E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

An Articulation of Encryption and Authentication Technique for Image Sharing

Aruna Trehan[#*], Parminder Kaur[#], G.N Verma[^] and Manpreet Singh[$]

[#]Electronics and Communication, Punjab Technical University, Jalandhar, India
[^]Applied Sciences, Punjab Technical University, Jalandhar, India
[$]Electronics and Communication, GNA University, Punjab, India

Received 01 May 2017, Accepted 10 July 2017, Available online 15 July 2017, **Vol.7, No.4 (Aug 2017)**

Abstract

In this paper, an articulation of encryption and authentication system for the purpose of information security in multimedia communication system is proposed. This technique is based on approach which merges an encryption algorithm: AES, the block cipher algorithm and proposed authentication technique. This technique provides a dual factor to secure data. This can help in restrict the confidential data of user to restricted persons only. This not only saves time but also reduces overhead of decrypting any falsely acquired data as it is easy to check and verify hash beforehand. Also, comparison of the proposed scheme with others is given in this paper.

Keywords: *Block cipher, encryption, image security, hash function, authentication.*

1. Introduction

Cyber warfare is the advanced form of warfare at present. A multimedia communication system's safety can only be secured if the internal network that connects to all domains of development remains safe and secure. But at the same time, this ease of transmission and sharing of data needs high security issues in terms of [A. J. Menezes *et al*, 1997].

1) Confidentiality- Information is kept secret from all non- authorized parties.
2) Availability- It ensures access to information in the normal scheduled conditions whenever needed by authorized parties.
3) Reliability- It is based on
   s

a) Integrity—The message has not been modified during transmission by non-authorized persons.
b) Authentication—A proof of the information origins and of its attachment to one person. Reliable pieces of information can be used confidently by the sender.

Cryptography is the only means to achieve any information systems, confidentiality of data, data integrity, and Non-repudiation services [C.Paar *et al*, 2009]. If once decrypted or its digital signature deleted or lost, one piece of information is no longer protected and it becomes hard to verify its integrity and its origin. From this outlook, these means of cryptographic, specially encryption, instead seem as an a priori protection mechanisms [D. Bouslimi *et al*, 2012]. Hash functions are very common and important cryptographic primitives. Their primary application is to use congregate with public-key cryptosystems in the digital signature schemes. They are also a hash building block of secret-key Message Authentication (MA). By far one of the most widely accepted hash functions is SHA-1 (Secure Hash Algorithm-1) [FIPS-180-4, 2012]. Depending on the matching between the hash function and the block cipher, it is easy to combine the hash code and the block cipher. The block cipher has only one input which is the key and one output, and a variable-length key block which is the same as hash function.

The rest of the paper is organized as follows. A brief overview of the AES encryption is exposed in section 2. Section 3 describe the proposed articulation of encryption and authentication technique. In section 4 we describe in performance evaluation of the obtained results. Conclusion is discussed in the last section.

2. Cryptographic Primitives

AES (Advanced Encryption Standard) is a symmetric cipher that processes data in 128-bit blocks [FIPS-197, 2001]. It supports key sizes of 128, 192 and 256 bits and maintaining the integrity of the specifications consists of 10, 12 and 14 iterations. Each round mixes the data with a round key, which is generated from the encryption key. The Cipher maintains an internal, 4x4

*Corresponding author's ORCID ID: 0000-0001-7923-1554 matrix of bytes, called state, on which operations are performed. Initially, state is filled with the input data block and XORed with the encryption key. Regular rounds consist of operations called Substitute bytes, Shift rows, Mix Columns, and Add Round key [M.Pitchaiah *et al* 2012].

(1) Substitution Bytes: The Substitution Bytes transformation is a nonlinear substitution operation that works on bytes. Each byte of the input state is replaced using the same substitution function (called S-Box). The S-Box is defined as the multiplicative inverse in the Galois Field GF. The Inverse Substitution Bytes transformation, which is needed for decryption, is the inverse of the affine transformation followed by the same inversion as in the Substitution Bytes transformation.

(2) Shift Rows: The Shift Rows transformation rotates each row of the input state to the left, whereby the offset of the rotation corresponds to the row number. The Inverse Shift Rows of this transformation is computed by performing the corresponding rotations to the right.

(3) Mix Columns: The Mix Columns transformation maps each column of the input state to a new column in the output state. Each input column is considered as a polynomial over GF (2^8) and multiplied with the constant polynomial. The coefficients of a(x) are also elements of GF and are represented by hexadecimal values in this equation. The Inverse Mix Columns transformation is the multiplication of each column.

