Image Encryption and Decryption Using VHDL
Kushal Patel Sneha Shah
1P.G Student Department of Electronics & Communication,  
2Assistant Professor, Department of Electronics & Communication, L.J. Institute of Engineering and Technology Ahmedabad, Gujarat, India.

Abstract—Presently on a daily basis sharing the information in image form over web is becoming a significant issue due to security problems. Thus lots of techniques are needed to protect the shared information in academic unsecured channel. The present work target cryptography to secure the image data whereas causing inside the network. Encryption has come up as a solution, and plays a very necessary role in image data security. This security mechanism uses MAES algorithm to scramble information into unclear text which can be exclusively being decrypted by party those possesses the associated key.  

Keywords: - cryptography, AES, MAES

I. INTRODUCTION
Cryptography is an efficient method for shielding sensitive info .it is a technique for storing and sending knowledge in kind that solely those it’s process for browse and process. For secure communication over public network knowledge may be protected by the method of encryption. Encryption converts that knowledge by any encryption algorithmic program using the ‘key’ in scrambled type. Solely user having access to the key will decipher the encrypted knowledge. Encryption may be an elementary tool for the protection of sensitive information. The aim to use encryption is privacy in communications. Here we tend to see the straightforward method of encryption & decryption.

II. ADVANCED ENCRYPTION STANDARD (AES)
Advanced Encryption Standard (AES) is published 1999 by Independent Dutch cryptographers. Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard re commenced by NIST to replace DES. The Advanced encryption standard (AES) algorithmic rule is capable of using crypto graphical keys of 128, 192, and 256 bits to inscribe and rewrite information in blocks of 128 bits. As the AES algorithm may be used with three different key lengths, these three different “flavors” are generally referred to as “AES=>128”, “AES=>192”, and “AES=>256”. AES uses several rounds in which each round is made of several stages. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. To provide security AES uses kinds of transformation. Substitution permutation, combination and key every round of AES except the last uses the four transformations.

Fig. 2: Process of AES

[Fig. 1: Encryption & Decryption Process

[B. Padmavathi, S. Ranjitha Kumari “A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique” , International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064]

Sub Bytes: This operation may be an easy substitution that converts each byte into a unique value. Shift Rows: every row is turned to the correct by a particular range of bytes

Mix Columns: Each column of the state array is processed singly to provide a brand new column. The new column replaces the previous one.

XorRoundKey: Adds the round key to the state using a bit-wise XOR operation. Following process used to encrypt a 128-bit block:
1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data.
III. MODIFY ADVANCED ENCRYPTION STANDARD (MAES)

We will modify the AES to be additional efficient and secure approach by adjusting the Shift-Row Transformation. Instead of the initial Shift-row, we have a tendency to modify it as:

Examine the value within the initial row and initial column, $(state[0][0])$ is even or odd?

If it’s odd, The Shift-Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by a particular offset. For MAES, the primary and third rows are unchanged and every computer memory unit of the second row is shifted one to the left. Similarly, the fourth row is shifted by three to the left.

If it is even, The Shift-Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by an exact offset. The initial and fourth rows area unit unchanged and every computer memory unit of the second row is shifted three to the right. Similarly, the third row is shifted by tow respectively on to the right.

**Fig. 3:** Shift-Row Transformation for Odd Rows


If it is even, The Shift-Rows step operates on the rows of the state; it cyclically shifts the bytes in every row by an exact offset. The initial and fourth rows area unit unchanged and every computer memory unit of the second row is shifted three to the right. Similarly, the third row is shifted by tow respectively on to the right.

**Fig. 4:** Shift-Row Transformation for Even Rows


IV. IMAGES OF DIFFERENT SIZE

(512X512)

Size on Disk: 84kb

**V. COMPARATIVE ANALYSIS OF DIFFERENT PARAMETERS**

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Image Size</th>
<th>Size On Disk</th>
<th>Data In</th>
<th>Algo.</th>
<th>Timing (us)</th>
<th>Memory (kb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>512X512</td>
<td>84kb</td>
<td>32 bit</td>
<td>AES</td>
<td>6112</td>
<td>140956</td>
</tr>
<tr>
<td>2</td>
<td>1024X1024</td>
<td>160kb</td>
<td>32 bit</td>
<td>MAES</td>
<td>3591</td>
<td>366520</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AES</td>
<td>4221</td>
<td>530660</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MAES</td>
<td>4220</td>
<td>562920</td>
</tr>
</tbody>
</table>
VI. CONCLUSION

In Image Data communication, encryption algorithm plays an important role. My thesis work surveyed the existing encryption techniques like AES, DES and MAES algorithms. Based on my thesis work, it was concluded that MAES algorithm consumes least encryption and decryption time. I also observed that decryption of MAES algorithm is better than other algorithms. Again from the reviewed stuff, I evaluated that MAES algorithm is much better than DES, AES algorithm.

REFERENCES


[18] Yong Zhang, “Encryption Speed Improvement on an Improvement over an Image Encryption Method Based on Total Shuffling”, 978-1-4673-6453-9/13/$31.00 ©2013 IEEE.
