ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.7

FPGA Implementation of Non Linear Equation Based Image Cryptosystem Using Different Adders

Rithmi Mitter
Assistant Professor
Department of ECE
KGiSL Institute of Technology, Coimbatore, Tamil Nadu, India

Abstract:
In today's environment, security becomes an important issue in communication. For secure transmission of data in open network, encryption is very important methodology. Though encryption we can prevent our data from unauthorized access during transmission. In recent years many image encryption methods have been proposed and used to protect data. In this paper a new approach for image encryption and decryption using chaotic map and BB equation is described. The comparisons between different adders are also performed to make the encryption process more secure and fast. VLSI architecture for the proposed algorithm is designed and realized using VHDL language in Xilinx ISE VLSI software and implemented using FPGA.

Keywords: BB equation, chaotic map, cryptography, image encryption, image decryption, VLSI.

I. INTRODUCTION

The new information and communication technologies require adequate security. Cryptology is the science that aims to provide information security in the digital world. Information security comprises many aspects, the most important of which are confidentiality and authenticity. Confidentiality means keeping the information secret from all except those who are authorized to learn or know it. Authenticity involves both ensuring that data have not been modified by an unauthorized person (data integrity) and being able to verify who is the author of the data (data origin authentication). Cryptology is usually split up into two closely related fields, cryptography and cryptanalysis.

Cryptography studies how to design good (secure and fast) encryption algorithms, and cryptanalysis tries to find security weaknesses of existing algorithms and studies whether or not they are vulnerable to some attacks.In the present world, the technologies have been advanced. Most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the internet. There are many possible ways to transmit data using the internet like: via e-mails, sending text and images, etc. However, one of the main problems with sending data over the Internet is the 'security' and authenticity. Data security basically means protection of data from unauthorized users or attackers. Encryption is one of the techniques for the information security. Image encryption is a technique that convert original image to another form that is difficult to understand.So one can access the content only by knowing the decryption key. Image encryption has applications in corporate world, health care, military operations, and multimedia systems. Encryption is a method of transforming original data, called plaintext or cleartext, into a form that appears to be random and unreadable, which is called ciphertext. Plaintext is either in a form that can be understood by a person or by a computer. Once it is transformed into ciphertext neither human nor machine can properly process it until it is decrypted. Decryption is changing it back to its original form. The encryption and decryption block diagram is as shown in Figure 1.

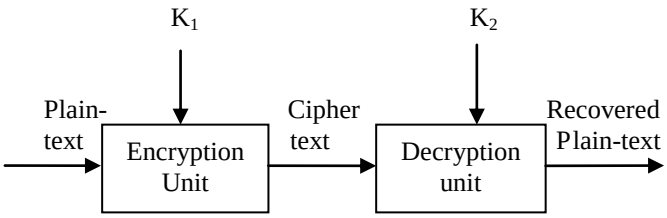


FIGURE 1. BLOCK DIAGRAM OF ENCRYPTION AND DECRYPTION

The original message for encryption is called plaintext, and the encrypted message is called cipher-text, which is denoted here by P and C, respectively [1]. The encryption procedure of a cipher can be described as $C=EK_1(P)$, where K_1 is the key used for encryption process and E(.) is the encryption function. Similarly, the decryption procedure is $P=DK_2$ (C), where K_2 is the decryption key and D(.) is the decryption function. When $K_1=K_2$, the cipher is called a private-key cipher or a symmetric cipher and when $K_1=!K_2$, cipher is called a public-key cipher or an asymmetric cipher [2].

In this paper a comparative study of image encryption and decryption based on chaotic map and BB equation using different adder is proposed.

