compute their correlation coefficient using the following formulae

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

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

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),$$

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

where x and y represent grey-scale values of horizontally adjacent pixels in the image. E(x) represents the mean of x values, D(x) represents the variance of x values, cov(x,y) represents covariance of x and y and r_{xy} represents correlation coefficient.
We have randomly selected 1200 pairs of two adjacent pixels from the plainimage Ship.bmp and its corresponding cipherimages encrypted first by using AES without *Shiftrows* stage, then by using AES without *Mixcolumns* stage and finally by using AES with both the stages omitted. Then we have generated histograms for plainimage and its encrypted images.

Then we have computed the correlation coefficient using the above equations.

The correlation coefficient for plainimage was found to be 0.962353. For ciherimage encrypted using AES without *Shiftrows* stage it is 0.009232, for ciherimage encrypted using AES without *Mixcolumns* stage it is 0.042035 and for cipherimage which is encrypted using AES with both the stages omitted, it is 0.057859. Figures 15 through 18 show the correlation distribution of two horizontally adjacent pixels for plainimage Ship.bmp and the encrypted images encrypted using AES without Shiftrows, AES without *Mixcolumns* and AES with both the stages omitted, respectively.

Similar results can be observed for AES-KDS with omitted stages. For ciherimage encrypted using case 3 of AES-KDS without *Shiftrows* stage it is 0.001801, for ciherimage encrypted using Case 3 AES-KDS without *Mixcolumns* stage it is 0.066177 and for cipherimage which is encrypted using Case 3 of AES-KDS with both the stages omitted, it is 0.012184. Figures 19 through 21 show the correlation distribution of two horizontally adjacent pixels for plainimage Ship.bmp and the encrypted images encrypted using AES-KDS without Shiftrows, AES-KDS without *Mixcolumns* and AES_KDS with both the stages omitted, respectively.

The correlation distribution graphs show similar results for all cases and hence we can cannot draw a clear cut inference from these. But correlation coefficients for AES-KDS without these stages appear to have lesser magnitudes compared to that of AES with omitted stages.

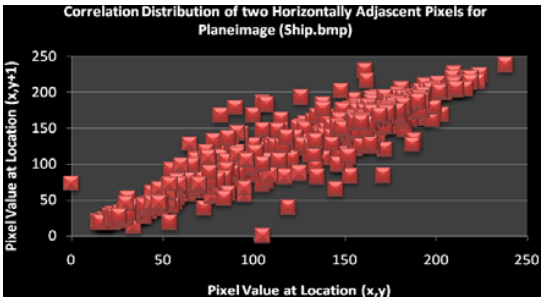


Fig .15 Correlation Distribution of two Horizontally adjacent Pixels for Plainimage (Ship.bmp)

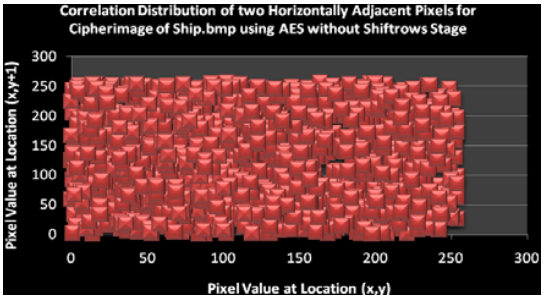


Fig. 16 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using AES without Shiftrows Stage

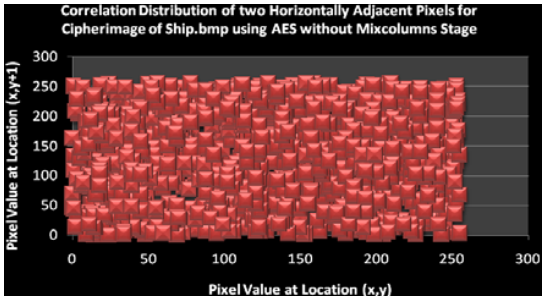


Fig. 17 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using AES without Mixcolumns Stage

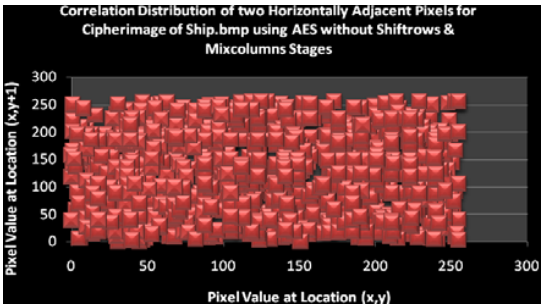


Fig. 18 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using AES without Shiftrows and Mixcolumns Stages

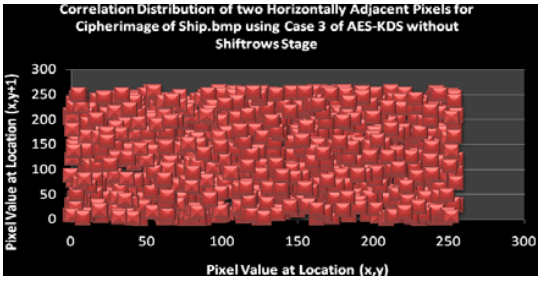


Fig. 19 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using Case 3 of AES-KDS without Shiftrows Stage

