International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 7, July 2015, PP 129-139
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

# Secure Data Communication using Cryptography and Steganography Standards

[1]N. Pavani, [2]B. Sarala

[1]*M.E Scholar, Dept. of Electronics & Communication Engg., M.V.S.R. Engineering College*
[2]*Associate Professor, Dept. of Electronics & Communication Engg., M.V.S.R. Engineering College*

## ABSTRACT

In the today's world, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks.RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. No other key can decrypt the message – not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. In this paper, we have done an efficient implementation of RSA algorithm using two public key pairs and using some mathematical logic rather than sending the value directly as a public key. Because if an attacker has opportunity of getting the e value they can directly find d value and decrypt the message.

**Keywords:** FPGA, Cryptography, RSA Algorithm, LSB, Stenography.

## INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into anunreadable format in which a message can be concealed from the casual reader and only the intended recipient will beable to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By usingcryptography we can assist this shaky information by secrete writing on our computer network. Cryptography rendersthe message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content ofdata like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is tokeep the data secure from unauthorized access. In traditional (symmetric-key) cryptography, the sender and receiver ofa message know and use the same secret key.The main challenge is getting the sender and receiver to agree on thesecret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phonesystem, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears orintercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key.

Because all keys in a secret-key (symmetric-key) cryptosystem must remain secret, secret-key cryptography often hasdifficulty providing secure key management.To solve the key management problem, Whitfield Diffie and MartinHellman introduced the concept of public-key cryptography in 1976. Public-key cryptography refers to a cryptographicsystem requiring two separate keys, one of which is secret and one of which is public. Although different,the two partsof the key pair are mathematically linked.

The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integerfactorization and discrete logarithm problems).Although it is easy for the recipient to generate the public and privatekeys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key,it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This iswhy, unlike symmetric key

***Address for correspondence:***

pavani.nukapally@gmail.com

algorithms, a public key algorithm does *not* require a secure initial exchange of one (ormore) secret keys between the sender and receiver.In practice, only a hash of the message is typically encrypted forsignature verification purposes.Public-key cryptography is a fundamental, important, and widely used technology. It isan approach used by many cryptographic algorithms and cryptosystems.

## CRYPTOGRAPHY AND TYPES

Cryptography uses the process of transposition and substitution of the characters to hide and retrieve the data. At thesender side we call it Encryption shown in Figure.1 and at the receiver side we called it decryption shown inFigure.2.We use the various keys to encrypt a decrypt the data. Keys are the special digital functions or methods thatconvert the plain text into inscribe format and it's vice versa. Every element of the network has two keys namelyprivate or personal key which is known to a particular person and public key which is known by all persons in thenetwork. There are two types of cryptography.

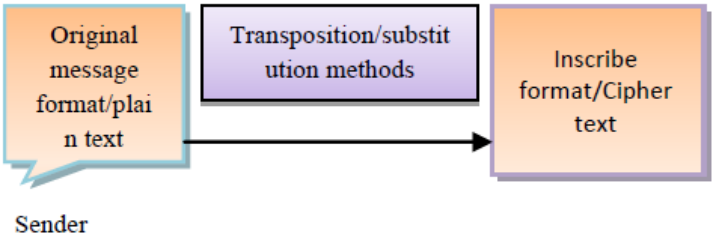



**Fig1.** *Encryption Process*

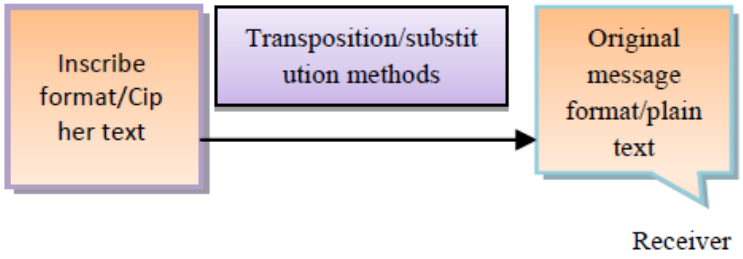



**Fig2.** *Decryption Process*

### Same key Cryptography or Private Key Cryptography

In this type of cryptography the receiver and sender applies the same key to encrypt and decrypt the message or recoverthe plaintext from cipher text and vice versa, so this type of cryptography is also known as symmetric encryption anddecryption. Figure.3 is showing the whole process of encryption and decryption which is carried out through receiver'sprivate key. Through this cryptography form, it is obvious that the secret key must be known to both the sender and thereceiver that why it is known as private key cryptography. Transmitting the secret key on insecure network can alsodestroy the security.