(4) Add Round Key: The Add Round Key transformation is self inverting. It maps a 128-bit input state to a 128-bit output state by XORing the input state with a 128-bit round key.

3. Proposed Articulate Encryption and Authentication Technique

In the proposed methodology, we have designed an authentication scheme which is embedded right next to AES in the same workflow. User can perform cryptographic operations like encryption and decryption alongside hash generation for verification of visual data.

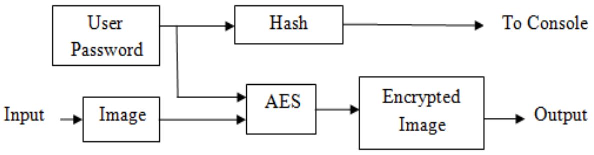

Figure 1: Process of encryption

This not only saves time but also reduces overhead of decrypting any falsely acquired data as it is easy to check and verify hash beforehand.

In our approach we use a robust method that can be able to encrypt any kind of image which of different sizes as well as for black and white image or colored image. The input image is of 128 bits. In this approach there will be a 10 rounds occur for 128 bits. There will be a four blocks in one round. Block diagram of proposed approach is shown in figure 1.

The function of AES is to encrypt the image. The user password is created which is applied to the hash function. It provides authentication to the system. The process of AES block is shown in figure 2.

The plaintext which is in the form of pixels i.e. 128 bits (block) and sub keys of 128 bits long are XORed and then applied to the first round of AES Block and soon. The output of tenth round is 128 bits cipher text. N is a variable. N can be minimum 10.In figure 3, shows the functions performed by rounds in AES block.

By using encryption method i.e. AES symmetric algorithm, information of colored image are encrypted and decrypted as shown in figure below. Table 1 represents the hash functions of colored image which is used for verification.

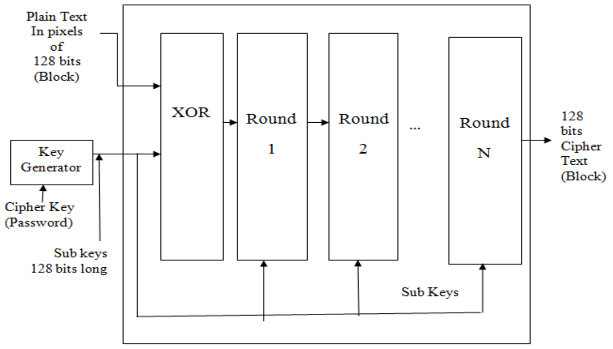

Figure 2: Process of AES Block

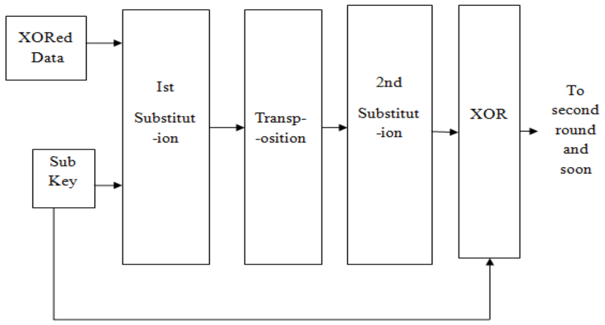

Figure 3: Functions performed by Rounds in AES Block

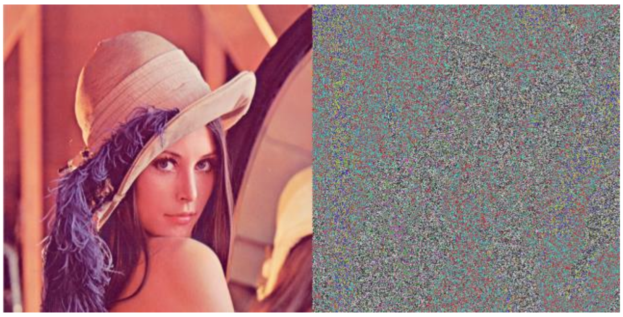

Figure 4: Encryption of Leena

Table 1: Hash Function for Leena

Data Set	Leena
Hash for original image	9bd8d9291ae2154e89960d8fc8da 46313b0f4090
Hash for decrypted image	9bd8d9291ae2154e89960d8fc8da 46313b0f4090
Hash generated for Signature	9bd8d9291ae2154e89960d8fc8da 46313b0f4090
Hash Verification	Hash Matched Successfully. Hence Verified.