II. CHAOTIC KEY BASED APPROACH (CKBA)

The common method of protecting the digital documents is to scramble the content so that the true message of the documents is unknown. There are various techniques to achieve this for example compression, digital watermarking, steganography and cryptography. One of the methods used for image Encryption is the chaos based approach. Chaos refers to randomness and it is defined as a study of nonlinear dynamic system. The characteristics of chaos systems are characterized mainly sensitivities to initial conditions and other system parameters. Due to this sensitiveness, the system acts very randomly. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, availability of huge number of variants of chaotic systems, large, complex and numerous possible encryption

keys and simpler design. This promises to provide strong encryption without compromising the usability system in terms of speed and robustness.

Based on chaotic key based approach gray levels of each pixel is xored or xnored to one of the two keys (key 1 and key 2) [3]. This approach has high hardware utilization efficiency, low hardware cost and high computing speed but has increased bit rate and computation time is more. Chaotic key based encryption and decryption process assume that the system security is derived from the fact that a cryptanalyst does not know the encryption system and hence it is very difficult to attack it with knowledge of cipher text alone. Systems that derive their security in this way are not worth very much as sooner or later the system will be known.

The chaotic function that is used is given by

$$X(i+1) = \mu x(i)\,(1-x(i)) \qquad (1)$$

Where $\mu = 3.9$

Figure 2 shows the architecture of the chaotic binary sequence generator (CBSG). It is composed of two multiplier, one subtractor, one dff and one multiplexer. The computation time to generate a chaotic bit string value is assumed to be the time for two multiplications and one multiplexing [3].

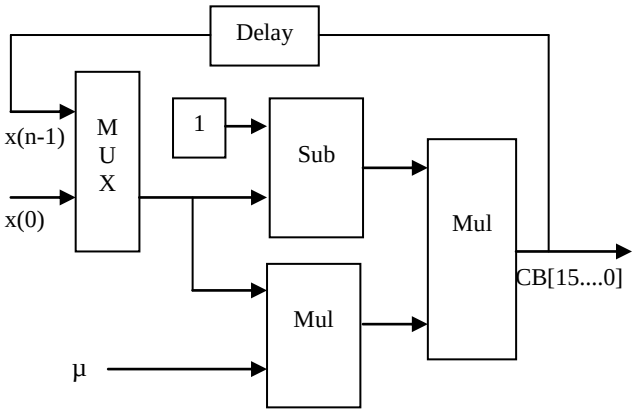


FIGURE 2. ARCHITECTURE OF CBSG

III. BB EQUATION

For the introduction of non linearity in any system we use BB equation. It employs block size that is variable. Fixed key size is not employed and a key of smaller size is employed. The key space is larger. It provides larger key space as the size of key is limited by hardware/software and real time speed considerations. It can potentially employ keys of smaller size as the key is distributed among one primary key p and two secondary keys.

Brahmagupta–Bhãskara (BB) equation is a quadratic Diophantine equation of the form $NX^2+K=Y^2$, where K is an integer and N is a positive integer. A particular case of the BB equation with K = 1 is also known as Pell equation in literature [4]. This equation in the Galois Field GF(p), where p is an odd prime has some practically useful properties.

The BB equation in Galois field GF(p), can be written as:

$$(nx^2+1)_p = (y^2)_p \qquad (2)$$

The subscript p stands for modulo operation by p on the argument values of the expressions.

For obtaining a valid quadratic residues solution of the BB equation in Galois field GF(p), Equation (2) can be written as

$$(nx^2)_p)_p+1 = (y^2)_p$$

This equation can be rewritten as

$$(nq_x+1)_p = (q_y)_p \qquad (3)$$

Where q_x and q_y are the quadratic residues solution of the BB equation in GF(p).

To solve the BB equation, find a possible pair (x,y) so the equation (1) is satisfied for given n and p.

Once x and y are found, and then q_x and q_y are computed as

$$q_x=(x^2)_p,\ q_y=(y^2)_p$$

The encryption process using BB equation is as follows:

1. n corresponds to the plaintext in a block that is being encrypted.
2. p corresponds to the primary secret key used in the encryption of the plaintext in a block.
3. The cipher text corresponding to n is the pair (q_x,q_y) of the corresponding BB equation.

