# FPGA Implementation of Image Encryption and Decryption using Fully Homomorphic Technique

**S. K. Alone**

*M.TECH, (Electronics System and Communication Engineering), GCOEA, Amravati, India*

---***---

**Abstract -** *Security of data is the difficult issue of today that have many areas including computers and communication. Modern cyber security attacks have surely affects of the users. Cryptography is technique used to create authentication, integrity, availability, secrecy and identificationof information data can be continued also security and privacy of information data can be given to the user. The cryptography methods and different methods are used to make available a high security to many applications. The greater use of multimedia applications in the industrial and IT process requires us to protect secret information data from unauthorized access. Cryptography is essential solution to protect our information against attacks. The increasing use of multimedia applications in the industrial and IT process requires us to protect confidential image data from unauthorized access. Cryptography is the most relevant solution to protect our information against attacks. There are many image encryption techniques like DES, AES and RSA. Homomorphic encryption is the encryption scheme which means the operations on the encrypted data. Homomorphic encryption can be applied in any system by using various public key algorithms.*

***Key Words***: *—Cryptography, public key algorithm, private key algorithm, Fully homomorphic encryption.*

## 1. INTRODUCTION

To meet the safety requirements, cryptography is a common technique to uphold image security. Cryptography is widely used today because of its security advantages. The major objectives of cryptography are control access, confidentiality, integrity, non-repudiation and authentication. There exist two main types of cryptographic algorithms, the symmetric-key family (the encryption/decryption key is shared between the two parties and remains secret) and the asymmetric-key family (the encryption key is public while the decryption key is private).The benefit of symmetric algorithms is that they do not consume too much of power and are characterized with high speed while encrypting the data. Symmetric key cryptosystems have higher speed than the asymmetric key cryptosystems. Due to various advantages, symmetric algorithms are practised for encryption and decryption of image.

Security is the prime requirement because of the increasing usage of the internet or public cloud for storing the data. Security is needed for preserving the integrity, confidentiality, availability of the information system resources. There can be collection of the data in the encrypted format in any database but if the operations or the computations on the encrypted data are needed to be performed then it is the compulsory to decrypt that data but the decrypted data are not assured any more thus, a new idea of the cryptosystem was proposed that allows the direct operations on the encrypted data. This concept is called privacy homomorphism. However, decryption is not carried out; the result obtained is identical as operations on plaintext. While exclusively controlling encrypted data, implicit additions and multiplications on plaintext values can be executed by the workers by using homomorphic encryption.

Security can be a major issue for such data centers when the information they have are touchy. A data center may be attacked, compromised and an addition the capability of insider attacks .The safety problems with the outward databases can be solved if the critical data are encrypted. Naturally it gives rise to the problem of how the data center can perform computation on encrypted data. Homomorphic encryption schemes, gives a solution for this statement: Such schemes enable for functions to evaluate encrypted data, the result of which is still encrypted data, but can be decrypted back into the result of the (logically)same function applied to the plain data.

## 2. LITERATURE REVIEW

Amal Hafsa, Anissa Sghaier, worked on AES image encryption techniques. The AES is a symmetric-cryptosystem, in which both who send and receives uses a single key for encoding and decoding of the message128 is the length of plaintext, while one hundred twenty two, one hundred ninety two and two hundred fifty six are either keylength. Advanced encryption standard method is an iteration based algorithm. One iteration is called as one round, for keylength one hundred twenty eight, one hundred ninety two, two hundred fifty six the no. of rounds required are ten, twelve and fourteen. The one hundred twenty eightbit algorithm is separated into 16 bytes. These bytes are shown as state array of 4*4 called state matrix, and all the various methods such as subbytes operation, shiftrows operation, mixcolumn operation and addround operation are executed on state matrix.

In the blowfish encryption scheme has been studied, Bruce Schneier, world's first cryptologist proposed the Blowfish algorithm [2] and made it accesable in the public sector. Blowfish is a varying key length, block cipher of 64 bit. The method was first proposed in 1993, and has not been broken yet. It can be modified applications of hardware because of its concentration.

The algorithm is as shown having two parts: first is expansion of key part and data- encryption part is the second part. In key expansion a key size of maximum 448 bit is change to some subkey array of 4168 bytes. Information encryption requires through a 16-round (commonly) network.

