Design and Implementation of Highly Secure Cryptosystem for Image Encryption

Suvarna.M, Prabhavathi.K, M.B.Anandaraju, Nuthan.A.C

Abstract— Chaos based encryption may offer new quality in secure data transmission. Recently proposed chaotic key based algorithms are found to be more susceptible to the known plain text attacks and cipher text attacks. In this paper BB (Brahmagupta-Bhaskara) equation is combined with chaos to give a non linear dependency and thus improved security. The proposed algorithm is designed and realized using MATLAB and Xilinx ISE software.

Keywords— Chaotic map, Security, BB equation, Image encryption.

I. INTRODUCTION

The field of encryption is becoming very important in the present era. Digital image security is of utmost concern as web attacks have become more and more serious. In order to transport a digital data over an unsecured communication channel or media (that is, a channel that does not guarantee inaccessibility to an eavesdropper or a cryptanalyst), encryption techniques are used. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Many image content encryption algorithms have been proposed [1]. Many among these are chaotic based [2-3] algorithms since chaotic system properties such as aperiodicity, sensitivity to initial conditions and system parameters are preferred. However, the encryption techniques based on chaos map was found to be insecure [5-6]. Brute Force Attack is the method of breaking a cipher by trying every possible key [7]. Recently, a cryptosystem based on BB (Brahmagupta Bhaskara) equation is proposed but is vulnerable to known plaintext attacks. Cryptographic application of BB Equation employs block size that is variable [8]. Also keys are of fixed size. 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 [9]. In the absence of any proofs the algorithms based on BB equation remains as one more addition to the so called "believed to be secure" class of algorithms. Attacks require as low as three known plaintext cipher text pairs to fully recover the secret key[10]. Hence a highly secure image encryption algorithm is developed by combining both chaos and BB equations together.

However, the key space of this algorithm depends strictly on system precision. For a high precision system the key space is large enough to resist brute force attack, but if the system is applied in a low precision system the key space becomes too small. Besides, the technique is insecure against chosen plaintext are proposed to enhance security of this technique. The improved technique has variable space, which is independent of system precision, and has high security.

The Brahmagupta–Bhãskara equation [11]–[14] is a quadratic Diophantine equation of the form

$$NX^2 + k = Y^2$$

where k is an integer (positive or negative) and integer such that √N is irrational. A particular case of the above BB equation with $k=1$ given below

$$NX^2 + 1 = Y^2 \qquad (1)$$

Is also known as Pell equation in the literature [15]–[19].We refer to a pair of positive integers X_i and Y_i $(i.e., X_{i,} Y_i \in Z_+)$ satisfying the above equation as its "root." Of particular interest to this paper (which is concerned with its application to the field of cryptography) are the properties of the BB equation in the finite field *GF(P)*

Where *P* is an odd prime. Towards the development in this direction let the notation $\langle r \rangle_m$ denote the least positive (or nonnegative) remainder of *r* modulo *m* with this notation, the BB equation in (1) takes the form

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

Where $n = \langle N \rangle_P$ and $1 \le n \le (p-1).$ We refer to (2) as BB equation in *GF(p)*.A pair of integers x_i and y_i in *GF(p)* with $1 \le x_i, y_i (p-1)$ satisfying the (2) denoted as (x_i, y_i) is referred to as its root. Clearly, $x_i = \langle X_i \rangle_p$ and $y_i = \langle Y_i \rangle_p$. In this paper, relevant properties of BB equation in GF(p) and their practical application in the two fields of cryptography are discussed.

II. PROPERTIES OF BB EQUATION IN GF (P)

Following observations of interest to this paper can now be Made with respect to BB equation in GF(*p*).

1) (0,1) is a trivial root. So is (0, p-1). (0, 0) cannot be a root A root cannot be of the form (0, j) where $2 \le j \le (p-2)$ as this would imply that 1 is quadratic residue for all these values of j. Hence, the number of nontrivial roots "r" is less than $(p^2 - p)$. It can be shown that the total number of nontrivial roots is exactly (p -3) if n is a quadratic residue and (p-1) if n is a non residue of p [6].

2) Given a root of the equation and the value of p, it is possible to determine uniquely the value of n. Example 1: Given (4,3) as a root in GF(11). We have $5n + 1 \equiv 9 \bmod 11$ or

Manuscript received June, 2013.

Suvarna. M, PG Student, VLSI Design and Embedded System, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Prabhavathi.K, Assistant Professor, Department of Electronics and Communication Engineering, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Prof. M.B.Anandaraju, Professor and HOD, Department of Electronics and Communication Engineering, B.G.S. Institute of Technology, B.G.Nagar, Mandya-571448, Karnataka, India.

Nuthan.A.C, Assistant Professor, Department of Electronics and Communication Engineering, G. Madegowda Institute of Technology, Bharathinagara, Mandya-571422, Karnataka, India.

equivalently $5n \equiv 8 \bmod 11$. n Can be computed by solving the condition that $n < 11$. We get $n = 6$ (for $k = 2$).

