INROADS (Special Issue)
Vol. 3, No. 1, Jan-June, 2014, pp-335-339

Cryptographic Primitives for Multimedia Security

Sakshi Dhall[#†1], Saibal K. Pal[*2] and Kapil Sharma[¥3]
[#]*Assistant Professor, Department of Mathematics, Jamia Millia Islamia University, New Delhi-110 025*
[†]*Research Scholar, Department of Computer Engineering, Delhi Technological University, New Delhi-110 042*
[*]*Scientific Analysis Group, DRDO, Metcalfe House Complex, Delhi-110 054, India*
[¥]*Department of Computer Engineering, Delhi Technological University, New Delhi-110 042, India*
Email: [1]sakshidhall@gmail.com; [2]skptech@yahoo.com; [3]kapil@ieee.org

ABSTRACT

Today, voluminous amount of sensitive digital information is exchanged through penetrable networks. Of late, with the advancements in the digital and mobile technology there has been a significant shift in the type of transmitted content. The transmissions are no more limited to text-based data; they contain significant percentage of multimedia-based content. Traditional symmetric ciphers like AES, DES IDEA & RC4 have been focusing on securing textual data, and are not found suitable for meeting the special resource efficiency requirements and catering the intrinsic properties of redundancy and bulkiness of multimedia. It has been largely observed that the focus of researchers has been limited to one of the two key aspects pivotal to multimedia security i.e. cost efficiency and strength, in-turn compromising on the others. Therefore, a need is identified for lightweight solution to secure multimedia with complete removal of redundancy for real-time and resource constrained environments. The work proposes designing new cryptosystems using primitives derived from chaos based sequence generation for substitution and diffusion. Also, scope for customization of standard cryptosystems using chaos is presented with supporting experimental results.

Keywords: Multimedia security, block cipher, efficiency, chaos

INTRODUCTION

The outgrowth of internet in its purpose and role has lead to an unending emergence of digitization in almost every aspect of life including military, medical science, banking, education, service industry, forensics, entertainment, tourism, social media, e-commerce etc… The diverse applications like Voice over IP (VoIP), audio/video-on-demand, broadcasting etc… clearly indicate the shift in the nature of data being transmitted from text to multimedia[1,2]. It makes it inevitable to address the emerging need for securing voluminous transmissions of multimedia content over inherently vulnerable networks.

Cryptography[3,4] provides mechanisms for concealing information content so that it is protected from unwanted parties. However, there is a stringent need for construction of cryptographic primitives suitable for multimedia security[5].

Permutation and substitution have been identified as the two major constituents for any encryption scheme. But, these operations require changes and improvements in efficiency for their use in multimedia encryption. This is because multimedia content contains high correlation among near-by pixels leading to significant levels of redundancy. Also, multimedia data are found to be much bulkier than the text-based data. Existing solutions for multimedia include the following approaches:

- ***Selective encryption***[6] where part of the whole content is encrypted to achieve cost efficiency.
- ***Chaos***[7,8] based sequences appears as noise to unauthorized users and are strongly dependent on the initial conditions and control parameters. Such sequences are used for generation of key-stream, permutation, S-Box generation etc...

- ***Transform-domain encryption***[9] where the input signal is converted in frequency domain using transforms like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) and operations are then performed on the transform coefficients.

In the light of the above, we note that the two key objectives while designing cryptosystems for multimedia are:

- complete removal of the redundancy in plaintext,
- achieving the first objective in a cost efficient way.

Normally, there exist a trade-off between these two objectives and the proposed work focuses on addressing both these objectives together.

In the Section II we discuss the proposed chaos-based primitive and its application for customizing AES[9] making it suitable for multimedia. Section III reports the experimental observations and analysis. Section IV concludes the work and proposes future scope.

PROPOSAL

The paper proposes construction of new cryptographic primitives based on chaos involving less computational cost which can be used in substitution, diffusion steps while designing cryptosystems for multimedia security. Following we discuss one such primitive.

A. Chaos-based Primitive

The proposed primitive involves very simple and highly inexpensive operations and is thus suitable to be used as primitive for substitution and diffusion steps in cryptosystems for multimedia security. It takes a chaos-based discrete sequence of bytes as input along with the data bytes and generates an equally sized cipher using the operations as described below:

```
for i = 0 to n-1
C[i] = P[i] <<< (cs[i] % 8)
C[0] = C[0] ^ cs[0]
for i = 1 to n-1
C[i] = C[i-1] ^ C[i] ^ (cs[i] % 8)
```

where P[i], cs[i], C[i] represents the ith byte of plaintext, chaotic sequence, and cipher respectively. 'n' denotes the total no. of bytes in plaintext or chaotic sequence. And operators '<<<', '^' correspond to the left circular shift and XOR (Exclusive OR) operations respectively.