RSA algorithm is called as the most excellent encryption public key algorithm. It has been widely applied to encryption and decryption and digital signature.[3] Basic steps are as follows:

(1)Consider two large random numbers and we call them $p$ and $q$. $p$ is unequal to q. Then compute $N$, which is equal to the value p*q;

(2)Choose an integer $e$ less than $\phi(n)$ and $\phi(n)=(p-1)*(q-1)$. Here $\phi(n)$ and $e$ should be comparatively prime numbers.

(3)Use Expanded-Euclidean algorithm to calculate $d$. The formula is given below:

$d * e \equiv 1 \bmod ((p-1)*(q-1))$After the above operation, $(N, e)$ is public key and $(N, d)$ is private key.

The determination of the Diffie-Hellman algorithm is to allowed two users to interchange a secret key confidentially that can be used for subsequent encryption of information. The Diffie-Hellman encryption depends on its difficulty of calculating discret logarithms. q is a prime number and α is an integer and are two publicly familiar numbers. α is a primitive root of q.Consider the consumer A and B wants to interchange a key.Consumer A choses a random number $X_A$<qand calculates the public key $\alpha^{X_A}$mod q.Similarly, user B separately selects a random number $X_B$<q and calculates public key $Y_{B=\alpha^{X}{}_{B}}$mod q. Each side the X value is kept secret and makes the value of Y accesable publicly to the opposite side. Consumer A calculates the key as $K = (Y_B)^{X_A}$ mod q. and consumer B calculates the key as $K = (Y_A)^{X_B}$mod q. Thus, both the sides have interchange a secrete key.

## 3. METHODOLOGY

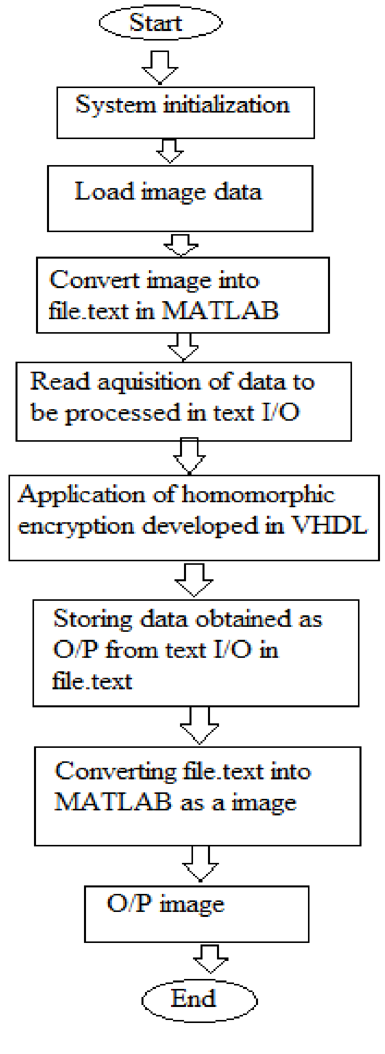
Start
System initialization
Load image data
Convert image into file.text in MATLAB
Read aquisition of data to be processed in text I/O
Application of homomorphic encryption developed in VHDL
Storing data obtained as O/P from text I/O in file.text
Converting file.text into MATLAB as a image
O/P image
End

Fig.1. Block diagram of proposed methodology

System is initialized first. Image is loaded in the MATLAB. Image is converted into file.text. Data to be processed in text I/O is read. Application of Homomorphic encryption is developed in VHDL. Data obtained as O/P from text I/O in file.text is stored. File.text is converted into image in MATLAB. Finally at the output original recovered image is acquire. The proposed methodology is splitted into following blocks:

A. Encryption
B. Decryption

A. Encryption Process

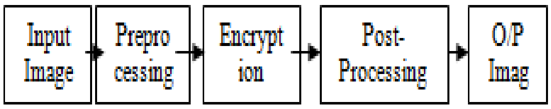

Fig.2. Encryption Process

The original image is read using Matlab and it is converted into text file by using preprocessing. It is given as input to homomorphic encryption algorithm developed in VHDL language. Homomorphic encryption algorithm simulated on Modelsim and synthesized on Quartus II and the result of implementation on the FPGA cyclone IV.E is presented in the console of the card DE2-115 in the form of the 256 * 256 pixels. Then the output of homomorphic algorithm is given to the postprocessing to get the encrypted image.

