Cryptanalysis of AES-128 and AES-256 Block Ciphers Using Lorenz Information Measure

Vetrivel Karuvandan[1], Senthamarai Chellamuthu[2], and Shantharajah Periyasamy[3]
[1]Department of Computer Applications, Anna University Regional Centre, India
[2]Department of Computer Applications, Government Arts College, India
[3]Department of Computer Applications, Sona College of Technology, India

Abstract: *Encryption algorithms will transform a human interpretable text block or information in to a non-interpretable block of symbols. The objective of any such encryption algorithm will be making the cipher block more non-interpretable and seemingly random block of symbols. So any cipher block will always be random and will purely be a set of random permutations of symbols. The efforts of distinguishing the cipher text of a cipher from random permutation and distinguishing a cipher blocks of different algorithms are called as "distinguisher attacks". Generally, almost all the classical ciphers are distinguishable and even breakable. But the modern ciphers have been designed to withstand against several kinds of attacks and even withstand against distinguisher attack. It means, we cannot even guess the type of cipher used for encryption only by seeing/analyzing the encrypted block of symbols. In this work our focus will be only on distinguisher attack on modern ciphers. For that, we have attempted to distinguish the cipher blocks of AES-128 and AES-256 using a metric called Lorenz Information Measure (LIM) which is commonly used in image and signal classification systems. In our findings, we showed that the cipher blocks of AES-128 and AES-256 are certainly distinguishable from one another.*

Keywords: *Encryption, cryptography, cryptanalysis, attack, distinguisher attack, AES.*

Received May 7, 2012; accepted February 11, 2013; published online June 11, 2015

1. Introduction

Cryptosystem or cipher system is a collection of algorithms which are labeled and the labels are generally called as keys. It is also, referred as a method of disguising messages which can limit the viewers. The disguised message is called as cipher text whereas the original message is plain text. Converting the plain text into cipher text is called encryption and the reverse is decryption. Cryptology is the study of cryptography and cryptanalysis refers to creation or usage of cryptosystems and breaking cryptosystems, otherwise, unauthorized viewers can access through disguise.

The evolution of cryptography has been paralleled by the evolution of cryptanalysis. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination and luck. Breaking a cipher simply means that finding a weakness in the cipher and can be exploited with a complexity less than brute force. The act of breaking a cipher text is called as attack. There are different kinds of attacks on different encryption algorithms such as cipher text only attack, known plaintext attack, chosen plaintext attack, chosen cipher text attack and chosen text attack. To start with a particular attack on a cipher text the cryptanalyst needs some of the following basic information:

- The cipher text to be attacked or decoded.
- Encryption algorithm originally used to get that cipher text.
- One or more plaintext and cipher text pairs.
- Plaintext chosen by the cryptanalyst and its corresponding cipher text.
- Cipher text chosen by cryptanalyst and its corresponding decrypted plaintext.

For each of the above said attacks, at least two more of the above mentioned basic information is needed. But in all kinds of attack, the most importantly needed information will be the "encryption algorithm originally used to arrive that cipher text". Without that information, one cannot do attack using any other information.

1.1. About this Work

A strong cryptosystem will certainly produce cipher text which appears random to all standard statistical tests. The scope of this research is to find any distinguishable characteristics from the so called random symbols of modern cipher block. In all kind of attack it was assumed that the "encryption algorithm originally used to produce that cipher text" was known to the cryptanalyst. The scope of this research is to identify the algorithm used for encryption directly from the given cipher text itself, using randomness and distribution of the symbols in the cipher text. As a first attempt, in this work, we tried to distinguish cipher blocks of AES-128 and AES-256 from one another.

In some of the practical applications or implementation of cryptographic communication systems, most of the protocols explicitly indicate type of the cipher during initial handshake. In such cases the usage of a distinguisher attack is meaningless. But in some more secured communication systems, initial handshake and key exchange will be handled by asymmetric-key cryptography and the mass data exchange will be handled by symmetric-key cryptography for performance reasons. In such case, the information indicating type of cipher (Symmetric-key cryptography part) can be exchanged through asymmetric-key technology. If we intervened with the communication for monitoring and auditing purpose, then finding the type of cipher will not be possible.