3) For $0 < n_{1,} n_2 < P$ and $n_1 \neq n_2$, equations $\langle n_1 x^2 + 1\rangle_p$ do not share common root(s).This is due to fact that the roots of $\langle n_1 x^2 + 1\rangle_p = \langle y^2\rangle_p$ and $\langle n_2 x^2 + 1\rangle_p = \langle y^2\rangle_p$ are obtained from modulo *P* of roots of $N_1 X^2 + 1 = Y^2$ and $N_2 X^2 + 1 = Y^2$ respectively, where $N_1 = n_1 + k\cdot p, N_2 = n_2 + k \cdot p$ and $k = 0,1,2,3,\ldots\ldots.$ when $N_1 \neq N_2$ the roots of $N_1 X^2 + 1 = Y^2$ and $N_2 X^2 + 1 = Y^2$ are differ rent and result follow. Conversely if (x_1, y_1) is a root of both $\langle n_1 x^2 + 1\rangle_p = \langle y^2\rangle_p$ and $\langle n_2 x^2 + 1\rangle_p = \langle y^2\rangle_p$ then $\langle n_1 x_1^{\ 2} + 1\rangle_p = \langle y_1^{\ 2}\rangle_p$ and $\langle n_2 x_1^{\ 2} + 1\rangle_p = \langle y_1^{\ 2}\rangle_p$ .This implies that $(n_1 - n_2)_p \langle x_1^2\rangle_p = (0)_p$. Since $\langle x_1^2\rangle_p$ cannot be as explained in paragraph 1 above, $n_1 = n_2 + k_{p.}$

III. COMPUTATION OF A ROOT IN GF (P)

For obtaining the roots of BB equation in GF(*p)*, we rewrite it as (3)

$$\left\langle n \left\langle x^2 \right\rangle_p \right\rangle_p + 1 = \left\langle y^2 \right\rangle_p$$

Let $q_1, q_2, q_{3,\ldots\ldots,} q_{(p-1)/2}$ be the quadratic residues [15], [19], [20] in GF(*p*). Further, let .$q_0=0$

Since $\langle x^2\rangle_p = q_i$ $\langle y^2\rangle_p = q_j$ and (3) reduces to

$$\left\langle \langle n q_i\rangle_p + 1 \right\rangle_p = q_j \tag{4}$$

Let $\langle q_i - 1\rangle_p = Q_j$ so that above equation becomes

$$\langle n \cdot q_i\rangle_p = Q_j \tag{5}$$

For a given p,q_i and Q_j (for i, j=0,1,2,…,(p-1)/2) are known a priori. The problem is to determine ($q_{i,}$ $Q_{j)}$ so that (5) is satisfied for a given n. Once q_i and Q_j satisfying (5) are found, a root of (2) will be (a,b) where a is $\sqrt{q_i}$ mod p, and b is $\sqrt{(Q_j+1)}$ mod p. Depending on q_i on the left-hand side and Q_j on the right hand side,(5) represents a set of congruence's. The number of congruence's is ((p-1)/2+1)*((p-1)/2+1) that is $(p+1)^2/4$.Each of these congruence's has a solution *iff*

$$\gcd(n,p)|Q_j.$$

Since gcd(n,p)=1, the solution is unique mod p. Let η represent the inverse of n in , that is n.η≡ 1 mod p. Then, one can successively compute $Z_j=(\eta.Q_j)$ mod p (for j=0,1,2,…,(p-1)/2) and at each stage find out if Z_j is a quadratic residue in p. This can be done by sequentially comparing Z_j with the entries in a table containing all precomputed values of g the quadratic residue modulo p. This table will have (p-1)/2+1=(p+1)/2 entries including the trivial quadratic residue of 0. In situations where it is not feasible to provide this table, one can generate its entries through the computation of g^{2n} mod p where g is the primitive in and n=0,1,2,….Alternatively, one can use Euler's criterion to test if z_j is a quadratic residue. If z_j is a quadratic residue, then further computations of z_j are abandoned and the desired a and b are obtained as

$$a = \sqrt{z_i} \bmod p \text{ and } b = \sqrt{(Q_j + 1)} \bmod p$$

IV. ALGORITHM

The chaotic function that is used is given by

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

Where $\mu = 0.39$

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 (x,y). q_x,q_y are computed using the BB equation. A non linear operation (mod operation) on the added value of qx, qy and key is performed.