B. Decryption Process

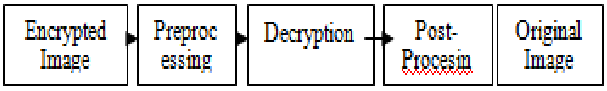

Fig.3. Decryption Process

In decryption process the encrypted image is given as input to the preprocessing. It is given as input to homomorphic decryption algorithm developed in VHDL language. Homomorphic decryption algorithm simulated on Modelsim and synthesized on Quartus II and the result of implementation on the FPGA cyclone IV.E is presented in the console of the card DE2-115 in the form of the 256 * 256 pixels. Then the output of homomorphic decryption algorithm is given to the postprocessing to get the decrypted image i.e. original image.

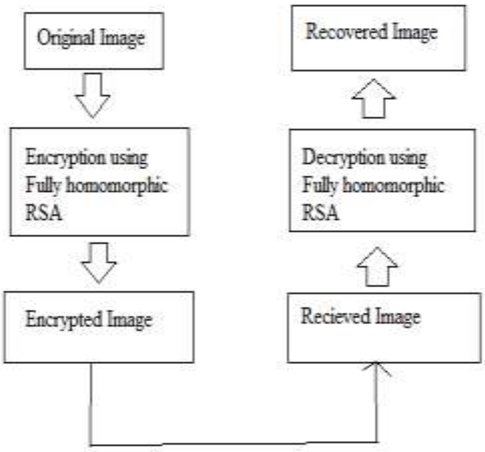
Original Image
Encryption using Fully homomorphic RSA
Encrypted Image
Recovered Image
Decryption using Fully homomorphic RSA
Recieved Image

Fig.4. Proposed Method Hybrid Homomorphic Encryption scheme

In this part, the possibility to fabricate another encryption scheme which supports all homomorphic tasks from the partial encryption schemes that supports a limited number of homomorphic operations (addition or multiplication). The partial homomorphic encryption schemes can support just only homomorphic property. While, the fully homomorphic encryption schemes can support all properties of homomorphic. To build a new fully homomorphic encryption scheme which supports all homomorphic operations from two partial homomorphic encryption schemes one supports only addition and other supports only multiplication operations. The hybrid homomorphic encryption scheme must preserve the algebraic structure.

Algorithm steps for Encryption and Decryption:

RSA Multiplicative PHE Rivest, Shamir and Adleman published their public key cryptosystem in 1978. Although it is a very basic algorithm, it is one of the most crucial building blocks of homomorphic encryption, which is why it has been included as an example of multiplicative partial homomorphic encryption technique. RSA algorithm is regarded as the most excellent public key encryption algorithm by far. It has been widely applied to encryption and decryption and digital signature. RSA key length increases along with the increase of con_dentiality level. Therefore, we need to continuous optimize the process of key generating in order to adapt the market demand.RSA algorithm as shown below:

(1)Generate two large random numbers and we call them p and q. p is unequal to q. Then compute N, which is equal to the value p multiplied by q.

(2)Choose an integer e less than $\varnothing(n)$ and $\varnothing(n) = (p - 1) * (q- 1)$. Here $\varnothing(n)$ and e should be comparatively prime numbers.

(3)Use Expanded-Euclidean algorithm to calculate d. The formula is given below: $d * e \equiv 1 mod((p - 1) *(q - 1))$ After the above operation, (N, e) is public key and (N,d) is private key.