This work addresses the methods for identifying or distinguishing a cipher block from random permutations which may commonly occur in communication scenarios. Further it will address the methods for differentiating one type of cipher from another. As a proof of concept, we will show that the AES-128 and AES-256 Cipher blocks are distinguishable using Lorenz Information Measure (LIM).

2. Related Works

There is not much previous works on distinguisher attack on modern ciphers. Some of the related research reports related with cryptanalysis that were previously published are reviewed and presented here.

2.1. Works Related with Cryptanalysis

Ajlouni *et al.* [1] specified AES is a variant of Rijndael algorithm, AES is symmetric block cipher and have simple design, highly efficient in term of space. This has a fixed block size of 128bits and a key size of 128, 192, or 256bits. Various methods in the key generation have been proposed.

Biham [2] described 2 new types of cryptanalytic attacks using related keys, which are based on the structure of key scheduling algorithms and independent of the number of rounds of the cipher.

Biryukov *et al.* [3] given that full AES-192 and AES-256 attacks are boomerang attacks, based on finding local collision in block ciphers and enhanced the boomerang switching techniques to gain free rounds in middle.

Bogdanov and Rijmen [4] proposed the concept of bicliques for block cipher cryptanalysis and give various applications to AES, including a key recovery method for the full versions of AES-128, AES-192~~,~~ and AES-256. Also, the data complexity of key recovery can be significantly reduced by sacrificing only a small factor of computational advantage. So, it concluded that properties of AES that allowed covering more rounds than in previous cryptanalysis methods.

Kaur [8] research report described that AES provides a better combination of performance and enhanced network security than DES and 3DES by being computationally more efficient than earlier standards. Also it supports large key sizes of 128, 192 and 256bits. So, AES offers higher security against brute force attacks.

Sharma *et al.* [15] discussed about hashing the plain text at the sender side using modified message digest algorithm and verifying that at the receiver end based on misleading text. This scheme can be applied for authentication like security in databases.

Mendel *et al.* [12] proposed two new ways to mount attacks on the SHA-3 candidates Grθ stl and ECHO, and apply these attacks also to the AES. The results improved upon and extend the rebound attack. Also the author presented an improved known-key distinguisher for 7-rounds of the AES block cipher and the internal permutation used in ECHO.

Later, Mondel [13] thesis work described about an attack based on key exchange protocols that allows an adversary to mount related key queries on the underlying cipher and proved it is extremely powerful.

A new paradigm of cryptography named quantum public key cryptosystem, which consists of quantum public key encryption and quantum digital signatures presented by Okamoto *et al.* [14]. The author proved that a concrete scheme is very efficient if quantum turing machine is realized.

In the recent development of cryptographic key strength, Kleinjung and Lestra [9] proposed a new methodology to assess cryptographic key strength used in cloud computing, by calculating the true economic cost of (symmetric- or private-) key retrieval for the most common cryptographic primitives.

Garfinkel [5] has discussed traditional anti-forensic techniques such as encrypted file system disk sanitization utilities and evaluated the effectiveness of anti-forensic tools for defecting computer forensic tools which allow investigators to recover deleted files, reconstruct intruder activities and gain intelligence about users of a computer.

Soleimany *et al.* [17] work was partially supported by Iran Telecommunications research center and the cryptography chair of the Iranian NSF. They evaluated the extended 8-round attack on 9-round AES-256 and is found more efficient than the previous attacks from both time and data complexity.

Shoup and Gennaroz [16] designed two very practical threshold cryptosystems TDH1 and TDH2 (diffie-hellman threshold) and proved that they are secure against chosen cipher text attack in the random hash function model. The main difference is instead of changing the group element with each encryption, it is chosen at key generation time.

Li *et al.* [10] examined the effect of weakly chosen password-keys on the security of block ciphers by introducing a new hybrid optimization heuristics cryptanalytic attack to conduct an intelligent key-search attack on classical and modern ciphers.

