Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES)
ISSN: 2566-932X, Vol. 1, Issue 2, May 2017.

A Review of AES and Visual Cryptographic techniques for added security

Nandini C S[1], Dr. K R Rekha[2]

[1.] MTech Digital Electronics, Department of ECE, College of SJBIT, nandinigowda1234@gmail.com

[2.] Professor, Department of ECE, College of SJBIT, rekha.sjbit@gmail.com

Abstract: With the increase in data theft, eavesdropping and hacking, a requisite for powerful data protection schemes arises. Many algorithms have been proposed in the past to enhance the speed and the security parameters of the cryptographic algorithms. The well-known algorithms that are currently in use are Advanced Encryption Standard (AES) for data and visual cryptography (VC) for the images. The scope of the project is to develop a highly secure encryption algorithm, by combining the AES and VC algorithms. The algorithms will be simulated in MATLAB and also, the architecture developed for the same will be downloaded on the Spartan 3E FPGA.

Keywords: Cryptography; AES; Simulation; image; Secret Sharing; Visual Cryptography

I. INTRODUCTION

Cryptography is the branch of science, which deals with encryption techniques. It helps for creating written or generated codes that allows information to be kept secret. Cryptography is the study of hiding information and it is used when communicating over an untrusted medium such as internet, where information needs to be protected from the third or unknown parties. In cryptography, the encryption algorithm can be used in two different methods i.e., substitution and transposition. Substitution means, where each element of input text like bit, letter, and group of letters or bits is mapped into another element and transposition means rearranging the elements of input text. In this way there will be no loss of information. Cryptography uses two different numbers of keys i.e. symmetric key and asymmetric key. Symmetric key means both the transmitter side and reception side use the same key and asymmetric key means it use different keys on both sides [1]. The modern popular methods of cryptography are DES (Data encryption standard), 3-DES (Triple-DES), AES (Advanced encryption standard) and VCS (Visual cryptography standard).

DES uses symmetric key and it can excrypt 64-bit text size with 56-bit key. It takes a 64-bit input text in block and also outputs a 64-bit text. Then the DES always works on same equal size of input text in block and it also uses the two encryption methods based on substitution and permutation. The main algorithm of DES is repeated 16 times to obtain the output text. Hence it is very difficult and no more invulnerable [2]. Triple-DES, as the name implies, performs triple times DES with using different keys for improving security of DES. Hence it is very simple, more secure but is too much slower [2]. AES, it is the improved version of DES and it also uses symmetric key encryption method. Then AES uses different numbers of keys size like 128,192 and 256, it operation slightly differs from the different keys size. Hence it is more efficient, as increasing the key size not only offers more number of bits, but also increases their complexity of this standard. Hence it is more secure and protects the secret information [2]. Visual cryptography is one of the newest techniques which provides the security and protect information. This can be used only on images. If the image needs to be encrypted, it has to be divided into N separate equal-sized shares and then transmitted through different channels. If anywhere unauthorized person will receive one image it is impossible to get the original image. For decrypting, the shares has to be overlapped to visually interpret the data.

II. AES IMPLEMENTATION

Advanced encryption standard was introduced by National Institute of Standard and Technology in 2001. AES was successor of (DES) data encryption standard, as DES did not provide long term security because of shorter key length of 56 bits. In this cryptographic technique, we use symmetric key form of 128 bits. It involves 4 steps to complete one round of simple AES operation [3]. They are:

1. Add round key
2. Substitute bytes
3. Shift rows
4. Mix-Columns

Add round key- Its doing bitwise XOR operation between the 128 bit input text and 128 bit key. Here both input and key are of 4x4 matrix bytes (16 bytes x 8 bits = 128 bits). Operation of add round key is shown in below figure 1[1][3].

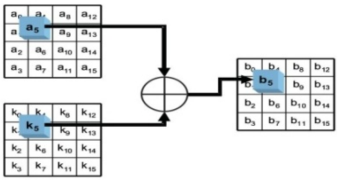


Fig 1. General add round key operation

In this process, the input data is represented by matrix-a, key input represented by the matrix-k and the XOR operation performed between two matrix-a and the matrix-k is the resultant matrix-b, which is output of this operation stage.

Substitute bytes- Non-linear operation performed by sub-bytes. This is the main goal for the safety in encryption. Each byte of input text is operated in a simple form of substitution from S-box. With the help of LUT, states with 16 bytes (input data) are replaced by parallel value found in table [1][3].