For Encryption cyphertext C = $M^e mod\, n$

For Decryption plaintext M = $C^d mod\, n$

By using Modulo Addition

C = $(M^e mod\, n) \oplus K$

## 4. RESULTS

MATLAB RESULTS:

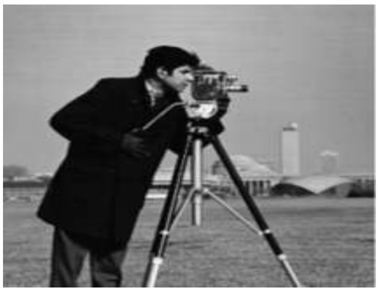

Fig.5.Original Image

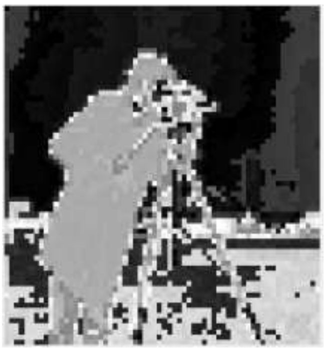

Fig.6.Encrypted image

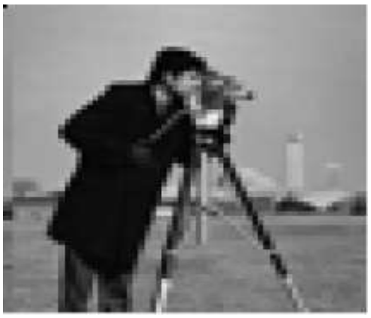

Fig.7.Recovered original image

SYNTHESIS RESULTS

| | |
|---|---|
| Quartus Version | 9.1 SP2 |
| Family | Cyclone II |
| Device | EP2C35F672C6N |
| Total logic elements | 734/33.216 (2%) |
| Total combinational function | 734/33.216 (2%) |
| Dedicated logic registers | 309/33.216 (2%) |
| Total Pins | 9/475 (2%) |
| Total thermal Power dissipation | 31.05 mW |

## 5. CONCLUSION

A fully homomorphic encryption scheme would appear to solve the security problem. Homomorphic encryption schemes permit anyone to evaluate functions on encrypted data, but the evaluators never see any information about the result. It is possible to construct an encryption scheme where a user can compute f(m) from an encryption of a message m, but she should not be able to learn any other information about m.

## REFERENCES

[1]Zainab Hikmat Mahmood, Mahmood Khalel Ibrahem "New Fully Homomorphic Encryption Scheme Based On Multistage Partial Homomorphic Encryption Applied In Cloud Computing" 2018 1st Annual International conference on Information and Sciences (AICIS).

[2] Kirandeep Kaur , Jyotsna Sengupta,"Optimizing Fully Homomorphic Encryption Algorithm using Greedy Approach in Cloud Computing", International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 4, Jul – Aug 2017).

[3]Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, Rutvij H. Jhaveri," Survey of Various Homomorphic Encryption algorithms and Schemes", International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014.

[4]Li Dongjiang, Wang Yandan" The research on key generation in RSA public- key cryptosystem", 2012 Fourth International Conference on Computational and Information Sciences.

[5] Amal Hafsa, Anissa Sghaier, Wajih Elhadj Yousef," Image Encryption /Decryption Design Using NIOSII Soft Core Processor", ICEMIS2017.

[6] Trivedi, M. A. Hasamnis," Development of Platform Using NIOS II Soft Core Processor for Image Encryption and Decryption Using AES Algorithm",IEEE ICCSP conference, 2015.

[7] M. P. Leongl, S. Z. M. Naziril, S. Y. Pemgl, "Image Encryption Design using FPGA", International Conference on Electrical, Electronics and System Engineering ,2013.

[8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption",International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:1, No:3, 2007.

[9] Melchor, Carlos Aguilar, et al. "Improving Additive and Multiplicative Homomorphic Encryption Schemes Based on Worst-Case Hardness Assumptions}." IACR Cryptology ePrint Archive 2011 (2011): 607.

[10]Vaidehi, E. "Computing Aggregation Function Minimum/Maximum using Homomorphic Encryption Schemes in Wireless Sensor Networks (WSNs)." California State University, East Bay Hayward, CA, USA. (2007).

[11]Xidan Song, Yulin Wang, "Homomorphic Cloud Computing Scheme Based on Hybrid Homomorphic Encryption," in *IEEE International Conference on Computer and Communication (ICCC ), Chengdu , China, 2017.*

[12]Abdellah EZZATI, Khalid EL MAKKAOUI , Abderrahim BENI HSSANE, "Homomorphic Encryption as a Solution of Trust Issues in Cloud," in *International Conference on Big Data, Cloud and Applications, Tetuan, Morocco, 2015.*