Academic research in block ciphers has progressed along a different course than research in stream ciphers. Block cipher papers have traditionally been concrete designs (with specific parameters and names) or breaks of those designs. Stream cipher papers are more often general design or analysis techniques, with general applications and examples.

While stream-cipher cryptanalysis is at least as important as block cipher cryptanalysis and is more important in military circle.

2.2. Works Related with Information Measure

Since 1980, numerous researchers have proposed many theories to analyze the retrieval of images. Chang and Yang proposed a specific innovation to simplify image data derived largely from histograms and suggested a formula called a Picture Information Measure (PIM) generalized from the LIM widely used in economics. The LIM is a function of the observed probability sequence of digital signals, similar to the signal entropy. Rorvig was among the first researchers to suggest the use of general features of images extracted from retrieval and represented as LIMs. In his research, six general pattern features were used such as gray level, edge intensity, edge slope, line length, line distance and angle distance from the origin. Later, Jeong explored color features in his research and Ju Han and Ma [6] proposed image analysis based on relative changes in image pixel values. During this period many researchers proposed different approaches to achieve content-based information retrieval [7]. In this work, we use LIM for measuring the cipher blocks of AES-128 and AES-256 to distinguish them from one another.

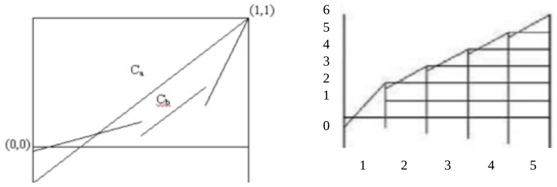
3. Modelling

3.1. Information Similarity Measure

We attempted to use information similarity measure from image mining domain to distinguish the encrypted blocks of different algorithms from one another.

The LIM is a function of the observed probability sequence of digital signals, similar to signal entropy, and is linearly related to Mean Absolute Error (MAE) in simulations employing uncorrupted and corrupted 2-dimensional Gaussian signals or distribution [11]. The LIM is commonly used information measure in image and signal processing. After finding histogram of a distribution, it will form a curve structure by sorting the histogram bins, the LIM is a measure which will indirectly measure or signify the curvature of the curve.

The *LIM*(P_1, …, P_n) is defined to be the area under lorenz information curve. Thus, from Figure 1-a, the area of *LIM* C_a is greater than the area of *LIM* C_b. Clearly, 0<=*LIM*(P_1, …, P_n)<=0.5. For any probability vector (P_1, …, P_n), *LIM*(P_1, …, P_n) can be calculated by the first ordering P_i's, then calculating the area under piecewise linear curve. Since, *LIM*(P_1, …, P_n) (which can be expressed as the sum of $f(P_i)$ and $f(P_i)$) is a continuous convex function, *LIM*(P_1, …, P_n) is considered as an information measure [11].



a) Curve.

b) Example.

Figure 1. The graphical representation of LIM.

After finding the histogram of a distribution, if we sort the histogram bins, then it will form a curve structure.

The following is Algorithm 1 to Compute *LIM*

Algorithm 1: Compute LIM.

```
# MAX=max (Histogram);
# Histogram= (Histogram/MAX)*100;
sd=sort (Histogram);
p= 0;
x=256;
w=1/x;
t=0;
for i= 1:256
    t= t+sd (i);
end
for i= 1:256
    p= p+ (x - i) * sd (i)/ t;
end
LIM= w * (p+0.5);
```

Intuitively, the LIM can be regarded as a global content-based information measure. To compute area of histograms, the histogram intervals are sorted from low to high, and the resulting off a diagonal shape is measured through differentiation.

Here, is an example to understand this formula by Visualization. Let's assume a simple histogram with 5 bins P_1 to P_5.

$$P_1=2, P_2=3, P_3=4, P_4=5, P_5=6$$

So, total number of elements is 20.