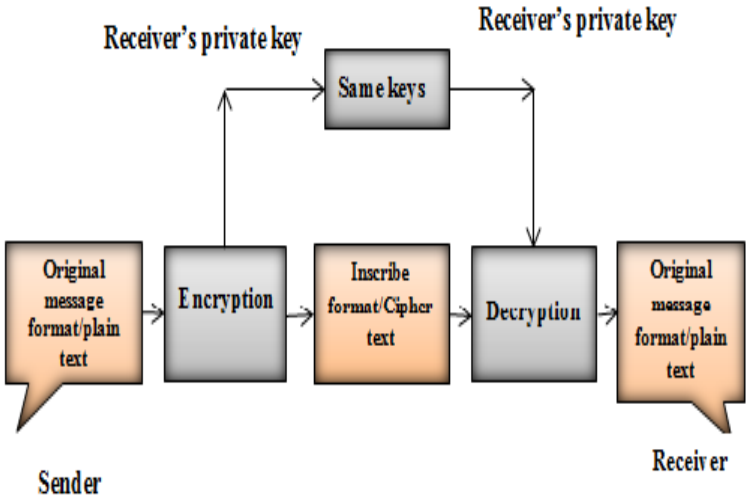



**Fig3.** *Same key cryptography*

### Different Key Cryptography or Public Key Cryptography

In this type of cryptography, the receiver and sender apply the Different keys to encrypt and decrypt the message orrecover the plaintext from cipher text and it's vice versa. This type of cryptography is also known as asymmetricencryption and decryption.Figure.4 is showing the whole process where receiver's public key is used for encryptionand receiver's private key is used for decryption. In public key cryptography, each user or the

workstation take part inthe communication have a pair of keys, a public key and a private key and a set of operations associated with the keysto do the cryptographic operations. Only a particular user/device knows the private key whereas the public key isdistributed to all users/devices taking part in the communication. Since the knowledge of public key does notcompromise the security of the algorithms, it can be easily exchanged online.

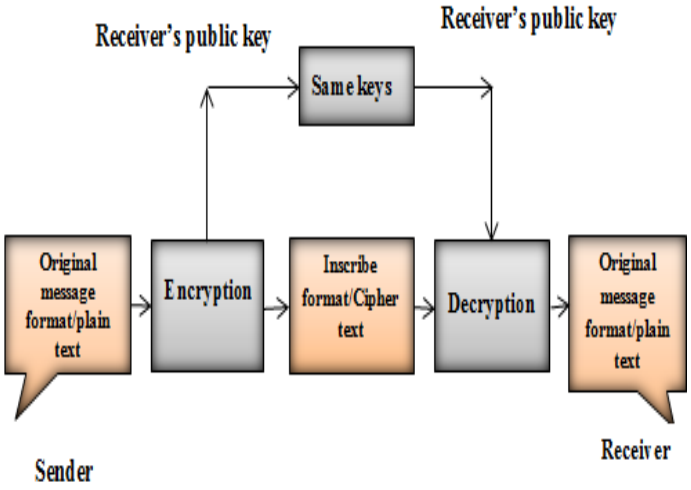



**Fig4.** *Different key cryptography*

## THE RSA ALGORITHM AND ITS MATHEMATICAL FOUNDATION

### The Mathematical Foundation for RSA Algorithm

The RSA digital signature has precise mathematical foundations, which are as follows [1]-

*Theorem* 1- (fundamental theorem of mathematics) any positive integer *a* can be denoted as ai=P1.....Pn, which *P*1 >*P*2>*P*3 … >*PT* are all prime numbers, *ai*> 0.

*Theorem 2*- (Euclid theorem) any two integers a and b has a greatest common factor d, in which d can be expressed asthe linear combination of a and b with integer coefficient, namely *s*, *t* ∈*Z*, which satisfies *d* = *sa* + *tb*.

