Image Encryption and Decryption Using VHDL

Kushal Patel Sneha Shah
[1]P.G Student Department of Electronics & Communication,
[2]Assistant Professor, Department of Electronics & Communication,
[1, 2] 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 degree 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.

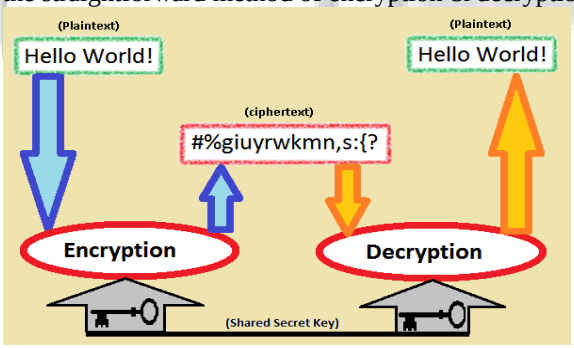


Fig. 1: Encryption & Decryption Process

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 commended 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 adding every round of AES except the last uses the four transformations.

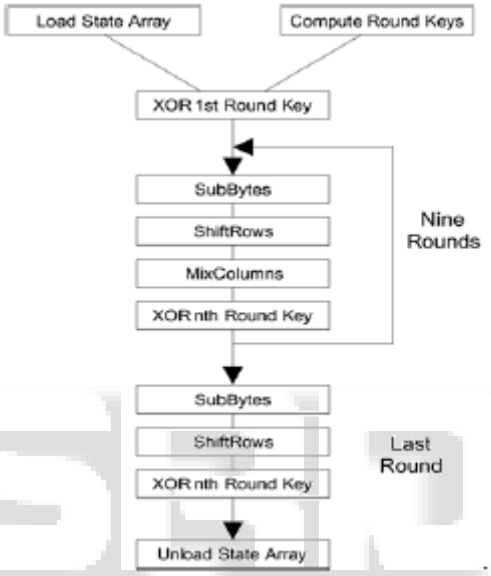


Fig. 2: Process of AES

[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 bite 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.

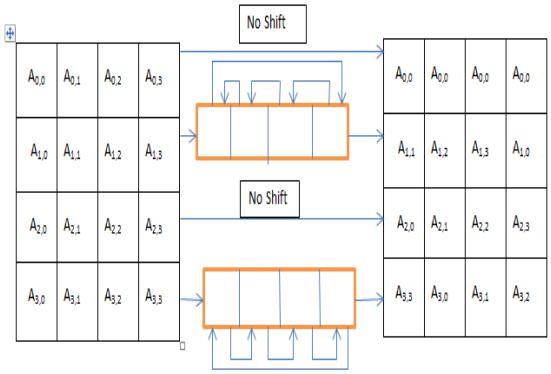


Fig. 3: Shift-Row Transformation for Odd Rows

[Seyed Hossein Kamali, Reza Shakerian, Mohsen Rahmani, Maysam Hedayati, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption",2010 International Conference on Electronics and Information Engineering (ICEIE 2010)]

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.

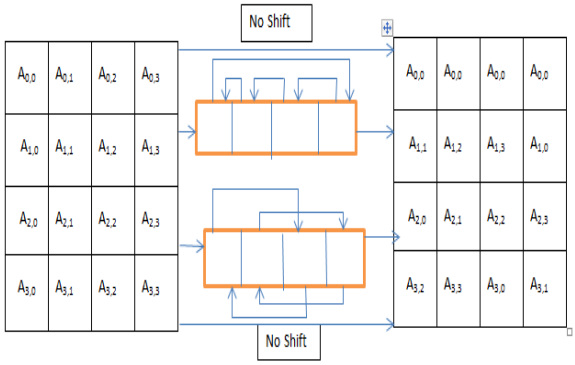


Fig. 4: Shift-Row Transformation for Even Rows

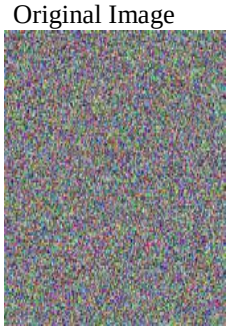
[Seyed Hossein Kamali, Reza Shakerian, Mohsen Rahmani, Maysam Hedayati, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption",2010 International Conference on Electronics and Information Engineering (ICEIE 2010)]