W=*I* then, according to the formula

$$\begin{aligned} LIM &= 1((2+3+4+5)+(2+1+1+1+1)/2)2*20 \\ &= 17/4 \\ &= 0.425 \end{aligned}$$

In Figures 1-a and b, the x-axis is the histogram bins (of elements/symbols) and the y-axis is the number of occurrences.

3.2. A Simple Model for Distinguishing Different Types of Cipher Blocks

The flow chart in Figure 2 shows that simple LIM-based model which can be used to distinguish cipher locks of different ciphers.

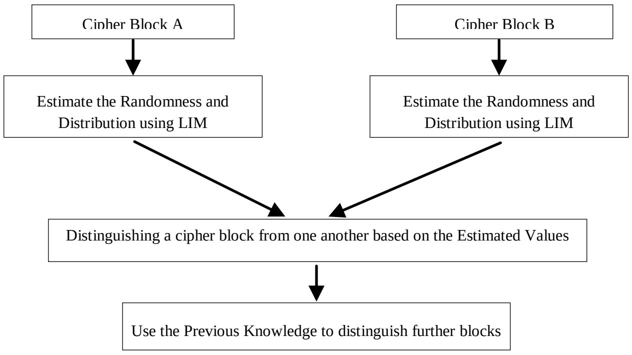

Cipher Block A
Cipher Block B
Estimate the Randomness and Distribution using LIM
Estimate the Randomness and Distribution using LIM
Distinguishing a cipher block from one another based on the Estimated Values
Use the Previous Knowledge to distinguish further blocks

Figure 2. Generic model for distinguishing different types of cipher blocks.

Practically, the use of single block will not lead to accurate result. So, it has to use a set of uniform blocks of same types to find *LIM* of individual blocks and take the average of all to get significant difference between two or more classes of cipher blocks. The process of distinguishing two cipher blocks have been shown as a flowchart in Figure 2.

The following is Algorithm 2 steps for calculating *LIM* of a cipher text:

Algorithm 2: steps for calculating LIM of a cipher text.

```
Take the cipher text which is to be distinguished
Split the cipher text in to N uniform blocks of text.
For each block
    Find the histogram
    Sort the histogram
    Find LIM of sorted histogram
    Store the LIM value of the block
Take Average of all the N LIM values of the individual blocks.
The Average LIM value will be used to distinguish the block from another.
```

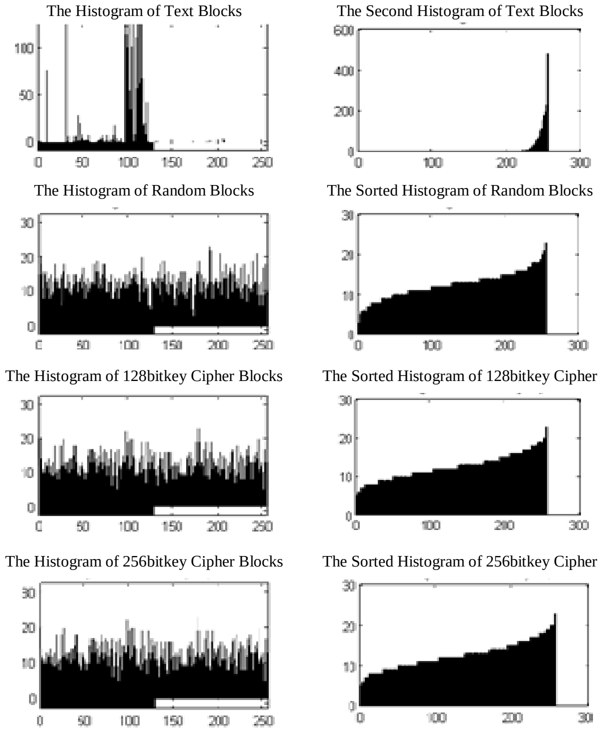


Figure 3. An example of histograms and sorted histograms calculating LIM.

Figure 3 shows that an example of histogram and sorted histograms calculating *LIM* value.