*Theorem 3*-(Fermat theorem) If *p* is a prime number then for any positive integer that prime to *p*, *a* *(p-1)* ≡1 (mod *p*).*Definition 1* (Euler function (*n*) ) When *n* = 1, ϕ (1) = 1, when *n* > 1, the value of ϕ (*n*) is the amount of positive integeris less than then and prime to *n*.

*Theorem 4*-If *p* and *q* are all prime numbers and *p*≠ *q*, then ϕ ( *pq*) =ϕ ( *p*)ϕ (*q*) = ( *p* −1)(*q* −1).

*Theorem 5*-**(**Euler theorem) If integer *a* is co prime to integer n, then a□(n) ≡ (mod *m*).

Above theorem have the following 3 deductions:

(1) If p is prime number and *n* = *p*, then *a(p-1)* ≡ 1(mod *p*), namely the Fermat theorem.

(2) *a*ϕ *(n+1)* ≡ a (mod *p*).

(3) If n = *pq*, *p* and *q* are prime numbers and p≠ *q*, for 0<*m*<*n*, if (*m*, *n*) = 1, then (n) 1 *m* *m*ϕ + ≡ (mod *n*), namelym(p- 1)(q-1)+1≡ (mod *n*).

Above five theorems will be used in the feasibility proof of RSA digital signature algorithm in the following section.

*Theorem 6*-If *p* and *q* are prime numbers and *p*≠ *q*, *rm*≡ 1 (mod (*p*− 1)(*q* − 1)) , *a* is any positive integer, *b* ≡ $a^m$mod*pq*, *c* ≡ $b^r$mod *pq*, then *c* ≡ *a* mod *pq*.

## RSA Key Generation Algorithm

**Step1-** Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of therequired bit length, e.g. 1024 bits.

**Step2-** Compute n = pq and (φ) phi = (p-1)(q-1) [Theorem 4].

**Step3-** Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1. [Theorem 2].

**Step4-** Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi). [Theorem 6].

**Step5-** The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

## Encryption Algorithm

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer *m*
3. Computes the cipher text $c = m^e \bmod n$.
4. Sends the cipher text *c* to B.

## Decryption Algorithm

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.

2. Extracts the plaintext from the message representative *m*.One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT andfirst published in 1978. The RSA scheme has become the most widely accepted and implemented approach to publickeyencryption. RSA is named after its inventors Rivest, Shamir, and Adleman.RSA is a block cipher in which theplaintext and cipher text are integers between 0 and *n*- 1 for some *n*.Encryption and decryption are of the followingform, for some plaintext block M and cipher text block C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the values of *n* and *e*, and only the receiver knows the value of *d*. This is a publickeyencryption algorithm with a public key of *KU = {e,n}* and a private key of *KR = {d,n}*.For this algorithm to besatisfactory for public-key encryption, the following requirements must be met:

1. It is possible to find values of *e*, *d*, *n* such that $M^{ed} = M \bmod n$for all M<*n*.

2. It is relatively easy to calculate $M^e$and$C^d$for all values of M <*n*.

***Steps-***

•**Step1-** Begin by selecting two prime numbers, *p* and *q*, and calculating their product *n*, which is the modulus forencryption and decryption.

• **Step2-** Next, we need the quantity φ*(n) re*ferred to as the Euler totient of *n*, which is the number of positive integersless than *n* and relatively prime to *n*.

• **Step3-**Then select an integer *e* that is relatively prime to φ*(n) (i*.e., the greatest common divisor of *e* and φ*(n)* is 1).

• **Step4-** Select two numbers a and b such that $b=a^e$

•**Step5-**Using this numbers formulate two public key {b,n},{a}

•**Step6-**Finally, calculate d as the multiplicative inverse of e(which is public key in normal RSA), modulo φ(n). But tocalculate it let the receiver choose any positive natural number and multiply it with a then add b, divide theresult by a and finally subtract the chosen value then the receiver has e. then calculate d as usual.

•**Step7-** Itcan be shown that d and e have the desired properties.

•**Step8-**Suppose that user A has published its public key and that user B wishes to send the message M to A.