4. Result Analysis

In this proposed work, ten images are taken for encryption and authentication scheme. The analyze parameters: Variance, Standard Deviation, Covariance and Correlation Coefficient and also compared the other encryption schemes with our proposed scheme.

Table 2: Performance results of proposed technique on various data sets.

Data Set	Var (β)	SD(σ)	Covar (α,β)	CC
Flowers	0.084	0.2899	0.000079045	0.001
Fruit Basket	0.084	0.2898	0.000032595	0.00031097
Airplane	0.0841	0.29	0.000069906	0.0019
Model	0.0839	0.2896	0.0001315	0.0016
Cameraman	0.0841	0.29	-0.000032218	-0.00045729
Fruits	0.0842	0.2902	0.00018745	0.0033
Hills	0.0837	0.2894	0.00018644	0.002
Leena	0.0839	0.2896	0.000079072	0.001
Gamer	0.0841	0.2899	0.000002087	0.000033251
Baboon	0.0841	0.2899	0.000001099	0.000023428

Correlation coefficient varies per image. The results are shown in figure 5 verifies the fact that if the images contain large area of black or white pixels, the correlation may give false positive. This technique tends to make the correlation coefficient of encrypted image towards zero (0), which means the encrypted image has no similarity with actual image.

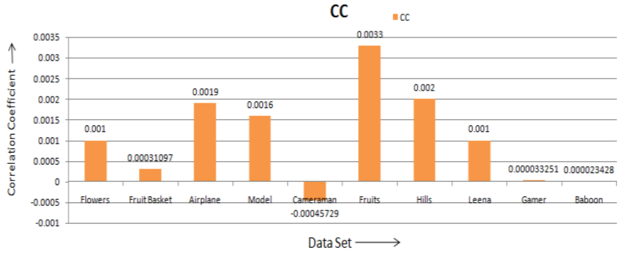

Figure 5: Correlation Coefficient graph of different encrypted images

Table 3: Encryption time comparison among different schemes (time in seconds)

Input File Size(Kb)	DES	TDES	AES	Proposed
114	0.51334	1.10031	0.91387	0.31323
168	0.54042	1.71358	0.96522	0.501236
152	0.53045	1.50382	0.96211	0.44321
65.3	0.46614	1.0172	0.92415	0.48465
136	0.51334	1.10031	0.91387	0.38987
178	0.56167	1.98931	0.96725	0.33568
1.52	0.40242	0.98336	0.82231	0.45798
462	0.61837	2.26394	1.01892	0.35561
96	0.50019	1.08931	0.93631	0.34126

From table 3, it is clear that the most time consuming approach is Triple-DES or TDES, while the least time consuming is by proposed technique. However, DES suffers a lot from security issues. The small key space offers less security. TDES scheme is equivalent to 3 rounds of DES and hence, the key space is undoubtedly large enough to provide better security model than DES. But this security comes with the compromise of encryption time.

Most recent standard AES is more secure and faster in operation than TDES. AES is nearly twice the time faster than TDES but it is slow as compared to DES. The security benefits of AES overcome the large encryption time drawback it possesses. The proposed approach has faster encryption rate than AES, TDES and DES.

Conclusion

In this proposed technique, the design and analysis of AES along with our own proposed signature generation system. This technique has less computational complexity as compared to RSA, sha1sum or even md5. The comparison of the proposed scheme with others had done in this paper. This delivers completely lossless results and provides authentication, which is the main significance of the approach. This also maintains the data size of image on storage. Also it provides data integrity.

References

J. Savard (1976), The ideal cipher: Kerckhoff's design goals for ciphers.1st ed. *McGraw-Hill Publications.*

FIPS-46 (1979), Data Encryption Standard, *National Institute of Standards and Technology.*

A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone (1997),Handbook of Applied Cryptography. 3rd ed. *CRC Press.*

R. L. Rivest (Mar. 1992),The RC4 encryption algorithm, *RSA Security Inc.*

C.Paar and Jan Pelzl (2009). Understanding Cryptography: A Textbook for Students and Practitioners, *Springer*, ISBN 978-3-642-04100-6 .

R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin (Aug. 1998), The RC6 block cipher, *MIT Lab. for Computer Science.*

FIPS-197 (Nov. 2001), Advanced Encryption Standard, *National Institute of Standards and Technology*

O. Goldreich (2004), Foundations of Cryptography: Basic Techniques. 1st ed. *Cambridge University Press*

D.R.Stinson,ChapmanandHall(2005),Cryptography:Theoryan d Practice. 2nd ed. CRC Press.