The left part of the figure represents all the plots of histograms of files with different kinds of blocks such as plain text file, a random permutation block file and two different cipher block files with bit keys 128 and 256. The x-axis is the index of symbols used in the block (there are 256 symbols in total, from the value 0 to 255). The x-axis is automatically scaled up to 300 but only having values up to 255. The y-axis denotes the total accuracy of the symbol in the block under consideration.

Right part is the corresponding sorted histograms of the left side histograms; perceived a slight difference in the shape of virtual curvature formed by the sorted bins of the histogram. This is the main aspect of LIM measure. The x-axis is the index of symbols after sorting them (there are 256 symbols in total, from the value 0 to 255). The x-axis is automatically/roughly scaled up to 250. The y-axis denotes the total accuracy of the symbol in the block under consideration. This sorted histogram is only used for the calculation of *LIM* value.

4. Results and Discussion

We have tried to distinguish the two different cipher blocks (AES-128 and AES-256), random blocks and plain text blocks using the LIM based metric. The text files used in this work were randomly collected from internet from different subject’s biology, mathematics, data mining etc. For calculating LIM values of text blocks and encrypted blocks the hexadecimal equivalent of the symbols were used. The encryptions of those files were done using randomly selected keys.

For each experiment, we have used 100 files from each class (4 classes-1.AES 128 Encrypted Block, 2.AES 256 Encrypted Block, 3.Random text Block and 4.Text Block) and 400 files in total for one set of experiment. We have repeated the experiment with three different sets of files and that makes 1200 files in total. Each file is 100 blocks in size. Each block is made up of 256bits. So, each file is around 3200bytes in size. Since, we have encoded the bytes in short integer format (stored in 3bytes for a symbol + a space delimiter), the file size was around 3200×4= 12800bytes (around 13kb).

In each experiment with 400 files (100 files in each class), the average was calculated in the increment of 10 and results were tabulated in Tables 1, 2 and 3. It ends up with three tables of results Tables 1, 2 and 3, since three different set of files were used. Finally, the overall average was also calculated.

The following tables and graphs were the results of first set of experiment.

Table 1. The avg. LIM values of experiment 1.

No. Files	128 Bit Encryption	256 Bit Encryption	Random Block	Text Block
10	0.499558	0.499576	0.501407	0.640818
20	0.499638	0.500065	0.500352	0.641900
30	0.500320	0.500784	0.500086	0.646120
40	0.499635	0.500728	0.499731	0.648295
50	0.499959	0.500949	0.499862	0.653283
60	0.499505	0.500303	0.499642	0.654741
70	0.499774	0.500781	0.499840	0.661034
80	0.499195	0.500691	0.499938	0.666788
90	0.499306	0.500778	0.499858	0.671259
100	0.499457	0.500826	0.500099	0.674276
Avg	**0.499635**	**0.500548**	**0.500082**	**0.655851**

Table 2. The avg. LIM Values of experiment 2.

No. Files	128 Bit Encryption	256 Bit Encryption	Random Block	Text Block
10	0.499617	0.499972	0.502185	0.640818
20	0.499835	0.499859	0.502281	0.641900
30	0.498867	0.500464	0.502033	0.646120
40	0.499852	0.500136	0.501777	0.648295
50	0.499576	0.500285	0.501418	0.653283
60	0.499547	0.500698	0.501597	0.654741
70	0.499343	0.500986	0.501626	0.661034
80	0.500085	0.501221	0.501184	0.666788
90	0.500065	0.500784	0.500762	0.671259
100	0.500173	0.501114	0.500482	0.674276
Avg	**0.500173**	**0.501114**	**0.500482**	**0.674276**

Table 3. The avg. LIM values of experiment 3.

