Modified MASK Algorithm for Image Encryption

Heera G. Wali\textsuperscript{a}, Nalini C. Iyer\textsuperscript{b}

\textsuperscript{a}Department of Electronics and Communication, B.V.B College of Engineering & Technology, Hubli-580 031, INDIA
\textsuperscript{b}Department of Electronics and Communication, B.V.B College of Engineering & Technology, Hubli-580 031, INDIA

Abstract

AES, a symmetric block cipher, is suitable for high-speed applications. The throughput as one of the bottlenecks for huge data sizes, such as images. Another symmetric block cipher, MASK, a matrix-based encryption technique, is also suitable for high-speed applications with a speed eight times that of AES. The proposed work discusses about AES and MASK algorithm and compares in terms of encryption speed, diffusion, confusion, and statistical attacks. Based on the analysis, a Modified MASK algorithm is designed to overcome the security weaknesses in the MASK algorithm. A hardware implementation of Modified MASK algorithm is done and validated.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the organizing committee of the ICISP2015

Keywords: Encryption; W7 stream cipher; cipher text; AES.

1. INTRODUCTION

With the fast evolution of digital data exchange, security of information becomes much more important in data storage and transmission. Due to the increasing use of images in various fields like military, medical, forensic, and satellite images, it is essential to protect the confidentiality of the images. An encryption algorithm has to be efficient enough to encrypt images, such that the encrypted image is not prone to any kind of attacks and has good encryption speed.

Although AES (Advanced Encryption Standard)\textsuperscript{1} by NIST is a symmetric block cipher, finds suitability in many applications, but has limitations in speed and area. The bottleneck being speed because of the iterative complex operations involved when the data is of huge size such as large image.

* Corresponding author. Tel.: +918904842764.
E-mail address: heerawali@bvb.edu
AES also suffers from textured zones for images having low entropy areas or zones. The MASK (Matrix Array Symmetric Key)\(^2\) algorithm is also a block cipher and encrypts images eight times faster than the AES (Advanced Encryption Standard)\(^1\). Its matrix-based encryption technique finds suitability for high-speed applications. The MASK algorithm has been analyzed for statistical attacks for images having low entropy regions.

The contribution for the proposal work is outlined below: The MASK algorithm uses a matrix-based encryption method, for achieving high speed. Although the MASK algorithm is efficient in terms of encryption speed, for images having low entropy regions, it’s prone to statistical attacks. This is the main security weakness of the MASK algorithm. We have extended the MASK algorithm to support the W7 stream cipher algorithm to overcome the security weakness. The rest of the paper deals with, Section 2 Overview of AES Algorithm, MASK algorithm in Section 3. Section 4 Analysis and discussions. Modified MASK algorithm in Section 5, Section 6 Results and Conclusion.

2. OVERVIEW OF AES ALGORITHM

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. Also accorded as a standard by NIST in October 2002. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, as shown in Figure 1 AES merely allows a 128-bit data length that can be divided into four basic operation blocks. These blocks operate on an array of bytes and organized as a 4x4 matrix that is called the state. The number of standard rounds depends on the data block and key length. If the maximum length of the data block or key is 128, 192, or 256, then the number of rounds is 10, 12 or 14, respectively. Each standard round includes four fundamental algebraic function transformations on arrays of bytes. These transformations are: Substitute Byte, Shift Row, MixColumn, and AddRoundKey addition. The final round of the algorithm is similar to the standard round, except that it does not have MixColumn operation. Substitute Byte is a non-linear transformation that operates independently on each byte of the state using a substitution table (called S-box). Decryption is performed by the application of the inverse transformations in the round functions.

![Figure 1. AES algorithm block diagram](attachment:image.png)
3. OVERVIEW OF MASK ALGORITHM

The encryption, $C = E_k(P)$, using the MASK (Matrix Array Symmetric Key) encryption algorithm consists of three Modules. It’s a block cipher with key size of 128 bits and block size of 128 bits. Figure 2 shows the block diagram of encryption process of the MASK algorithm. Algorithm comprises of:

3.1. Initialization Module

A 16x256 initialization matrix is constructed using the secret key. This is further used to generate key subsets in the key scheduler module. The first column in $i^{th}$ row of matrix is the $i^{th}$ character of the secret key and then the subsequent elements of the $i^{th}$ row are filled one increment of the previous value until the last column element i.e. the 256th column.

