ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

FPGA Based Data Encryption and Decryption Using Hill Cipher Technique

Prabhavati Mali[1], Snehal Sorte[2], Rupali Umbare[3], Anjali A. Shrivastav[4]

UG Student, Dept. of E&TC Engineering, PCCOE, Pune, Maharashtra, India[1,2,3]

A.P, Dept. of E&TC Engineering, PCCOE, Pune, Maharashtra, India[4]

ABSTRACT: In today's era of communication, data security is very important issue. If one person is sending message to another person, third person might intercept that message and can misuse the information. Thus to overcome this problem, we need a communication device which can not only be used as a wireless paging system but it also ensures the security of the users information. This project describes a design of effective security for data communication through use of Hill Cipher technique for encryption and decryption.

KEYWORDS: FPGA, Hill cipher, MATLAB, Encryption

I.INTRODUCTION

The aim of the proposed system is to develop a cost effective solution that will provide a secured communication. It describes a design of effective security for data communication through use of Hill Cipher technique for encryption and decryption. The data encrypted using this technique will then be hidden in the image using MATLAB software. This encrypted data will then be processed and transmitted. This transmitted data will then be received by FPGA and decrypted using same technique to obtain the original sent data.

II.RELATED WORK

Till now, different approaches have been proposed highlighting the importance of security in the cryptology which is the science of securing particular application from unauthorized access or from getting hacked. Various researchers provides efficient software implementation in securing software applications, but there is limited amount of hardware implementation of the cryptographic algorithms and the hardware implementations which are available follows a single encryption technique and the importance of resource consumption getting neglected while we are securing the application. Developing the hardware platform using the cryptographic algorithms is not an easy task; rather it is a tedious task. So to provide the security and achieving optimization in terms of resource consumption, we have chosen RSA. For achieving the security of the large applications, we can use advance encryption algorithm, since it provides significant level of security. But during the research process, we found that in order to provide optimal level of resource utilization, we have to focus on different parameters i.e. simplicity, security, and operations involved. RSA although is very efficient and standalone algorithm which provides a great amount of security, it provides great level of security but it increases the complexity of the system. We selected Hill Cipher under RSA which is a light weight cryptographic technique, and which can effectively used for small applications since it is known for its simplicity. Some of the limitations which were encountered during the research process are, firstly neglecting the process of efficient resource consumption and its management while securing the applications, secondly single round of encryption, which can be attacked or leaked by unauthorized parties. For more security we have included stenography which helps us to hide our encrypted data into image.

III.PROPOSED HILL CIPHER APPROACH

The core of Hill-cipher is matrix manipulations. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929.

For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher each character is assigned a numerical value like:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

a=0,
b=1,
…..
…..
z=25.
The substitution of cipher text letters in place of plaintext leads to m linear equations. For m=3, the system can be described as follows:
C1=(K11P1+K12P2+K13P3)MOD26---------(2.3) C1=(K21P1+K22P2+K23P3)MOD26---------(2.4)
C1=(K31P1+K32P2+K33P3)MOD26---------(2.5)
18
This can be expressed in terms of column vectors and matrices: C=KP
Where C and P are column vectors of length 3, representing the plaintext and the cipher text and K is a 3*3 matrix, which is the encryption key. All operations are performed
mod 26 here. Decryption requires the inverse of matrix K. The inverse K-1 of a matrix K
is defined by the equation.
K K-1= I where I is the Identity matrix.
K-1 is applied to the cipher text, and then the plain text is recovered. In general terms we can write as follows:
For encryption: C=Ek(P)=Kp
For decrypti on: P=Dk(C)
=K-1 C= K-
1Kp=P

IV. HARDWARE ENVIRONMENT

Since we are concentrating on the hardware implementation of the proposed approach using cryptographic algorithm i.e.,RSA, so the hardware platform which can be used comes in two flavours i.e. FPGA or ASIC, selection of such platform depends on the application, designer of the particular application and its constraints. FPGA refers to Field Programmable Gate Arrays which consist of collection of CLB's which incorporates different operations and logic depending upon the algorithm used .ASIC which refers to the application specific integrated circuits, this is usually used when we have pre determined and specific task since it cannot be customized further and require proper training before handling such task. The following Table 1 will provide the generalized comparative analysis of both the hardware environment; the parameters which will be focused are their purpose, cost factor, reusable component factor, flexibility and their advantages& limitations.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Table 1: Comparative Analysis of FPGA &ASIC

Sr. no.	Parameters	FPGA	ASIC
1	Purpose	Used for General Purpose	Used for Application specific needs of designer
2	Reusable factor	Provides reprogrammable computing and can be modified.	Design for specific need of customer and it can't be modified or reprogrammed.
3	Cost Factor	Cheaper, used for testing	Expensive since it is application specific
4	Flexibility	Highly Flexible	Low Flexibility
5	Advantages	1.Applicability on low volume production circuits, 2.Better & faster time to market 3.Simpler design cycle 4.Used for smaller applications 5. No-upfront non-recurring expenses	1.Applicability on high volume production circuits 2.Low power requirements 3.Lower unit costs 4.Used for large design applications 5. Full custom capability
6	Disadvantages	1.Little more power consumption 2. Limited Design Size	1.Development time is much more than FPGA 2.Expensive design affair 3. Design Issues