No. Files	128 Bit Encryption	256 Bit Encryption	Random Block	Text Block
10	0.499558	0.499576	0.501407	0.640818
20	0.499638	0.500065	0.500352	0.641900
30	0.500320	0.500784	0.500086	0.646120
40	0.499635	0.500728	0.499731	0.648295
50	0.499959	0.500949	0.499862	0.653283
60	0.499505	0.500303	0.499642	0.654741
70	0.499774	0.500781	0.49984	0.661034
80	0.499195	0.500691	0.499938	0.666788
90	0.499306	0.500778	0.499858	0.671259
100	0.499457	0.500826	0.500099	0.674276
Avg	**0.499635**	**0.500548**	**0.500082**	**0.655851**

4.1. The Significance of LIM Values

If the distribution of the symbols in encrypted block is purely random, then we may consider it as a very good encryption algorithm of course the entire encryption algorithm will try to accomplish that level of randomness. If the *LIM* value is 0.5 or almost 0.5, then it signifies that the symbols in that block are purely random. But if the *LIM* value is deviating from 0.5, then it signifies that there exists some pattern in the occurrences and distribution of symbols.

The following bar chart Figure 4 shows the average values of *LIMs* of four classes of the blocks used in the first set of experiment. For the first look, we cannot distinguish any difference in the values of the first three (AES-128blocks, AES-256blocks and random blocks). All the three seems to be almost equal. The only observable difference is, the *LIM* of the text block is well distinguishable from the other three.

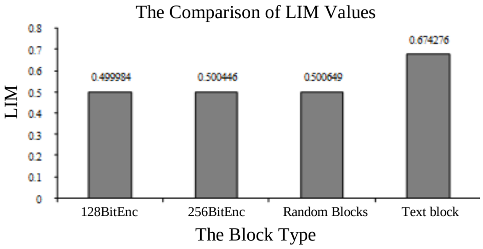


Figure 4. LIMs of experiment 1.

But, if we carefully observe the *LIM* values of AES-128 and AES-256, then there was obvious and distinguishable. It was clearly observed that a distinguishable difference between the *LIM* values of AES-128 and AES-256 from the chart as depicted in Figure 5.

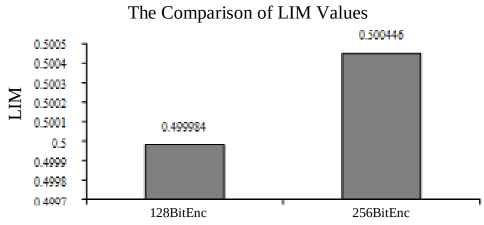


Figure 5. LIMs of cipher blocks of experiment 1.

Table 2 and charts in Figures 6 and 7 were the results of second set of experiment. From the output of second experiment it was observed that all the first three seems to be almost equal. The only observable difference is the *LIM* of the text block is well distinguishable from the other three.

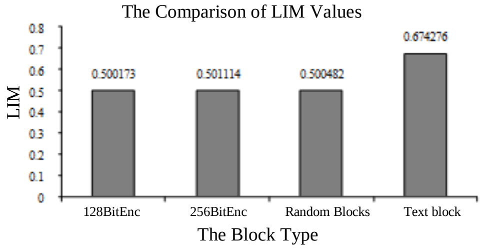


Figure 6. LIMs of experiment 2.

It was observed that in the case of experiment 2 also there was a distinguishable difference in the LIM values of AES-128 and AES-256. This difference is clearly illustrated as a chart in Figure 7.

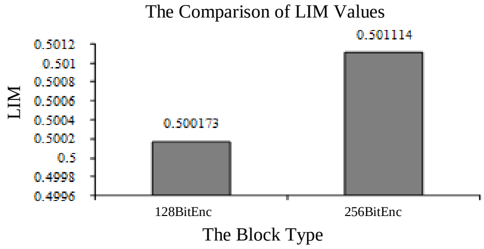


Figure 7. LIMs of cipher blocks of experiment 2.

Table 3 and charts in Figures 8 and 9 shows results of third set of experiment.

It was observed that the results of experiment 3 also proved that all the first three blocks are equal and the text block of *LIMs* value is higher than that of other three blocks.

But, it was observed that the *LIM* values of AES-128 and AES-256 in experiment 3 has also given a distinguishable difference between these cipher blocks which is represented as a chart in Figure 9.