B.Customization of AES using Chaos-based Primitive

Advanced Encryption Standard (AES)[3] is a block cipher based on symmetric key encryption. It encrypts a plaintext of 128 bits into an equal-sized cipher taking 128, 196 or 256 bits sized secret key performing 10, 12 or 14 rounds of operation respectively. The input block is treated as a 4x4 state matrix on which several rounds of operations are performed using the round keys obtained by expanding the original secret key. One round of operation comprise of the following four basic operations:

- **Substitute Byte:** This is a simple look-up based substitution operation, where a 16x16 matrix called S. Box is used for substituting bytes of the state matrix. The first 4 bits of the input data byte act as the row index and its last four bits act as the column index for locating the substituting byte in the S-Box.
- ***Shift Rows:*** In this operation the bytes of the *ith* row of the state matrix is circularly left shifted ***i*** no. of times.
- ***Mix Column:*** This operation is used to achieve diffusion by multiplying the state matrix with a fixed matrix. Hence each byte of the output matrix is contributed by all the four bytes present in its column in the input state matrix.
- ***Add Round key:*** This involves simple bitwise XOR operation between the bytes of the state matrix and the corresponding round key bytes.

The AES scheme in its original form is not directly suitable for multimedia because for bulky multimedia the computational cost of the operations involved do not make it practically suitable for multimedia. Hence, we propose customization of AES scheme using the already discussed chaos-based primitive. The experimental results reported in the next section show that the customization improves the cost efficiency and the basic security analysis done demonstrate that the overall strength of the scheme is maintained.

Mix Columns operation has been identified as the most costly operation of all the four operations comprising one round of AES. Therefore, in the customized AES version we propose to replace the Mix Column operation with the proposed chaos-based primitive to reduce the computational cost. Further, to generate the chaotic sequence, logistic map has been used with its control parameter set to 4 i.e.

$$x_{n+1} = 4x_n (1- x_n)$$

Also, the initial condition x_0 (i.e. for n=0) has been made dependent on the secret key. In the original AES scheme the secret key is used only in the Add Round Key operation. By introducing this dependency of the highly sensitive chaotic sequence on the key we have attempted to increase the key space also, as this chaotic sequence significantly contributes in the chaos-based primitive which replaced the Mix Column operation of standard AES scheme in the proposed scheme. This thereby ensures the dependence of two operations per round on the key instead of a single operation as per the original scheme. The following figure (Fig. 1) depicts the block diagram for original and customized AES scheme.

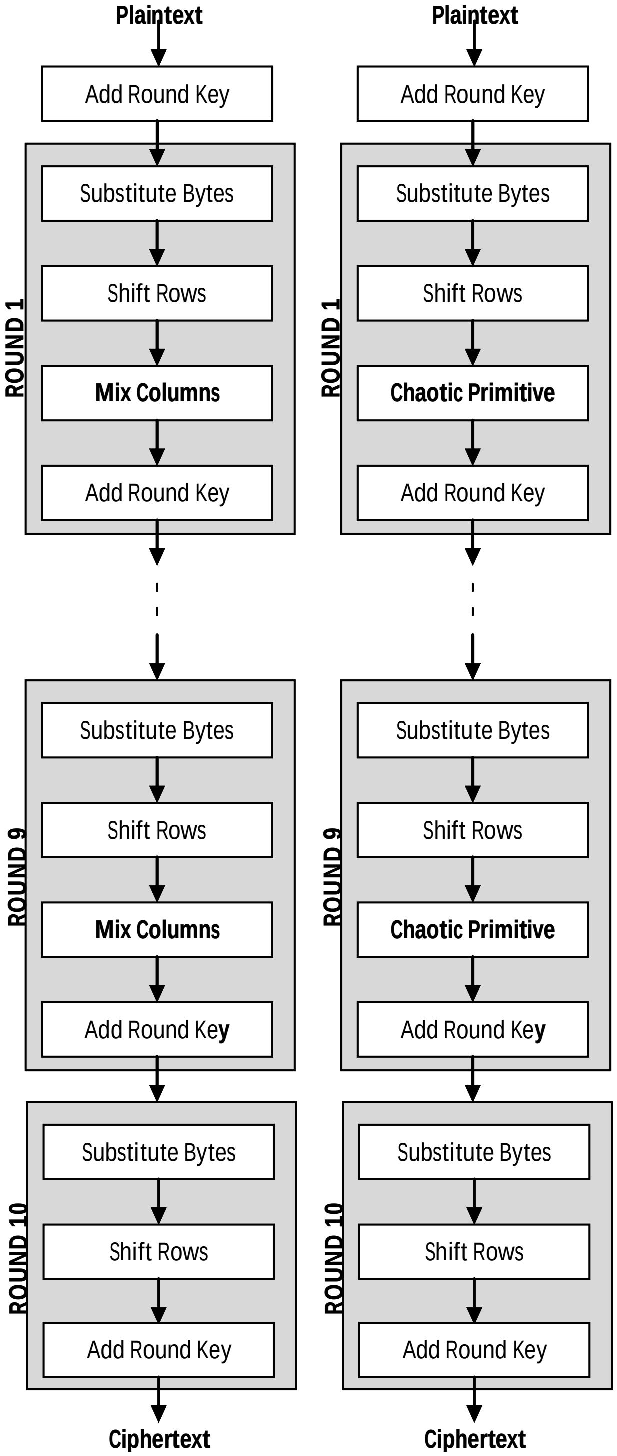
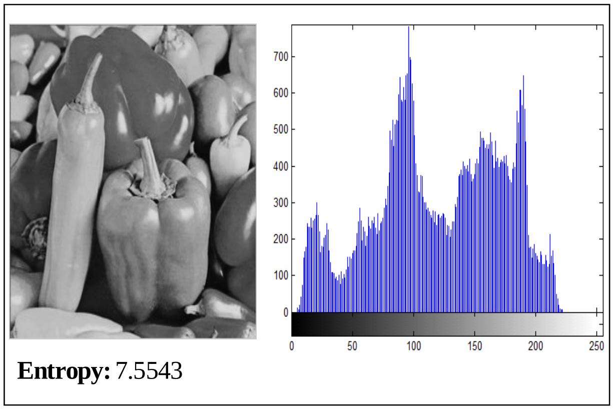