•**Step9-** Then B calculates C = $M^{b/a}$(mod n) and transmits C.

•**Step10-** On receipt of this cipher text, user A decrypts by calculating M = $C^{d}$(mod n).

## Steganography

Steganography is that the methodology cowl} information during a cover media like text, audio, image, video, etc. In different words, Steganography is that the method of concealing a secret messages at intervals a bigger one in such the way that somebody cannot understand the presence or contents of the hidden message. Steganography can hide the message thus there's no data of the existence of the message within the place. The term Steganography is forked from the Greek words "stegos" that means "Cover" and "grafia" that means "writing" process it as "covered writing". Generally, there are 2 forms of information concealing techniques mistreatment images: abstraction and frequency domain. The abstraction domain is predicated on embedding message within the leastsignificant bit (LSB) of image picture element. The fundamental LSB methodology is straightforward for implementation and its high capability. However it's weak versus some attacks like low-pass filtering and compression. The frequency domain embeds the messages within the frequency coefficients of pictures. These concealing ways overcome the issues found within the abstraction domain. Steganalysis is nothing however the method of police works hidden informationwhich is crested mistreatment Steganography. Steganalysis detects Stego-images by analyzing varied image options between Stego-images and cover-images. In recent researches, various Steganography techniques supported genetic algorithms is free. Currently daily the Steganography techniques are developed on varied FPGA hardware. Field programmable gate array i.e. FPGA, provides the re configurability similarly because the hardiness for the image process. Due to the utilization of FPGA we will develop another approach supported AN embedded FPGA system for image processing. Field Programmable Gate Array (FPGA) is wide utilized in embedded applications like automotive, communications, industrial automation, control, medical imaging etc. And while not requiring hardware change out,the uses of FPGA kind Devices will expand the merchandise life by change information stream files. FPGAs have capability to hold a complete system on one chip additionally it permits in-Platform testing and debugging of the system. Moreover, it offers the chance of utilizing hardware/software co-design to develop a high performance system for various applications by incorporating processors.

## Proposed SteganographyMethod

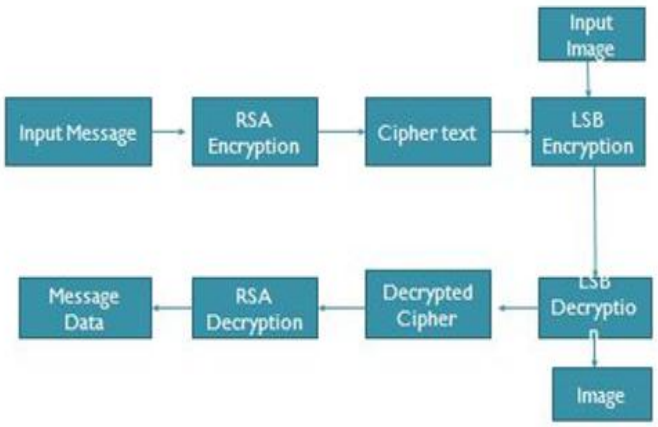



**Fig5.** *Block Diagram of Invisible Stenography*

Message coding on a picture may be divided in to 2 components, one portion is knowledge activity different is Reversible knowledge activity. In knowledge activity half there's a digital image within which we have a tendency to write secret message by removing LSB of image pel and add our secret message on corresponding LSB position, then the output image is termed Stego image. For retrieve the key message program splits the image into its channels and applies the inverse lifting theme to every channel to the extent such as by the user. Once the transformation is completed, the program retrieves the message out of the pixels of the duvet image. Different streams of digital media may be used as a canopy stream for a secret message. Steganography is that the art of writing secret message in order that solely the sender and therefore the supposed recipient are responsive to the hidden message. A prospering info activity ought to end in the extraction of the hide knowledge from the image with high degree of knowledge integrity. Current trends favour exploitation digital image files because the cowl files to cover another digital file that contains the key message or info.

## Header File Creation

To creating the header file for Cover image and secret Message by using GUI in Matlab software.