V. RESULT AND DISCUSSION

In our project,encryption of data is done in MATLAB and for more security it is hided into image. The image which contains encrypted data is sent toFPGA1. We are using FPGA only for transmission purpose. Now the image is received by FPGA2 and it is transmitted to PC at the receiver side. Then the image from FPGA2 is taken by PC in MATLAB to decrypt data which is present in that image. We have made 2 GUI, that's why the whole process to understand is quite easy.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

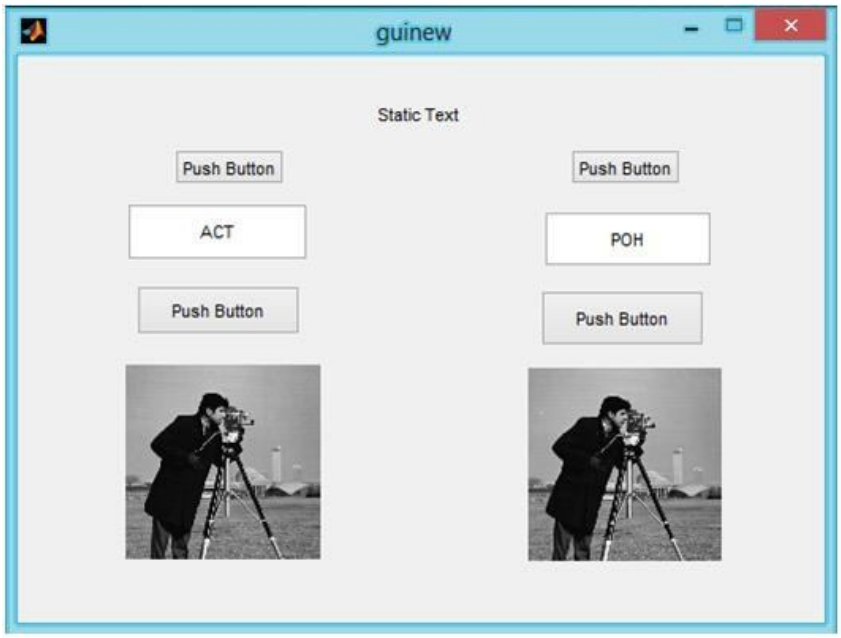

Fig.1: Result of Encryption

In fig.1 the data to be encrypt is ACT, after encryption the data becomes POH. First cameramen image is the original image. The encrypted data POH is hided into this image. The next cameramen image shows the encrypted image. The change in both pictures is change in pixel values of image.

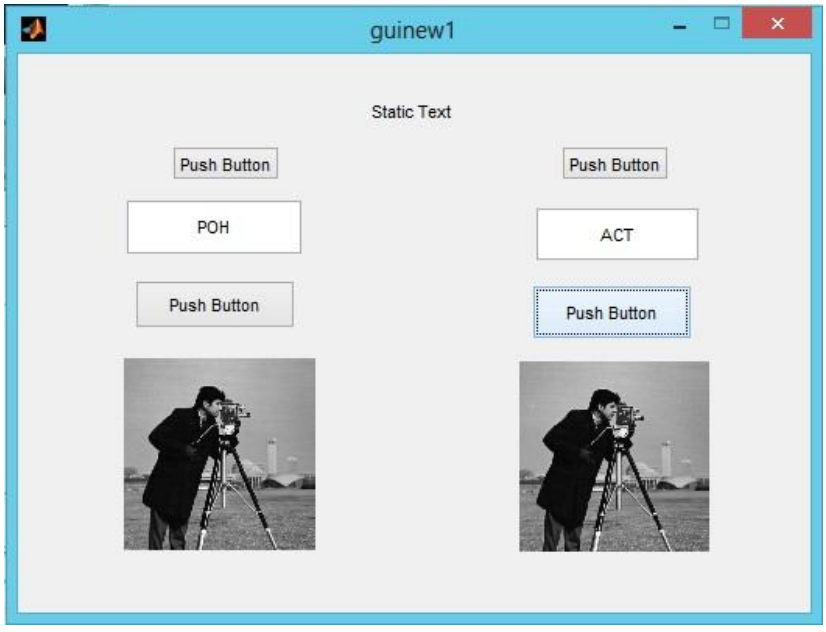

Fig.2: Result of Decryption

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

In fig.2 the data to be decrypt is POH, after decryption the original data is recovered which is ACT. First cameramen image is the encrypted image that we have received. The encrypted data POH is hided into this image. The next cameramen image shows the original image after decryption.

REFERECES

1. Abrams, m., and podell, h. "Cryptography" potentials, ieee, vol. 20, pp.36-38, 2001
2. N khanna, j nath , j james, s chakraborty, a chakrabarti, a nath, " New symmetric key cryptographic algorithm using combined bit manipulation and
msa encryption algorithm: njjsaa symmetric key algorithm", 2011 international conference on communication systems and network technologies, pp
125-130, 2011.
3. M.g. madiesh, m.l. mcguire, s.w. neville," Secret key generation within peer-to-peer network overlays", p2p, parallel, grid, cloud and internet
computing (3pgcic), 2012 seventh international conference, pp 156-163, 2012.