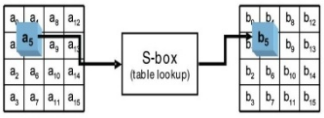
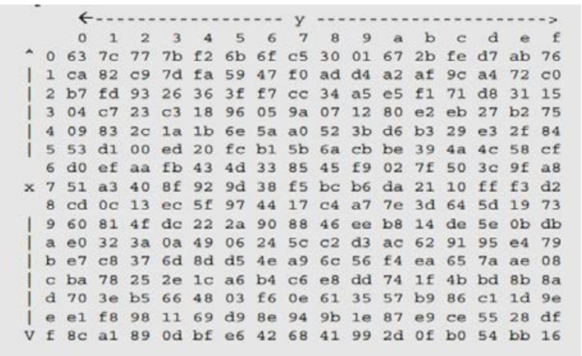


Fig 2. General sub byte operation block diagram



```
          <--------------------- y ---------------------------->
        0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
  ^  0 63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
  |  1 ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
  |  2 b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
  |  3 04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
  |  4 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
  |  5 53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
     6 d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
  x  7 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
     8 cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
  |  9 60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
  |  a e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
  |  b e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
  |  c ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
  |  d 70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
  |  e e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
  V  f 8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
```

Fig 3. S-box representation

In case of Shift rows, the result of s-box matrix is shifted to left circularly. First row of input remains unchanged, second row of input is shifted to left by 1-byte, third row by 2-bytes finally fourth row by 3-bytes as shown in figure 4 [1][3].

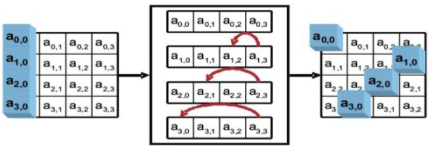


Fig 4. Shift row operation

Mix-Column – Here the matrix resulted from shift rows is multiplied with the key “2 3 1 1” using Galois Field Multiplication.

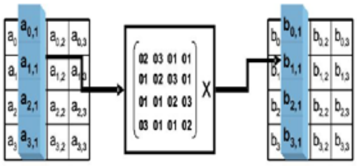


Fig 5. Mix-column operation

Single column transition can be expressed as given below.

$$b0,\ j=(2\bullet a0,\ j)\oplus(3\bullet a1,\ j)\oplus a2,\ j\oplus a3,\ j$$
$$b1,\ j=a0,\ j\oplus(2\bullet s1,\ j)\oplus(3\bullet a2,\ j)\oplus a3,\ j$$
$$b2,\ j=a0,\ j\oplus a1,\ j\oplus(2\bullet a2,\ j)\oplus(3\bullet a3,\ j)$$
$$b3,\ j=(3\bullet a0,\ j)\oplus a1,\ j\oplus a2,\ j\oplus(2\bullet a3,\ j)$$

Fig 6. Galois field Multiplication

III. VISUAL CRYPTOGRAPHY

Shamir & Naor introduced the concept of visual cryptography, that works only on the encoded text to be encrypted as a images or graphics [5].

Later, Naor & Pinkas, proposed a how to use visual cryptography for the identification of a person without believing the underlying system [6].

IV. CONCLUSION

Out of these, AES is proved to be the best method while working on data such as text & Visual Cryptography is the most advanced method for encrypting images. It can be seen now a days that AES can also be hacked by the hackers to get sensitive data. Using only AES is prone to hacking. Visual Cryptography is best suited for images only.

V. FUTURE SCOPE

When the person wants to access the confidential data online, the person enters the details like username, password, credit card number. Etc but this data can be hacked by the attackers using phishing techniques [7].

Thus, for added security, a combination of AES and visual cryptography can be performed that allows establishing a secure channel between two known persons and can be used for secure communication or interaction.

REFERENCES

[1] William stallings“Advanced encryption standard” in cryptography and network security principles and practice, sixth edition,dorling Kindersley(india) pvt.Ltd,licensees of pearson education in south asia

[2] Jai Singh, KanakLata and Javed Ashraf, “Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB”, International Journal of Current Engineering and Technology

[3] Quist-aphetistkester, Laurent nana and Anca Christine pascu, “a novel cryptography encryption techniqus for securing digital images in the cloud using AES and RGB pixel displacement”,IEEE 2013

[4] Praveen kumar. P and sabitha.S “user authentication using visual cryptography”,IEEE, 2015

[5] NaorS94] Moni Naor and Adi Shamir. Visual Cryptography, EUROCRYPT ’94,Volume 950 of Lecture Notes in Computer Science, pp. 112. Springer-Verlag, 1995.

[6] Moni Naor and Benny Pinkas. Visual authentication and Identication. In Lecture Notes in Computer Science, Springer-Verlag, 1997, pp. 322-336

[7] Divya James, Mintu Philip, A Novel Anti Phishing framework based on Visual cryptography in International Journal of Distributed and Parallel Systems Vol.3, No.1, January 2012, pp. 207-218