3.2. Key scheduler Module

Sub-keys sets $K_{s1}$ and $K_{s2}$ are generated using the initialization matrix. These keys are used in the substitution and diffusion rounds. Using complex procedure to derive the elements of $K_{s1}$ and $K_{s2}$ from the base initialization matrix.

- With one bit change in the secret key the element of $K_{s1}$ can have up to eight count change.
- Elements of $K_{s2}$ are derived on the values of the columns of $K_{s1}$ and can have up to eight counts change for one bit change in the secret key.
- Both $K_{s1}$ and $K_{s2}$ are 16x16 matrices.

3.3 Substitution and Diffusion Module

- It has up to sixteen rounds of iterations.
- The plaintext is of 128 bits, is given as input to the module. Where each plaintext byte is substituted from the base initialization matrix.
- This acts as the typical block cipher where a block of 128 bits are encrypted together using sub key sets $K_{s1}$ and $K_{s2}$ generated in key scheduler Module.
- The iteration rounds consist of data based XOR, key based XOR and Transpose operations.

![Figure 2. MASK algorithm block diagram](image-url)
4. ANALYSIS AND DISCUSSIONS

The MASK algorithm has been tested with different images of various sizes and the results are compared with AES (Advanced Encryption Standard)\(^1\). 

Comparison of MASK and AES

1. Encryption time: The MASK algorithm\(^2\) encrypts images eight times faster than AES (Advanced Encryption Standard)\(^1\). Table 1 gives the encryption time comparison of AES and MASK for different image sizes for ten cipher rounds.

2. Confusion: For a single bit change in the secret key MASK provides more number of bit changes in the sub keys than the AES. Table 2 gives a comparison between AES and MASK for the total number of bit changes in the sub keys. MASK algorithm is more efficient in generating sub keys for bit changes in the secret key than AES.

3. Diffusion: It’s a measure of dissipation of plaintext in ciphertext. Comparison between AES and MASK is shown in Table 3. The total number of bits changed in the ciphertext caused by one bit change in the plaintext of AES is comparable with MASK algorithm. Therefore diffusion property of MASK and AES is more or less the same.

4. Statistical attacks: In cryptography, statistical attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertext. The attack is completely successful if the corresponding plaintexts can be deduced. Since the cipher key set encrypting these highly correlated regions remain the same, therefore grey or white texture zones are seen in the cipher image even when the entropy of the cipher image is nearing to maximal as seen in Figure 3. It’s the security weakness in MASK algorithm. This is also seen with AES as seen in Figure 4.

### Table 1. Encryption speed

| Image  | AES 128 x 128 | MASK 128 x 128 | AES 256 x 256 | MASK 256 x 256 |
|--------|---------------|----------------|---------------|----------------|
| Lena   | 1158.6        | 140.6          | 1109.7        | 149.7          |
| Peppers| 1071.4        | 145.7          | 1106.2        | 149.8          |
| Baboon | 1125.8        | 143.7          | 1175.5        | 142.5          |
| Barche | 1091.6        | 148.3          | 1063.8        | 142.4          |

### Table 2. Confusion property

| Key | 4C,69,66,65,27,73,20,62,65,61,75,74,69,66,75,6C |
| Key2 | 4C,69,67,65,27,73,20,62,65,61,75,74,69,66,75,6C |

| Total number of bit changes in sub keys |
|----------------------------------------|
| Cipher rounds | 1st | 2nd | 3rd | 4th | 5th | 6th | 7th | 8th | 9th | 10th |
| AES | 4   | 26  | 34  | 35  | 38  | 31  | 33  | 42  | 31  | 28   |
| MASK | 54  | 60  | 54  | 61  | 57  | 56  | 51  | 56  | 50  | 48   |