IV. IMAGES OF DIFFERENT SIZE

(512X512)
Size on Disk: 84kb


Original Image


Gray scale Image


Encrypted Image


Decrypted Image

(1024X1024)
Size on Disk: 160kb


Original Image


Gray scale Image


Encrypted Image


Decrypted Image

V. COMPARATIVE ANALYSIS OF DIFFERENT PARAMETERS

Sr. No.	Image	Size On Disk	Data_IN	Algo.	Timing (us)	Memory (kb)
1	512X512	84Kb	32 bit	AES	6.112	349936
				MAES	3.911	366320
2	1024X1024	160Kb		AES	6.321	530160
				MAES	4.128	562928

Sr. No.	Image	Size On Disk	Data_IN	Algo.	Timing (us)	Memory (kb)
1	512X512	84Kb	64 bit	AES	7.591	403938
				MAES	7.128	436706
2	1024X1024	160Kb		AES	7.988	567778
				MAES	7.3110	633314

Sr. No.	Image	Size On Disk	Data_IN	Algo.	Timing (us)	Memory (kb)
1	512X512	84Kb	128 bit	AES	9.441	451424
				MAES	9.121	516960
2	1024X1024	160Kb		AES	9.998	615264
				MAES	9.628	746336

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

[1] Seyed Hossein Kamali, Reza Shakerian, Mohsen Rahmani, Maysam Hedayati, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption",2010 International Conference on Electronics and Information Engineering (ICEIE 2010)

[2] 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

[3] Shashi Mehrotra Seth, Rajan Mishra ,"Comparative Analysis Of Encryption Algorithms For Data Communication",Ijcst Vol. 2, Issue 2, June 2011 I S S N : 2 2 2 9 - 4 3 3 3 (P R I N T) | I S S N : 0 9 7 6 - 8 4 9 1 (On L I N E).

[4] Arjen K. Lenstra, "Unbelievable Security Matching AES security using public key Systems".

[5] Eman A. Abdel-Ghaffar, Mahmoud E. Allam, Hala A. K. Mansour, and M. A. Abo-Alsoud, "A Secure Face Recognition System",978-1-4244-2116-9/08/$25.00 ©2008 IEEE.

[6] Eustace Painkras, "Efficient Modeling and Implementation of Advanced Encryption Standard using S ystemC",0-7803-8689-2/04/$20.00 Q2004 IEEE.

[7] K. Guo, Y. Xue and C. Li, "An FPGA Implementation of the Advanced Encryption Standard with Composite Field S-box"

[8] Kevin Allison,KeithFeldman,Ethan Mick, "Blowfish"

[9] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994. B. Schneier, Description of a New Variable-Length Key, 64-BitBlock Cipher (Blowfish)Fast Software Encryption, Cambridge Security Workshop Proceedings(December 1993), Springer-Verlag, 1994, pp. 191-204.

[10] Vikendra Singh, Sanjay Kumar Dubey, "Analysing space complexity of various encryption algorithms",ISSN 0976 – 6367(Print) ISSN 0976 – 6375(Online) Volume 4, Issue 1, January- February (2013), pp. 414-419

[11] Amit Dhir ,"Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs", WP115 (v1.0) March 9, 2000

[12] ZHANG Yun-peng, ZHAI Zheng-jun, LIU Wei, NIEXuan, CAO Shui-ping, DAI Wei-di ,"Digital Image Encryption Algorithm Based on Chaos and Improved DES", 978-1-4244-2794-9/09/$25.00 ©2009 IEEE.

[13] M. Brahmaji Rao,"Classification of RSA and IDEA Ciphers".

[14] D.I.Manfred Lindner, Institute of Computer Technology-Vienna University of Technology.-Presentation.

[15] Hui QIN, Tsutomu SASAO, Yukihiro IGUCHI, "A Design of AES Encryption Circuit with 128-bit Keys Using Look-Up Table Ring on FPGA", IEICE TRANS.INF. &SYST.MARCH 2006.

[16] Rashi Kohli,Manoj Kumar, "FPGA Implementation of Cryptographic Algorithms using Multi-Encryption Technique", International Journal of Advanced Research in Computer Science And Software Engineering.

[17] Abraham Panicker.O, A.Jabeena, Abdul Hassan Mujeeb, "Advanced Image Encryption and Decryption Using Sandwich Phase Diffuser and False Image Along with Crypto graphical Enhancement", 978-1-4244-7286-4/10/$26.00 ©2010 IEEE.

[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.

[19] Swati Paliwal, Ravindra Gupta, "A Review of Some Popular Encryption Technidues"," International Journal of Advanced Research in Computer Science and Software Engineering.

[20] Hiral Rathod,Mahendra Singh Sisodia,Sanjay Kumar Sharma, "A Review and Comparative Study of Block based Symmetric Transformation Algorithm for Image Encryption",IJCTEE,Volume 1,Issue 2