L. Pérez-Freire, F. Pérez-González, T. Furon, and P. Comesaña (2006) Security of Lattice-Based Data Hiding Against the Known Message Attack, *IEEE Transactions On Information Forensics And Security*, Vol. 1, No. 4, December.

S. Lian, , Z. Liu, Z. Ren, and H. Wang (2007) Commutative Encryption and Watermarking in Video Compression, *IEEE Transactions On Circuits And Systems For Video Technology*, Vol. 17, No. 6.

G. Coatrieux, C. Le Guillou, Jean-M. Cauvin,and C.Roux (2009) ,Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images*, IEEE Transactions On Information Technology In Biomedicine*, Vol. 13, No. 2.

W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, and Ch. Roux (2011), Reversible Watermarking based on Invariant Image Classification and Dynamical Error Histogram Shifting, *33rd Annual International Conference of the IEEE* .

FIPS-180-4 (2012), Secure Hash Standard, *National Institute of Standards and Technology*.

D. Bouslimi*.* G. Coatrieux, M.Cozic and C. Roux (September 2012), A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images*, IEEE Transactions On Information Technology In Biomedicine*, Vol. 16, No. 5.

M.Pitchaiah, Philemon Daniel, Praveen (March-2012), Implementation of Advanced Encryption Standard Algorithm*, International Journal of Scientific & Engineering Research* Volume 3, Issue 3.

R. K. Ibraheem, R. AJ. Kadhim and A. Alkhalid(2015),Anti-Collision Enhancement of a SHA-1 Digest Using AES Encryption By *LABVIEW, IEEE.*

R. Prema (2016), AES Algorithm Based Secure Data Transmission for Wireless Sensor Networks, *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 11, Number 5 pp 3670-3674

M. Mohurle and V. V. Panchbhai Review on Realization of AES Encryption and Decryption with Power and Area Optimization, *1st IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems*

R. Dhagat and P. Joshi (2016), New Approach of User Authentication Using Digital Signature , *Symposium on Colossal Data Analysis and Networking (CDAN)*, *IEEE.*

B. Gadanayak, C. Pradhan, U. Chandra Dey (July 2011), Comparative Study of Different Encryption Techniques on MP3 Compression, *International Journal of Computer Applications* (0975 – 8887) Volume 26– No.3.

G. Gupta (2012), Review on Encryption Ciphers of Cryptography in Network Security, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.2, Issue7.

Y. Mote, P. Nehete, S. Gaikwad (2012), Superior Security Data Encryption Algorithm*, International Journal of Engineering Sciences*, Vol.6.

M. Anand Kumar, Dr. S.Karthikeyan (2012), Investigating the Efficiency of Blowfish and Rjindael (AES) Algorithms, *International Journal Computer Network and Information Security*,vol.2,issue22

G Ramesh, Dr R Umarani (2012),A New Symmetrical Encryption Algorithm with High Security and Data Rate For WLAN andwidth Line, *International Journal of Information Technolog*y, Vol.2, Isssue4.

M. Mathur, A. Kesarwani (2013),Comparison between DES, 3DES, RC2, RC6, Blowfish and Aes*, Proceedings of National Conference on New Horizons in IT.*

R.Rayarikar, S. Upadhyay, P. Pimpale (2012),SMS Encryption Using AES Algorithm on Android , *International Journal of Advanced Computer Applications*, Vol.50, No.19.

G. Ramesh, Dr.R Umarani (2012), A Survey on Various Most Common Encryption Technique*, International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.2, No.2.

A.D.Suarjaya (2012),A New Algorithm for Data Compression Optimisation*, International Journal of Advanced Computer Science and Applications*, Vol.3, No.8.

H. Lee, K. Lee, Y. Shin (2009),AES Implementation and Performance Evaluation on 8-bit Microcontrollers, *International Journal of Computer Science and Information Security*, Vol. 6 No. 1.

Z. Su, G. Zhang and J. Jiang (2012),Multimedia Security: A Survey of Chaos-Based Encryption Technology, *School of Computer and Information, Hefei University of Technology China*, No.5.

S.Sharma, L. Kumar,H. Sharma (2013) Encryption of an Audio File on Lower Frequency Band for Secure Communication, *International Journal of Advanced Research in Computer Science and Software Engineering*,Vol.3,Issue7.