Fig. 1: Block Diagram for Original and Customized AES scheme

OBSERVATIONS, RESULTS AND ANALYSIS

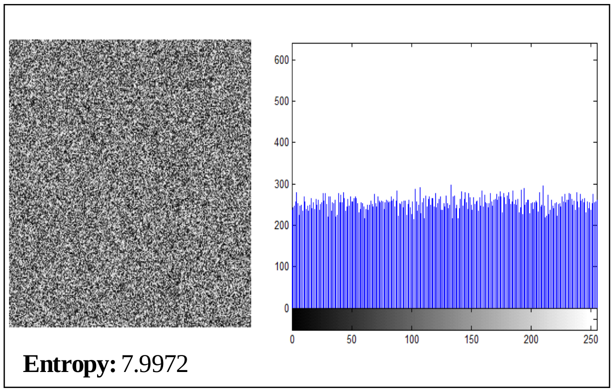
In this section we demonstrate the experimental observations made to display the impact on strength and time efficiency of our proposal of chaotic primitive and its subsequent application to standard encryption scheme like AES. In the Fig. 2, the original Peppers image with its entropy and corresponding histogram is shown. Fig. 3 & Fig. 4 respectively show the encrypted image (with entropy), corresponding histogram and Block-wise entropy variation in the encrypted image obtained using the standard AES scheme.

We observe that our customization maintains the strength of the scheme which is clearly visible from the corresponding encrypted image (with entropy), histogram and Block-wise entropy plot as shown in Fig. 5 and Fig 6. Similar observations have been taken



Entropy: 7.5543

Fig. 2: Original Peppers Image & Histogram



Entropy: 7.9972

Fig. 3: Encrypted Image & Histogram (Standard AES)

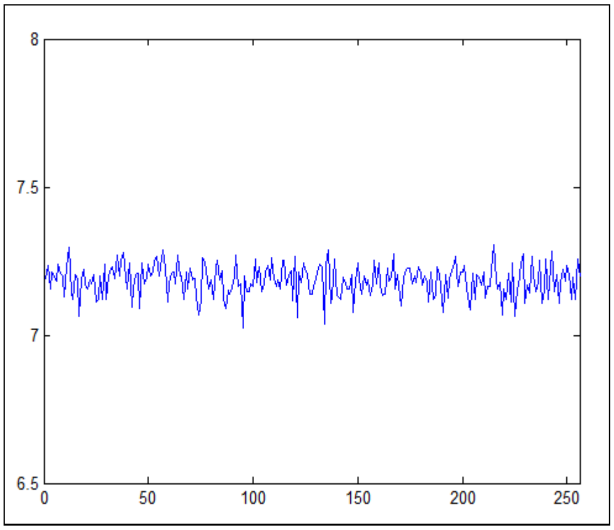
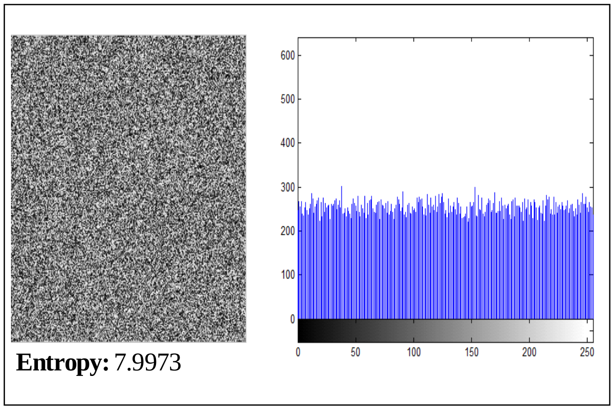