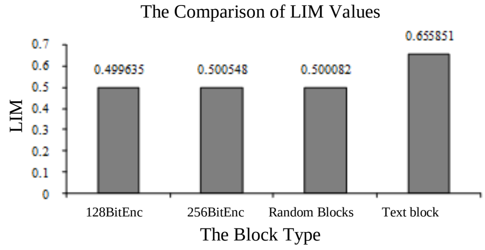


Figure 8. LIMs of experiment 3.

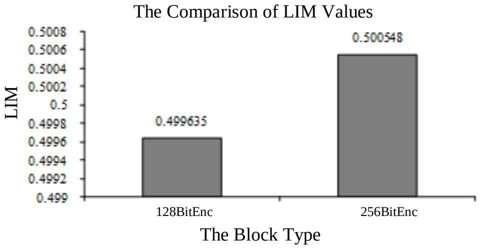


Figure 9. LIMs of cipher blocks of experiment 3.

From the above results, particularly the AES-128 and AES-256 comparison charts, it was observed that a significant and distinguishable difference in the text block and the cipher blocks. In all the three cases, *LIM* values of the AES-128 encrypted blocks were less than that of the *LIM* values of AES-256 encrypted blocks.

The results of the above three set of experiments clearly shows the measurable statistical relationship among different cipher blocks, text blocks and random blocks. Even though it is a small difference in *LIM* values, this will certainly open new possibilities of more complicated statistical analysis on the cipher blocks of unknown algorithm to identify the algorithm used.

5. Conclusions

We have successfully implemented and evaluated a LIM based distinguisher attack for distinguishing AES-128 and AES-256 cipher blocks. Our experimental results prove that the different kinds of cipher blocks of AES are distinguishable if there is few cipher blocks of them is available. Our experiment shows that, even the text blocks arbitrarily chosen and encrypted with arbitrary random key can be distinguishable. As shown the charts of previous section, the attack based on *LIM* metric was successful and the results were more significant and comparable.

The results of previous section shows that the number of occurrences and distribution of symbols the encrypted blocks of AES-128 and AES-256 were not purely random and there exists a statistical relationship between the symbol distribution in encrypted form and the encrypting algorithm. Even though with the minimum differences, they were certainly measurable. This result shows the very possibility of distinguisher attack on modern encryption algorithms.

In this work, we have only considered AES-128 and AES-256 cipher blocks for the attack since we expected some obvious difference in the distribution of the symbols with respect to the key size. The future works will address the problems in distinguishing other cipher blocks and will address a generalized model for a classification system based on *LIM* metric. We will explore the possibilities of applying other statistical techniques such as Principal Component Analysis (PCA) and least Linear Discriminant Analysis (LDA) for more accurate and distinguishable results. Further we will address the possibilities of using neural network based machine learning techniques for modeling an automated cipher block classification system. In this work, our attempts to distinguish the difference between a cipher block and random permutations (blocks) did not produced any significant result. Even though we perceive little difference in *LIM* values, it was not significant enough to support that idea. Future works may address the methods to magnify this slight difference and address a method to distinguish a random block from a cipher block.

Acknowledgments

We would like to thank the reviewers for their valuable suggestions and comments to improve the quality of the paper. We are also grateful to Dr.G.Arumugam, Principal Investigator, CDBR-SSE Project Sponsored by National Technical Research Organization (NTRO), Government of India, Madurai Kamaraj Universiy, Madurai.

References

[1] Ajlouni N., El-Sheikh A., and Rashed A., "A New Approach in Key Generation and Expansion in Rijndael Algorithm," *the International Arab Journal of Information Technology*, vol. 3, no. 1, pp. 35-41, 2006.

[2] Biham E., "New Types of Cryptanalytic Attacks using Related Keys," *Journal of Cryptology*, vol. 7, no. 4 , pp. 229-246, 1994.

[3] Biryukov A., Khovratovich D., and Nikolic I., "Distinguisher and Related-Key Attack on The Full AES-256," *in Proceedings of the 29th Annual International Cryptology Conference*, Santa Barbara, USA, pp. 231-249, 2009.

[4] Bogdanov A. and Rijmen V., "Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers," *Designs, Codes and Cryptography*, vol. 70, no. 3, pp. 369-383, 2011.