IV. PROPOSED CRYPTOSTSTEM FOR IMAGE ENCRYPTION AND DECRYPTION

The flow chart of the proposed cryptosystem for encryption and decryption is shown in figure 3.Here, for a given primary key p, the root pairs of the BB equation corresponding to each pixel of the image is found. Now the result is XORed or XNORed using the key obtained by chaotic bit sequence.

A. Proposed Encryption Algorithm

The chaotic function that is used is given by

$$X(i+1)=\mu x(i)(1-x(i))$$

Let n denote an image of size M xN pixels and $n(x,y), 0\le x\le M-1, 0\le y\le N-1$, be the gray level n at position (x,y). q_x,q_y are computed using the BB equation [5]. The proposed encryption algorithm is as follows.

Step 1: Choose p, key 1 and key2 and set j=0.

Step 2: Choose the initial point x (0) and generate the chaotic sequence x (0), x (I), x(2), ..., x (MN/16-1) using chaotic sequence generator.

Step 3: For x=0 to M-1
For y=0 to N-1

Obtain $q_x(x,y)$, $q_y(x,y)$ for chosen p and given n(x,y) from the solution of BB equation.

Switch (2xb(j) + b(j+1))

Case 3:

$q_{xe}(x,y) = q_x(x,y) +key1)$

$q_{xe}(x,y) =q_{xe}(x,y)$ XOR key1

$q_{ye}(x,y)= q_y(x,y) +key1$

$q_{ye}(x,y) =q_{ye}(x,y)$ XOR key1

Case 2:

$q_{xe}(x,y) = q_x(x,y) +key1)$

$q_{xe}(x,y) =q_{xe}(x,y)$ XNOR key1

$q_{ye}(x,y)= q_y(x,y) +key1$

$q_{ye}(x,y) =q_{ye}(x,y)$ XNOR key1

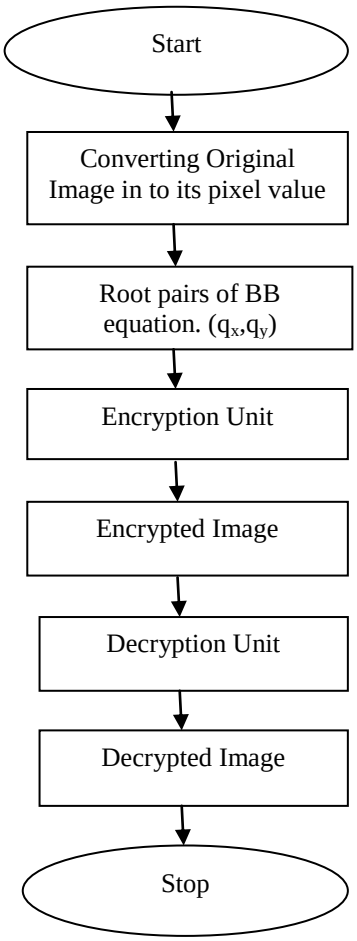


FIGURE 3. FLOW CHART OF THE PROPOSED CRYPTOSYSTEM FOR ENCRYPTION AND DECRYPTION

Case 1:

$q_{xe}(x,y) = q_x(x,y) + key2)$

$q_{xe}(x,y) = q_{xe}(x,y)$ XOR key2

$q_{ye}(x,y) = q_y(x,y) + key2$

$q_{ye}(x,y) = q_{ye}(x,y)$ XOR key2

Case 0:

$q_{xe}(x,y) = q_x(x,y) + key2)$

$q_{xe}(x,y) = q_{xe}(x,y)$ XNOR key2

$q_{ye}(x,y) = q_y(x,y) + key2$

$q_{ye}(x,y) = q_{ye}(x,y)$ XNOR key2

J=j+2

End; End

Step 4: Stop the algorithm when the result q_{xe}, q_{ye} is obtained.