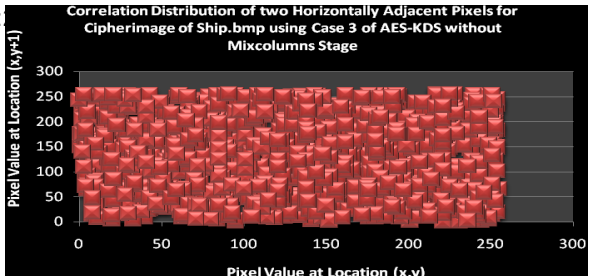


Fig. 20 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using Case 3 of AES-KDS without Mixcolumns Stage

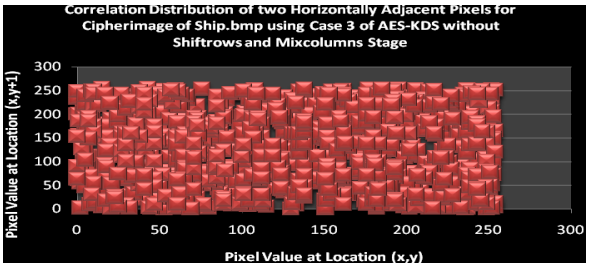


Fig. 21 Correlation Distribution of two Horizontally Adjacent Pixels for Cipherimage of Ship.bmp using Case 3 of AES-KDS without Shiftrows and Mixcolumns Stages

VI. Conclusion

We have made an attempt to analyze the security of original and modified version of AES algorithm after removal of either shiftrows or mixcolumns or both the stages. By this, we have shown the importance of these two stages and their contribution to the security of the algorithms.

References

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

[2] B. Schneier, "Applied Cryptography – Protocols, algorithms, and source code in C", John Wiley & Sons, Inc., New York, second edition, 1996.

[3] William Stallings, "Cryptography and Network Security", Third Edition, Pearson Education, 2003

[4] Krishnamurthy G N, Dr. V Ramaswamy "Making AES Stronger: AES with Key Dependent S-Box", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008, pp 388-398.

[5] Harley R. Myler and Arthur R. Weeks, "The Pocket Handbook of Image Processing Algorithms in C", Prentice-Hall, New Jersey, 1993

[6] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images", Journal of Optical Engineering, vol. 45, 2006

[7] Krishnamurthy G N, Dr. V Ramaswamy "Encryption quality analysis and Security Evaluation of Blow-CAST-Fish using digital images", Communicated to International Journal of Computational Science 2008.

[8] Krishnamurthy G N, Dr. V Ramaswamy, "Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its modified version using digital images", communicated to IAENG International Journal of Computer Science, 2008.

[9] Krishnamurthy G N, Dr. V Ramaswamy "Performance Analysis of Blowfish and its modified version using Encryption quality, Key sensitivity, Histogram and Correlation coefficient analysis", communicated to International Journal Conference in Recent Trends in Computer Science, India 2009.

[10] Hossam El-din H. Ahmed, Hamdy M. Kalash. And Osama S. Farang Allah, "Encryption Effeciency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", International Journal of

Computer, Information, and System Science, and Engineering: volume 1 number 1 2007 ISSN 1307-2331. pp 33-38.

Krishnamurthy G N born on 15th March 1974, at Davangere, India. He

has applied for membership of IAENG. He obtained his B.E. degree in Electronics & Communication Engineering from Kuvempu University in 1996 and M.Tech. degree in Computer Science & Engineering from Visveswaraya technological University, India in 2000. He has obtained his Ph.D. from Visveswaraya Technological University, India under the guidance of Dr. V Ramaswamy. He has published papers in national and international conferences, journals in the area of Cryptography. After working as a lecturer (from 1997) he has been promoted to Assistant Professor in the Department of Information Science & Engineering, Bapuji Institute of Engineering & Technology, Davangere, affiliated to Visveswaraya Technological University, Belgaum, India. He has worked as Professor and Head at Cambridge Institute of Technology and BNM Institute of Technology, Bangalore, from where he has been deputed to VTU, Belgaum and is presently working as Registrar(evaluation), Visvesvaraya Technological University, Belgaum. His area of interest includes Design and analysis of Block ciphers. Currently he is guiding two Ph.D. scholars under Visvesvaraya Technological University, Belgaum. He is a life member of Indian Society for Technical Education, India.

Dr. V Ramaswamy obtained his Ph.D. degree from Madras University, in

1982. He has applied for the membership of IAENG. He is working as Professor and Head in the Department of Information Science and Engineering. He has more the 25 years of teaching experience including his four years of service in Malaysia. He is guiding many research scholars and has published many papers in national and international conference and in many international journals and authored one book. He has visited many universities in USA and Malaysia. He is working as research head in the department of Computer Science & Engg., at Mahaveer Jain College of Engg., Bangalore, India. He is a life member of Indian Society for Technical Education, India.