[5] Garfinkel S., "Anti-Forensics: Techniques, Detection and Countermeasures," *in Proceedings of the 2nd International Conference on i-Warfare and Security*, pp. 77-84, 2006.

[6] Han J. and Ma K., "Fuzzy Color Histogram and its Use in Color Image Retrieval," *IEEE Transactions on Image Processing*, vol. 11, no. 8, 2002.

[7] Jeong K., Rorvig M., Jeon J., and Weng N., "Image Retrieval by Content Measure Metadata Coding," available at: http://www10.org/ cdrom/posters/p1142/index.htm, last visited 2001.

[8] Kaur A., "Efficient Hardware Implementation for the Advanced Encryption Standards and RC6 Algorithms," *Thesis Report*, Thapar University, 2011.

[9] Kleinjung, T., and Lenstra K., Page D., Smart P., "Using the Cloud to Determine Key Strengths," *in Proceedings of the 13th International Conference on Cryptology in India*, Kolkata, India, pp. 17-39, 2012.

[10] Li H., Samsudin A., and Belaton B., "Heuristic Cryptanalysis of Classical and Modern Ciphers," *in Proceedings of the 7th International Conference on Communication, Maylaysis*, pp. 6, 2005

[11] McMurray T. and Pearce J., "Theoretical and Experimental Comparison of the Lorenz Information Measures, Entropy and the Mean Absolute Error," *in Proceedings of the IEEE Southwest Symposium Image Analysis and Interpretation*, Dallas, TX, pp. 24-29, 1994.

[12] Mendel F., Peyrin T., Rechberger C., and Schlaffer M., "Improved Cryptanalysis of the Reduced Grθstl Compression Function, ECHO Permutation and AES Block Cipher," *in Proceedings of the 16th Annual International Workshop*, Alberta, Canada, pp. 16-35, 2009.

[13] Mondal M., "Cryptanalysis of Ciphers based on AES Structure," *Thesis Report*, IIT Kharagpur, 2010.

[14] Okamoto T., Tanaka k., and Uchiyama S., "Quantum Public-Key Cryptosystems," available at: citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.119.8671&rep=rep1&type=pdf, last visited 2000.

[15] Sharma N., Sharma A., and Lovellin, "A New Encrypting Scheme for Hiding Text Messages," *International Journal of Advances in Computer Networks and its Security*, vol. 1, pp. 418-420, 2011.

[16] Shoup V. and Gennaroz R., "Security Threshold Cryptosystems against Chosen Ciphertext Attack," available at: https://www.iacr.org/ archive/asiacrypt2001/22480353.pdf, last visited 1997.

[17] Soleimany H., Sharifi A., and Aref M., "Improved Related-Key Boomerang Cryptanalysis of AES-256," *in Proceedings of International Conference on Information Science and Applications*, Seoul, pp. 1-7, 2010.

Vetrivel Karuvandan received his MCA degree from Anna University, India in 2007. He is pursuing his PhD degree in Computer Applications at Anna University, India. Currently, he is working as a Teaching Assistant in the Department of Computer Applications, Anna University Regional Centre Coimbatore, Tamil Nadu, India. His research interests are in the area of computer communication networks, data mining.

Senthamarai Chellamuthu received her BSc (Physics), MCA degree from University of Madras in 1987 and 1991 respectively and PhD in Computer Applications from the Periyar University in 2008. Her research interest includes grid computing, cloud computing, data mining and computer communication networks. She is currently working as an Assistant Professor of Computer Applications in Government Arts College (Autonomous), India. She has more than 18 Years of teaching and 10 Years of research experience. She has published 10 research papers in various National and International Conferences and has 4 International publications. She has delivered special lectures at Conferences, Seminars and Workshops. She is a life member of ISTE and CSI.

Shantharajah Periyasamy Prof. of Computer Applications, in Sona College of Technology, India. His research interest includes network security data mining. He has published 9 papers in various National and International Journals. He is a life member of ISTE, CSI