B Architecture of Encryption Process

The hardware architecture of encryption unit is shown in figure 4.The architecture consists of two keys, one for the generation of chaotic bits (CB) and other for encryption or decryption. The equation used for the generation of CB is same as given in equation 1, where the word length of x(0) and μ are 32 bits. The concept of parallel processing is adopted to the encryption and decryption so that 16 data values can be performed at the same time [6]. This architecture consists of one 32 bit parallel in parallel out register, and 16 encryption processing elements (EPEs). The hardware architecture of decryption unit is similar to that of encryption unit except that the EPEs are replaced by decryption processing elements (DPEs) with the encrypted data as the input. Comparison table of different adders used in encryption unit is shown in table1.

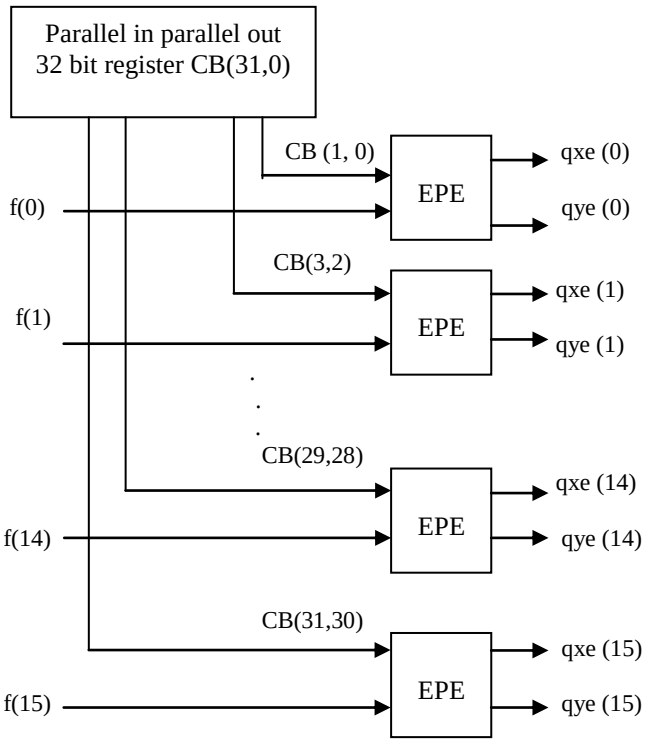


FIGURE 4. ARCHITECTURE OF ENCRYPTION UNIT

The cascade architecture of the Encryption Processing Element (EPE) is shown in Figure 5, which consists of EPE1 and EPE2 units. The architecture of EPE1 is shown in Figure 6 which consists of two multipliers, two mod operators and one comparator. The architecture of EPE2 is shown in Figure 7 which consists of four multiplexers, two adders, two xor gates, two inverters, two serial to parallel converters and four parallel to serial converters.

TABLE 1. COMPARISON BETWEEN DIFFERENT ADDERS

DIFFERENT ADDERS	NO:OF MACROCELLS USED	AREA
Carry Look ahead Adder	9	68.300ns
Carry Select Adder	9	41.900ns
Ripple Carry Adder	8	42.900ns
Kogge-Stone Adder	6	28.700 ns