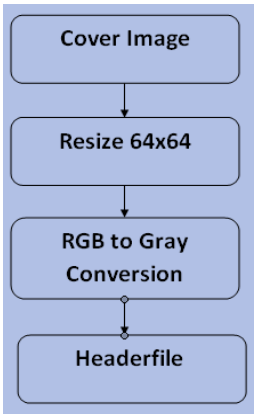



**Fig6.** *Header File conversion by using Matlab software*

## Least Significant Bit (LSB) Technique

Fig7. shows the 1-bit LSB. In Fig., the picture element price of the quilt image is 141(10001101)2 and therefore the secret knowledge is zero. It applies to LSB-1 that the modified picture element price of the quilt is 140(10001100)2. LSB will store 1-bit in every picture element. If the quilt image size is sixty four x sixty four pictureelement image, it will therefore store a complete quantity of bytes of embedded knowledge.

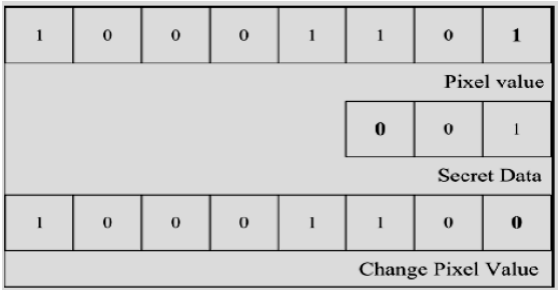



**Fig7.** *Example of LSB*

Proposed methodology supported LSB technique; we have a tendency to propose a replacement watermarking algorithmic rule. Most of researchers have planned the primary LSB and therefore the third and forth LSB for activity the information however our planned watermarking algorithmic rule is victimization the third and fourth LSB for activity the information And victimization the RGB watermark image embedding in blue element of original image attributable to less sensitivity. This can be attributable to the protection reason. So, nobody can expect that the hidden information within the third and therefore the forth LSB. Fig. a pair of shows the framework of the planned methodology. First, we have a tendency to choose the image that may be a colour image and that we can transfer the information to binary worth when writing it. Then, we have a tendency to hide the information within

the image victimization the planned algorithmic rule. Fig. three shows the embedding algorithmic rule in VLSI.

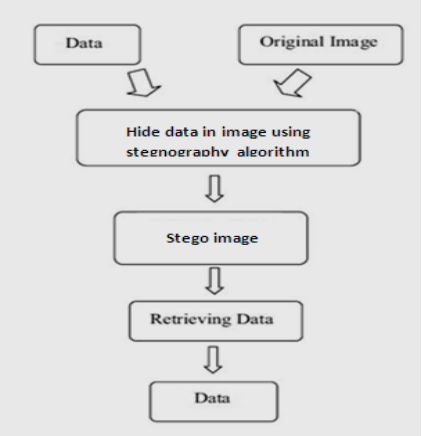



**Fig8.** *Frame work of Steganography*

## EXPERIMENTAL SETUP

### Xilinx Platform Studio

The Xilinx Platform Studio (XPS) is that the development setting or interface used for planning the hardware portion of your embedded processor system. B. Embedded Development Kit Xilinx Embedded Development Kit (EDK) is an integrated software tool suite for developing embedded systems with Xilinx Micro Blaze and PowerPC CPUs. EDK includes a spread of tools and applications to help the designer to develop an embedded system right from the hardware creation to final implementation of the system on an FPGA. System style consists of the creation of the hardware and computer code parts of the embedded processor system and therefore the creation of a verification part is elective.

A typical embedded system design project involves: hardware platform creation, hardware platform verification (simulation), computer code platform creation, computer code application creation, and computer code verification. Base System Builder is that the wizard that's accustomed mechanically generates a hardware platform in step with the user specifications that's defined by the MHS (Microprocessor Hardware Specification) file.

The MHS file defines the system design, peripherals and embedded processors]. The Platform Generation tool creates the hardware platform victimisation the MHS file as input. The computer code platform is defined by MSS (Microprocessor computer code Specification) file that defines driver and library customization parameters for peripherals, processor customization parameters, commonplace a hundred and ten devices, interrupt handler routines, and different computer code connected routines. The MSS file is associate degree input to the Library Generator tool for personalisation of drivers, libraries and interrupts handlers.

