Secure the Secret Data’s by Double Encryption using Image Processing and VLSI Technology

R.Vinoth, M.Balaji, S.Shobana, D.Vinoth, R.Nivethitha

Abstract— Transmission of confidential data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity and non reproduction of exchanged information. This project combines the steganography and cryptography to protect the information. Least significant method is used to hide the information. The symmetric key algorithm of AES used to encrypt the image. The encrypted image has been implemented in FPGA.

Index Terms— AES algorithm, FPGA, LSB

I. INTRODUCTION

This project has a combination of steganography and cryptography. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words “steganography means hiding one piece of data within another”. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphē meaning "writing". A cryptographic algorithm has three classifications: symmetric, asymmetric and cryptographic hash function. Data encryption standard (DES) is a widely-used method of data encryption. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. DES applies a 56-bit key to each 64-bit block of data. The process can run in several modes and involves 16 rounds or operations.

Advanced encryption standard (AES) is a symmetric 128-bit block data encryption technique. The terms AES and Rijndael are used interchangeably; there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

II. PROPOSED METHOD

In the proposed method the combination of Image Steganography and cryptography has been achieved by using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES is used to encrypt and decrypt the stego image. To protect the confidential information from the unauthorized users the encrypted stego image has been implemented in FPGA. In this work a prototype has developed for providing security to confidential information’s. The following figure shows the operation of proposed method:

Figure:1 Block diagram of proposed method

A. AES Algorithm for Images

The AES algorithm is a symmetric key block cipher with a block length of 128 bits and a support for key lengths of 128,192 and 256 bits. AES algorithms is a symmetric key algorithm which means the same key is used for both encryption and decryption. Cipher text produced by the AES algorithm is same size as the plain text

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Number of rounds(Nr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-128</td>
<td>10</td>
</tr>
<tr>
<td>AES-192</td>
<td>12</td>
</tr>
<tr>
<td>AES-256</td>
<td>14</td>
</tr>
</tbody>
</table>

Table:1 AES keys and number of rounds
Secure the Secret Data’s by Double Encryption using Image Processing and VLSI Technology

c. Key Expansion
The AES key expansion algorithm takes as input a 4-word (16-byte) key and gives a linear array of words, providing a 4-word round key for the initial Add round key stage and each of the 10 rounds of the cipher. It involves copying the key first in to the group of 4 words, and then constructing subsequent groups of 4 based on the values of the previous 4th words. The first word in each group of 4 gets “special treatment” with rotate + S-box + XOR constant on the previous word before XOR’ing the one from 4 back.

d. Shift rows Transformation
The first row of State array is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed. The operation of shift row is shown in figure 5:

```
<table>
<thead>
<tr>
<th>S</th>
<th>S'</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0(0)$</td>
<td>$S(0)_0$</td>
</tr>
<tr>
<td>$S(1)_0$</td>
<td>$S(1)_1$</td>
</tr>
<tr>
<td>$S(2)_0$</td>
<td>$S(2)_1$</td>
</tr>
<tr>
<td>$S(3)_0$</td>
<td>$S(3)_1$</td>
</tr>
</tbody>
</table>
```

Figure: 5 Shift row operations

e. Mix columns Transformations
It operates on every column independently. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The substitution makes use of arithmetic over GF (28). It is designed as a matrix multiplication where each byte is treated as a polynomial in GF (28). The inverse used for decryption involves a different set of constants. This gives good mixing of the bytes within each column. Combined with the “shift rows” step provides good avalanche, that reflect within a few rounds, all output bits depend on all input bits. Figure 3.5 shows the operation mix column transformation

```
<table>
<thead>
<tr>
<th>S</th>
<th>S'</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S(0)_0$</td>
<td>$S(0)_1$</td>
</tr>
<tr>
<td>$S(1)_0$</td>
<td>$S(1)_1$</td>
</tr>
<tr>
<td>$S(2)_0$</td>
<td>$S(2)_1$</td>
</tr>
<tr>
<td>$S(3)_0$</td>
<td>$S(3)_1$</td>
</tr>
</tbody>
</table>
```

Figure: 6 Mix columns Operation
III. RESULT
For using 128 bit in AES algorithm has 10 rounds. Each round using the four transformations and the final round does not use the mix column operation. The following figure shows the final output of the encrypted image.

Input keys:
0000000000000000000000001000000001000000010000000101000000010100000001
000010000000110000001100000010010000001010000001011

Figure: 7 Output of encrypted image

CONCLUSION
In this project, we proposed the combination of image steganography and cryptography has been achieved using the LSB technique and AES algorithm. LSB technique is used to hide the secret data into an image and AES is used to encrypt the stego image. Here the double encryption is used to encrypt the confidential information. The encrypted image has been implemented in FPGA. This method provides the most security for confidential information.

REFERENCES

R. Vinod was born in Tamilnadu, India in 1985. He received his Bachelors Degree, B.E- ECE from Mohamed Sathak Engg College, Keelakari, Ramanathapuram, India, under the Anna University, Chennai, in the year 2007 and Masters Degree, M.E- VLSI Design from Muthayammal Engg College, Raspuram, India under the Anna University of Technology, Coimbatore, in the year 2009 and Master of Human Resources Management from Periyar University, Salem in the year 2012. Currently he is pursuing Doctor of Philosophy, (Ph.D) in the area of VLSI Image Processing Under the Anna University, Chennai. His Area of Interest includes Image Processing, Signal Processing, VLSI design, etc. He is having more than 5 years of teaching experience in the Anna University Affiliated Engg Colleges. He published more than 10 research papers in International Journals and presented more than 10 papers in International and National Conferences. He is a Life Member of ISTE.

M. Balaji was born in Tamilnadu, India in 1988. He received his Bachelors Degree, B.E- ECE from M.P.Nachimuthu M.Jaganathan Engineering College, Erode India, under the Anna University, Chennai, in the year 2010 and Masters Degree, M.E- Embedded Systems from Sathyabama University, Chennai, in the year 2013. His Area of Interest includes Microprocessor, Image Processing, etc. He published more than 5 research papers in International Journals and presented more than 5 papers in International and National Conferences. He is a Life Member of ISTE.