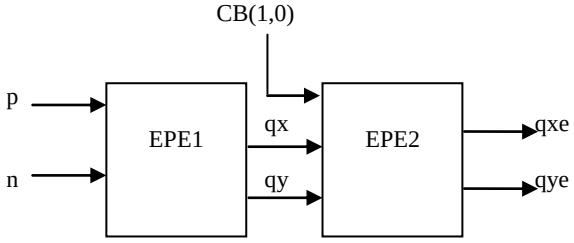


FIGURE 5. CASCADE ARCHITECTURE OF EPE

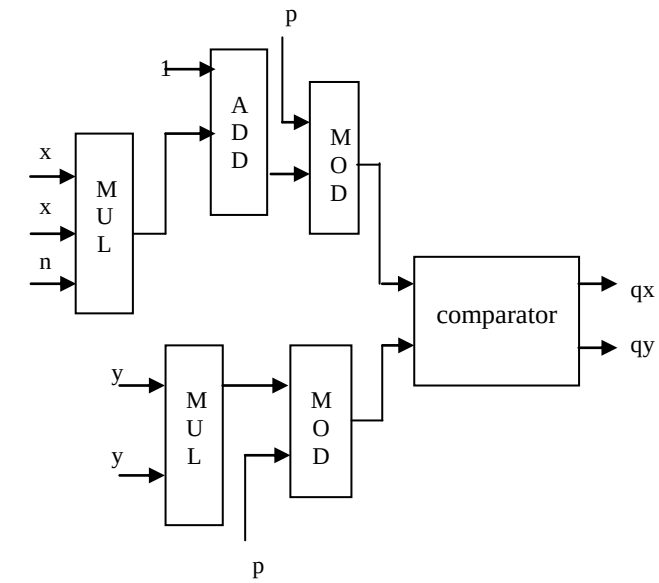


FIGURE 6. ARCHITECTURE OF EPE1

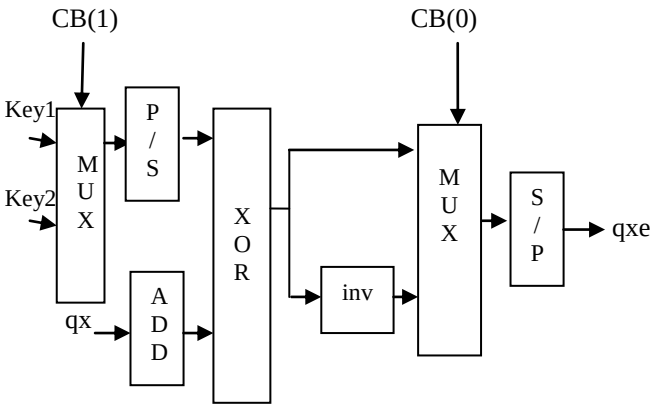


FIGURE 7. ARCHITECTURE OF EPE2

C. Decryption Algorithm

Decryption is the reverse process of encryption, so the exact reverse process is carried out to decrypt the encrypted output[6] [10].

The decryption algorithm is as follows.
Step 1: Choose p, key 1 and key2 and set j=0.

Step 2: Choose the initial point x (0) and generate the chaotic sequence x (0), x (I), x(2), ..., x (MN/16-1) using chaotic sequence generator.The encryption unit is shown in figure 4.

Step 3: For x=0 to M-1
For y=0 to N-1
Obtain $q_x(x,y)$, $q_y(x,y)$ for chosen p and obtained q_{xe} and q_{ye}.
Switch (2xb(j) + b(j+1))
Case 3:
$q_x(x,y) = q_{xe}(x,y)$ XOR key1)
$q_x(x,y) = q_x(x,y)$ - key1
$q_y(x,y) = q_{ye}(x,y)$ XOR key1
$q_y(x,y) = q_y(x,y)$ - key1
$f(x,y) = (q_x(i))^{-1} (q_y(i)-1) \bmod (p)$
Case 2:
$q_x(x,y) = q_{xe}(x,y)$ XNOR key1)
$q_x(x,y) = q_x(x,y)$ - key1
$q_y(x,y) = q_{ye}(x,y)$ XNOR key1
$q_y(x,y) = q_y(x,y)$ - key1
$f(x,y) = (q_x(i))^{-1} (q_y(i)-1) \bmod (p)$
Case 1:
$q_x(x,y) = q_{xe}(x,y)$ XOR key2)
$q_x(x,y) = q_x(x,y)$ - key2
$q_y(x,y) = q_{ye}(x,y)$ XOR key2
$q_y(x,y) = q_y(x,y)$ – key2
$f(x,y) = (q_x(i))^{-1} (q_y(i)-1) \bmod (p)$
Case 0:
$q_x(x,y) = q_{xe}(x,y)$ XOR key2)
$q_x(x,y) = q_x(x,y)$ - key2
$q_y(x,y) = q_{ye}(x,y)$ XOR key2
$q_y(x,y) = q_y(x,y)$ – key2
$f(x,y) = (q_x(x,y))^{-1} (q_y(x,y)-1) \bmod (p)$
J=j+2
End;End
Step 4: Stop the algorithm when the result f is obtained.