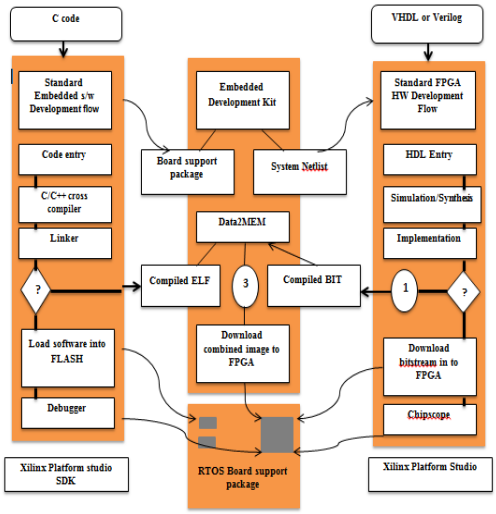



**Fig9.** *Embedded Development Kit Design Flow*

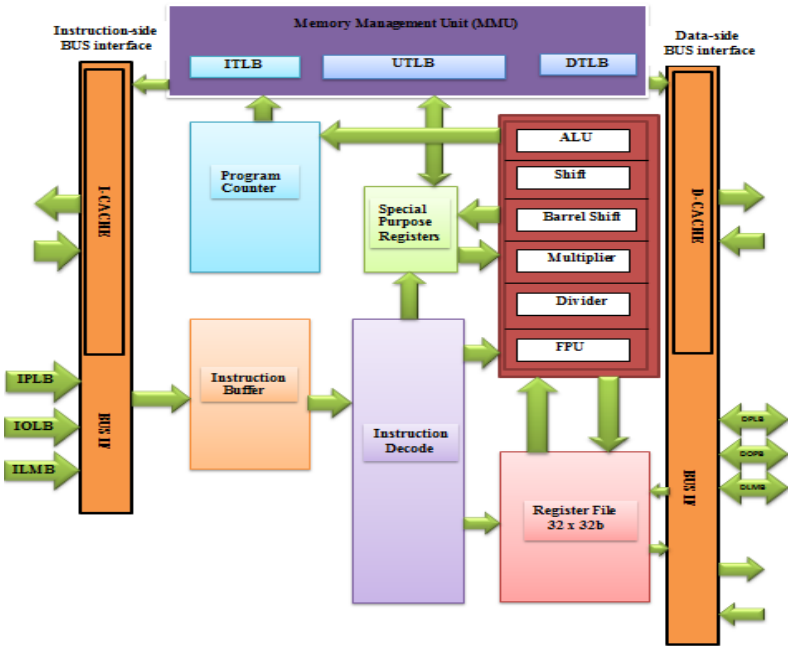
The creation of the verification platform is no obligatory and is predicated on the hardware platform. The MHS file is taken as Associate in Nursing input by the Simgen tool to make simulation files for a particular machine. 3 styles of simulation models will be generated by the Simgen tool: behavioural, structural and temporal arrangement models. Other helpful tools offered in EDK area unit Platform Studio that provides the interface for making the MHS and MSS files. Produce / Import information science Wizard that permits the creation of the designer's own peripheral and import them into EDK comes. Platform Generator customizes and generates the processor system within the variety of hardware netlists. Library Generator tool configures libraries, device drivers, file systems and interrupt handlers for embedded processor system. Bit streamInitialize tool initializes the instruction memory of processors on the FPGA shown in figure2. Wildebeest Compiler tools area unit used for compilation and linking application executables for every processor within the system [6]. There are unit 2 choices offered for debugging the applying created mistreatment EDK namely: Xilinx chip correct (XMD) for debugging the applying software system employing a chip correct Module (MDM) within the embedded processor system, and software system computer program that invokes the software system computer program similar to the compiler getting used for the processor. C. software system Development Kit Xilinx Platform Studio software system Development Kit (SDK) is Associate in Nursing integrated development surroundings, complimentary to XPS, that's used for C/C++ embedded software system application creation and verification. SDK is made on the Eclipse open supply framework. Soft Development Kit (SDK) may be a suite of tools that permits you to style a software system application for designated Soft information science Cores within the Xilinx Embedded Development Kit (EDK).The software system application will be written in a very "C or C++" then the whole embedded processor system for user application are going to be completed, else correct & transfer the bit file into FPGA. Then FPGA behaves like processor enforced on that in a very Xilinx Field Programmable Gate Array (FPGA) device.