Fig. 4: Block-wise Entropy Variation (Standard AES)



Entropy: 7.9973

Fig. 5: Encrypted Image & Histogram (Customized AES)

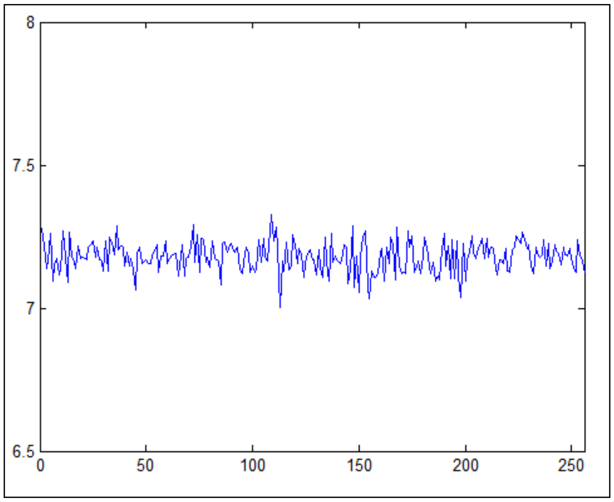


Fig. 6: Block-wise Entropy Variation (Customized AES)

on several standard images which demonstrated consistent results.

Also, the following table (Table 1) show that there is a significant improvement in the computational efficiency. With our proposed customization to AES scheme the cost has reduced to nearly 1/5th of the original cost.

Table 1: Comparision of Computational Cost

Image	AES (seconds)	Customized AES (seconds)
Peppers	95.956	19.344
Water Lilies	96.643	18.938
Baboon	95.956	18.985
Lena	96.237	19.063

CONCLUSIONS & FUTURE WORK

The paper proposed an approach for designing cryptosytems for multimedia security using inexpensive chaotic primitives. A new chaos based primitive suitable for substitution and diffusion has been also proposed and its implementation and experimental observations while customizing existing standard encryption scheme like AES has been shown. The observations clearly reflect that the computational cost has been significantly improved and entropy, histogram and block-wise entropy variation display no degradation in the overall strength of the scheme.

In future, we intend to design more such chaos based primitives and perform thorough security analysis and cryptanalysis to prove their strength.

REFERENCES

[1] B. Furht (ed.), *Encyclopedia of Multimedia*, Springer, 2005.

[2] R.C. Gonzalez and R.E. Woods, *Digital Image Processing, Third Edition*, Prentice Hall, 2007.

[3] W. Stallings, *Cryptography & Network Security Principles and Practices*, Third Edition, Pearson Education, 2004.

[4] A. Menezes (ed.), *Handbook of Applied Cryptography*, CRC-Press, 1996.

[5] S. Lian, D. Kanellopoulos, G. Ruffo, “Recent Advances in Multimedia Information System Security”, *Informatica*, vol. 33, pp. 3–24, 2009

[6] X. Liu, A.M. Eskicioglu, “Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions”. [Online]. Available: http://web.cs.gc.cuny.edu/~xliu/index_files/CIIT2003.pdf

[7] A.N. Pisarchik, M. Zanin, “Chaotic Map Cryptography and Security, Encryption: Methods”, *Encryption: Methods, Software and Security*, Nova Science Publishers, Inc. pp. 1-28, 2010.

[8] A. Pande, J. Zambreno, “The secure wavelet transform”, *J Real-Time Image Proc* DOI 10.1007/s11554-010-0165-6

[9] K. Gupta, S. Silakari, “New Approach for Fast Color Image Encryption Using Chaotic Map”, *Journal of Information Security*, vol. 2, pp. 139-150, 2011.

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, “A Modified AES Based Algorithm for Image Encryption” in *Proceedings of the World Academy of Science, Engineering and Technology*, Vol. 21, May 2007.