D. Architecture of Decryption Process

The cascade architecture of the Decryption Processing Element (DPE) is shown in Figure 8, which consists of DPE1 and DPE2 units. The architecture of DPE1 shown in figure 9 is same as that of EPE2 with qxe and qye as inputs. The architecture of DPE2 is shown in figure 10, which consists of one subtractor, one division block and one mod operation.

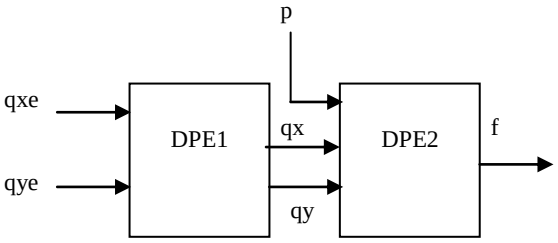


FIGURE 8. CASCADE ARCHITECTURE OF DPE

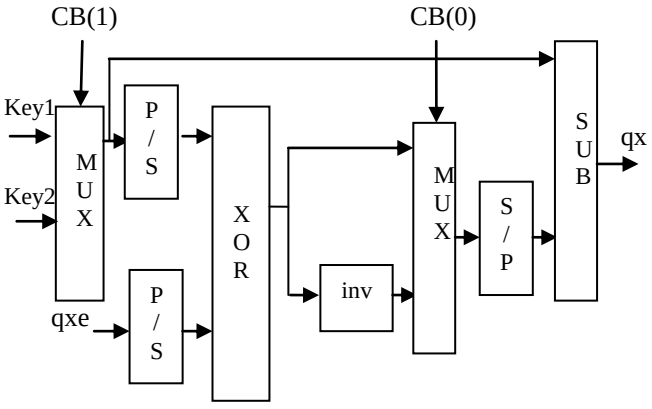


FIGURE 9. ARCHITECTURE OF DPE1

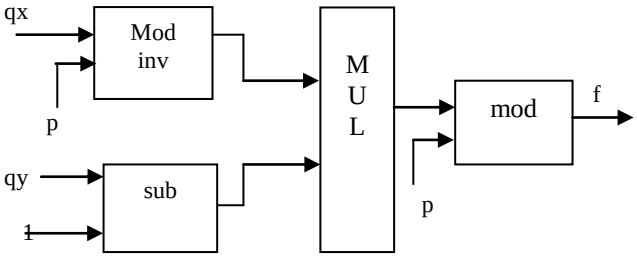


FIGURE 10. ARCHITECTURE OF DPE2

V. SIMULATION RESULTS

A. Converting image in to its pixel value

Convert the image in to its pixel value for providing image as input to the encryption process. For that a 256x256 image is considered and the corresponding pixel matrix (256x256) is obtained using MATLAB.The original image that was used is shown in figure 11(a).

B. Chaotic bit sequence generator

The chaotic signal is used for secure data transmission. The chaotic function that is used is given by equation 1. The function is generated using MATLAB .The output obtained is 1101100011011000. When CB(0)and CB(1) is 00 then case 3 is executed. Similarly for 01 case 2, for 10 case 3 and for 11 case4 is executed.

C. Generation of q_x and q_y

q_x and q_y value is obtained using the BB equation. Initially the x and y values are to be known, for that the BB equation is solved for different values of n.