Features of small Blaze Processor

The small Blaze soft core processor is very configurable and therefore the feature set of the processor includes:

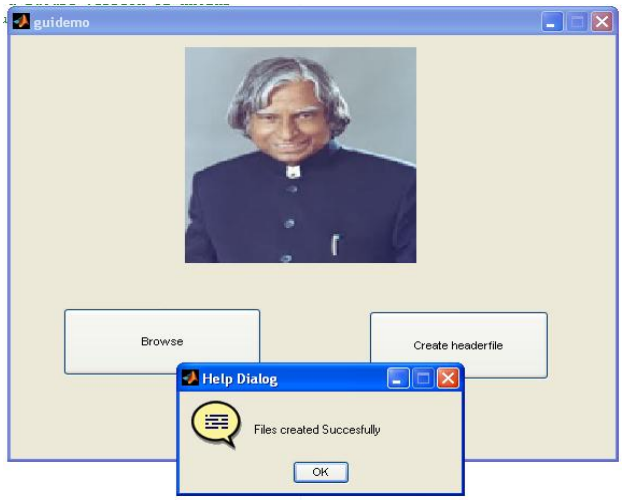
- 5 Stage Pipeline
- Cardinal 32-bit general purpose registers
- 32-bit instruction word with 3 operands and 2 addressing modes,

32-bit address bus and Single issue pipeline. Additionally to those mounted options, the small Blaze processor is parameterized to permit selective facultative of extra practicality. Xilinx recommends that every one new styles use the newest most popular version of the small Blaze processor.