### Table 3. Diffusion property

| Plaintext 1 | C6,09,2C,1F,F5,15,70,44,99,0F,25,2A,BF,FC,19,F4 |
| Plaintext 2 | C6,09,2C,1F,F5,15,70,44,99,0F,25,29,BF,FC,19,F4 |

| Number of bit change in each byte of the cipher text |
|-----------------------------------------|
| AES | 7, 3, 1, 3, 2, 3, 5, 4, 5, 4, 5, 6, 6, 2, 6, 3 |
| MASK | 4, 4, 5, 5, 2, 6, 1, 3, 3, 4, 6, 3, 5, 3, 4, 4 |
Figure 3. Image and Cipher Image using MASK with histogram

Figure 4. Image and Cipher Image using AES with histogram
5. MODIFIED MASK ALGORITHM

To improve the security weakness in MASK algorithm against the statistical attacks, a W7 key stream generator is added to MASK algorithm for image encryption as seen in Figure 3. The W7 algorithm is a byte-wide, synchronous stream cipher optimized for efficient hardware implementation at very high data rates. It is a symmetric key algorithm supporting key lengths of 128 bits. W7 cipher contains eight similar models [C1-C8]. Each model consists of three LFSR’s and one majority function. W7 architecture is composed by a control unit and a function unit. Each cell has two inputs and one output. The one input is the key and it is the same for all the cells. The other input consists of control signals. Finally, the output is of 1-bit long. The outputs of each cell form the key stream byte.

6. RESULTS & CONCLUSION

MASK image encryption algorithm is tested and evaluated based on software and hardware simulation. The results are obtained from a Xilinx Virtex5 xc5vlx50t FPGA. Comparison of algorithms on Device xc5vlx50t is
shown in Table 4. Different test images have been used “lena,” “peppers,” “baboon,” “barche” (greyscale format). The modified MASK algorithm, for each round of encryption of the plaintext a different set of sub keys are generated Therefore even for contiguous same plaintext data will not be ciphered to the same value. This eliminates the statistical attacks on the cipher text. As seen in Figure 6.

MASK algorithm is extended to support key stream generator. The modified MASK algorithm, a highly secure symmetric matrix based image encryption technique, has been implemented. It is realized in both hardware and software. The key stream generator has an important influence on the encryption performance.

Table 4. Comparison of algorithm on Virtex5 FPGA

| Algorithm     | No of Slices | % of Slices utilized |
|---------------|--------------|----------------------|
|               | Used         | Available            |
| MASK          | 3,792        | 28,800               | 13%                  |
| W7            | 337          | 28,800               | 1%                   |
| MASK+W7       | 4,341        | 28,800               | 15%                  |

References

1. Federal Information Processing Standards Publications (FIPS 197), 2001, Advanced Encryption Standard (AES).
2. Paul A.J. P. Mythili, K. Paulose Jacob. Matrix based Cryptographic Procedure for Efficient Image Encryption. Recent Advances in Intelligent Computational systems (RAICS) IEEE, pp.173–177; 2011.
3. Krishnamoorthy G.N, V. Ramaswamy. Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version using Digital Images. International Journal of Network Security & its Application,1(1), pp. 28-33; 2009.
4. X. Zhang and K. K. Parhi. Implementation Approaches for the Advanced Encryption Standard Algorithm. IEEE Circuits and Systems Magazine, Fourth Quarter, 4(70), (4), 2, pp.24-46; 2002.
5. William Stallings, Network Security Essentials (Applications and Standards) Pearson Education, pp. 2- 80; 2004.
6. J.J. Amador, R. W. Green. Symmetric-Key Block Cipher for Image and Text Cryptography” International Journal of Imaging Systems and Technology, ( 3) ;2005, pp.178-188.
7. M.D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C.E. Goutis. Comparison of the hardware architectures and FPGA implementations of stream ciphers. in Proceedings of 11th IEEE International Conference on Electronics, Circuits and Systems (ICECS’04); 2004.
8. Nalini C. Iyer, M.C Aralimarad . Image Encryption Using AES with Chaotic series for key generation” International Conference on Electronic Design and Signal Processing(ICEDSP), MIT, Manipal; 2009.
9. V.D.Kulkarni, Nalini Iyer,P.V Anandmohan, D.V Poornaiah, Optimized S-Box Design for AES Core, Journal of Information Systems,(2),pp 76-83;2008.