D. Generation of q_{xe} and q_{ye}

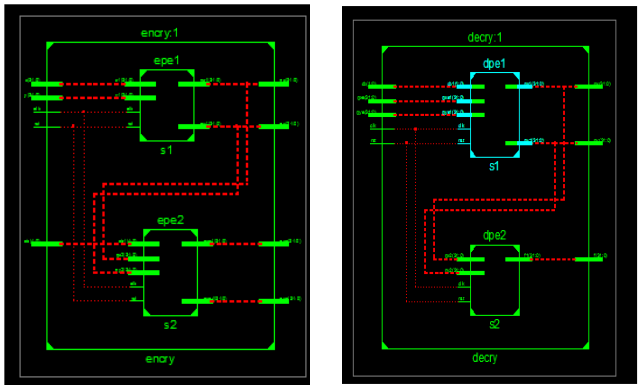
The q_{xe} and q_{ye} values are obtained for various q_x and q_y. As per Figure 6 either of the two keys are selected randomly depending on the CB values and added to the q_x value. The obtained result is again XORed or XNORed with the key selected depending on the CB value. Now the encrypted pixel values are converted into corresponding encrypted using MATLAB. The pixel values are read using MATLAB and the image obtained is as shown in figure 12(b).

(a) Original Image (b) Encrypted Image

FIGURE 11. ENCRYPTION PROCESS

E. Decryption Process

The exact reverse process is carried in order to obtain the decrypted image. For this the encrypted pixels are taken as input and the corresponding qx and qy values are obtained through DPE1. The original pixel value is then obtained through DPE2 unit. The RTL schematic of EPE unit and DPE unit are as shown in figure 12 (a) and (b) respectively.



(a)EPE UNIT (b)DPE UNIT

FIGURE 12. RTL SCHEMATIC OF CRYPTOSYSTEM

VI. CONCLUSION

In this paper, a comparison study between different adders is considered for optimization and hence the image encryption and decryption based on chaotic map and BB equation is designed and relized using XILINX ISE VLSI software and the result is implemented on FPGA.

REFERENCES

[1] K.Sakthidasan, B.v Santhosh Krishna "A New Chaotic Key Based Design for Image Encryption and Decryption of Digital Color Images" A, International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011

[2] Ambika Oad, Himanshu Yadav, Anurag Jain "A Review: Image Encryption techniques and its terminologies", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.

[3] Jui-cheng..Yen and Jiun-In Guo, "A New Chaotic Key Based Design for Image Encryption and Decryption", Proc. IEEE International Symposium on Circuits and Systems, May 28- 31, 2000, Geneva, Switzer; and, vol.IV, pp.49-52.

[4] N.Rama Murthy and M.N.S.Swamy, "Cryptographic Applications of Brahmagupta Bhaskara Equation", IEEE Transactions on circuits -1,Regular papers, vol.53, July2006, pp.1565-1571

[5] Rithmi Mitter, M.Sridevi Sathya Priya, "A Non Linear Equation Based Cryptosystem for Image Encryption and Decryption", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[6] K.Dheergha Rao and Ch.Gangadhar, "Modified Chaotic Key Based Algorithm for Image Encryption and its VLSI Realization," IEEE International conference on Digital Signal Processing (DSP-2007), July1-4, 2007, Cardiff, Wales, U.K, pp.439-442.

[7] G.Alvarez,L.H.Encinas, and I.M.Masque,"Known-plaintext Attack to Two Cryptosystems Based on the BB equation", IEEE Transactions on Circuits and Systems II: Express briefs volume 55,Issue 5,May 2008 page(s) :423-426.

[8] S.I.Li and X.Zheng, "On the security of an image encryption method," Proc. IEEE International Conference on Image Processing (ICIP2002), vol.2, pp.925-928, 2002

[9] G.Alvarez, F.Montoya, M.Romera, and G.Pastor, "Cryptanalysing a discrete time chaos synchronization secure communication systems," Chaos, solutions and fractals, 2003,vol.21,no.3,pp.689-694.

[10] K Dheerga Rao,K.Pravween Kumar, and P.V.Muralikrishna, "A New and Secure Cryptosystem for Image Encryption and Decryption", appear in IETE Journal of Research, March-Apr.2011.