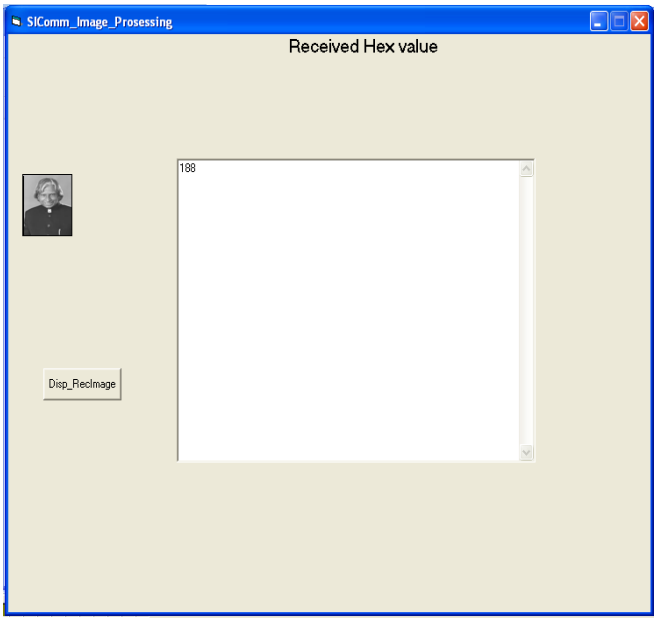



*Micro Blaze processor*

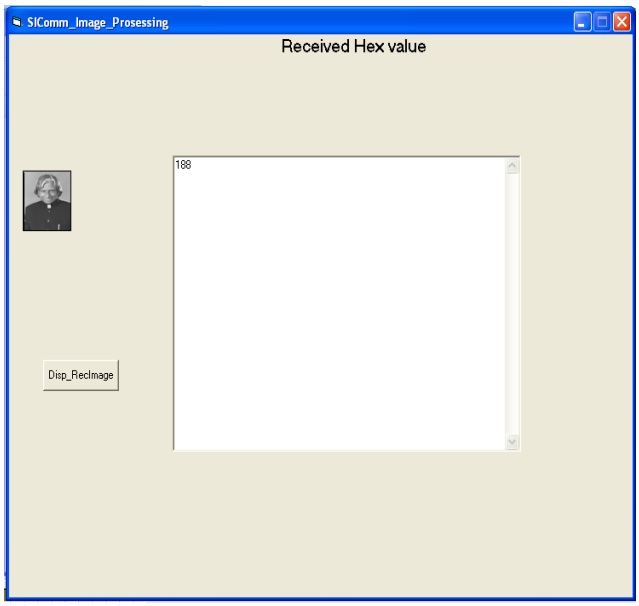
## RESULTS



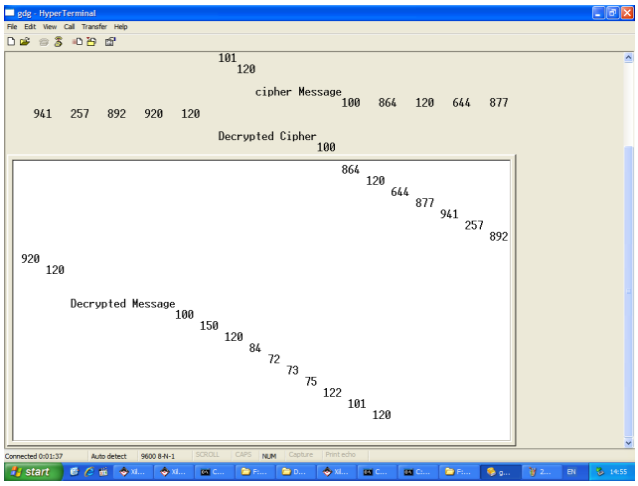

*Headerfile creation*




*Cover Image*




*Output Image*




*Outputin Hyper terminal*

## CONCLUSION

In this paper an algorithm is proposed for RSA, a method for implementing a public-key cryptosystem (RSA) using two public key and some mathematical relation. This two public keys are sent separately, this makes the attacker not to get much knowledge about the key and unable to decrypt the message. The proposed RSA is used for system that needs high security.

This paper has also mentioned some Steganography techniques that space unit planned on field programmable gate array. Mainly the spatial domain and work domain techniques space unit taken into thought. Once inquiring the synthesis results for individual techniques discovered that FPGA is the simplest resolution for the economical image method. Also by correct hardware style development square measure is ready to improve the results for spatial domain i.e. LSB technique.

Also future work is going to be done on improvement of developed hardware architectures with improve in power, timing, and area.

## REFERENCES

[1] MaheswariLosetti, Kanaka RajuGariga "An Enhanced Rsa Algorithm for Low Computational Devices" International Journal of Advanced Research and Innovations Vol.1, Issue .2, pp 114-118.

[2] Kuldeep Singh, Rajesh Verma, Ritika Chehal "Modified Prime Number Factorization Algorithm (MPFA) For RSA Public Key Encryption"International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, September 2012, pp 204-206.

[3] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012, pp134-138.

[4] MJ Wiener. (1990), "Cryptanalysis of short RSA secret exponents", IEEE Transactions on Information Theory, Vol 36, No 3, pp 553-558.

[5] R Gennaro. (2000), "RSA-Based Undeniable Signatures", Journal of Cryptology, Vol 13, No. 4, pp 397-416.

[6] R Cramer, V Shoup. (2008), "Signature schemes based on the strong RSA assumption", ACM Transactions on Information and System Security, Vol 3, No 3, pp 161-185.

[7] Gennaro. (2008), "Robust and Efficient Sharing of RSA Functions", Journal of Cryptology, Vol 13, No 2, pp 273-300.

[8] D Boneh, M Franklin. (2001), "Efficient generation of shared RSA keys", Journal of the ACM, Vol 48, No. 4, pp 702-722.

[9] Rivest, R.; A. Shamir; L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM21 (2): 120–126, doi: 10.1145/359340.359342, 1977.

[10] B. Schneier, Applied cryptography, second edition, NY: John Wiley & Sons, Inc., 1996.

[11] William Stallings, Cryptography and Network Security, Pearson Education, Fourth Edition.

[12] AtulKahate, Cryptography and Network Security, Tata McGraw-Hill Publishing Company Limited.

[13] NidhiSinghal, J.P.S.Raina "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011.

[14] Priti V. Bhagat, Kaustubh S. Satpute and Vikas R. Palekar "Reverse Encryption Algorithm: A Technique for Encryption &Decryption" International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013,pp 90-95.

[15] Gagandeepshahi, Charanjitsingh "Cryptography and its two Implementation Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 3, May 2013,PP 668-672.