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

Step 2: chose the initial point x (0) and generate the chaotic sequence using chaotic sequence generator. Binary sequence is generated using binary sequence generator. The encryption unit is as shown in figure 1.

```
Step 3: For x=0 to M-I
          For y=0 to N-I
Obtain $q_x(x,y)$, $q_y(x,y)$ for chosen p and given f(x,y) from the solution of BB equation as shown in figure 3.
Case 3:
$q_{xo}(x,y) = mod((q_x(x,y)+key 1), 2^{n-1})$
$q_{xo}(x,y) = q_{xo}(x,y)$ XOR key 1
$q_{yo}(x,y) = mod((q_y(x,y)+key 1, 2^{n-1})$
$q_{yo}(x,y) = q_{yo}(x,y)$ XOR key 1

Case 2:
$q_{xo}(x,y) = mod((q_x(x,y)+key 1), 2^{n-1})$
$q_{xo}(x,y) = q_{xo}(x,y)$ XNOR key 1
$q_{yo}(x,y) = mod((q_y(x,y)+key 1, 2^{n-1})$
$q_{yo}(x,y) = q_{yo}(x,y)$ XNOR key 1

Case 1:
$q_{xo}(x,y) = mod((q_x(x,y)+key 2), 2^{n-1})$
$q_{xo}(x,y) = q_{xo}(x,y)$ XOR key 2
$q_{yo}(x,y) = mod((q_y(x,y)+key 2, 2^{n-1})$
$q_{yo}(x,y) = q_{yo}(x,y)$ XOR key 2

Case 0:
$q_{xo}(x,y) = mod((q_x(x,y)+key 2), 2^{n-1})$
$q_{xo}(x,y) = q_{xo}(x,y)$ XNOR key 2
$q_{yo}(x,y) = mod((q_y(x,y)+key 2, 2^{n-1})$
$q_{yo}(x,y) = q_{yo}(x,y)$ XNOR key 2
J – j+2
End;End
```

Step 4: The result $qx_o(x,y)$, $qy_o(x,y)$ is obtained as shown in figure 4 and stop the algorithm. The basic criterion to select key1 and key 2 is

$$\sum_{i=0}^{m-1} a_i \text{ xor } d_i = m/2$$

Where Key 1 = $\sum_{i=0}^{m-1} a_i \times 2^i$

Key 2 = $\sum_{i=0}^{m-1} d_i \times 2$

V. ARCHITECTURE OF THE ENCRYPTION UNIT

The architecture consists of two key modules, one for the generation of chaotic bits (CB) and the other for encryption or decryption. The equation to generate CB is same as given in equation 3. The word length of x(0) and μ are 32 bits. The concept of parallel processing is taken to the encryption and decryption so that 16 data values can be performed at the same time. Figure 1 shows the hardware architecture of the encryption unit. This architecture consists of one 32 bit parallel in parallel out register, and 16 encryption processing elements.

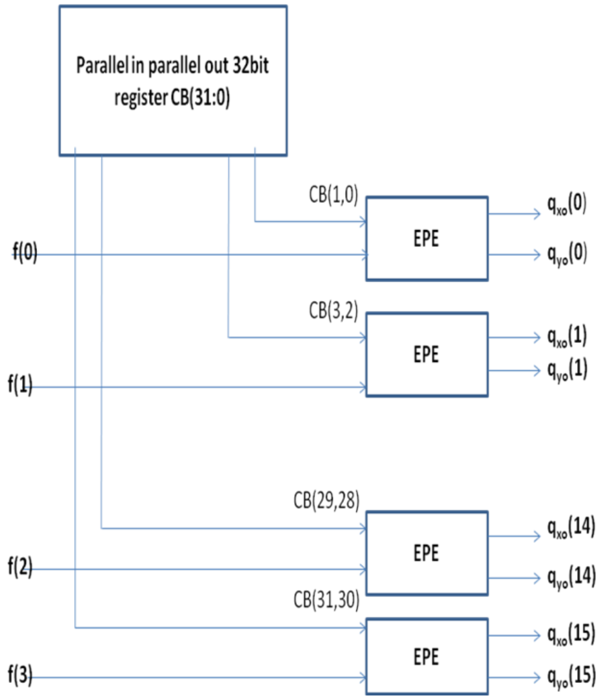


Figure 1 Architecture of Encryption Unit

The cascade architecture of the Encryption Processing Element (EPE) is shown in figure 2. The architecture of EPE 1 is shown in figure 3 which consists of three multipliers, one adder, two mod operators and one comparator. The architecture of EPE2 is shown in figure 4 which consists of four data multiplexers, two adders, two xor gates, two MOD operations, and two inverters, four parallel to serial converters, and two serial to parallel converters.

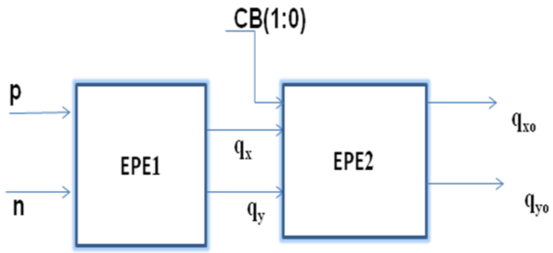


Figure 2 Cascaded architecture of EPE

A. Generation a of Chaotic Binary Sequence

The chaotic signal is used for secure data transmission The chaotic function that is used is given by equation 3. The function is generated using MA TLAB with the help of 'seqgen' function. The output obtained is 1101100011011000. When CB(0)and CB(1) is 00 then case 3 is executed. Similarly for 01 case2, for 10 case1 and for 11 case0 is executed. These 32 bits i.e. two bits each is one of the inputs to the 16 EPEs used in the encryption process. In order to reduce the execution time chaotic circular shift is used for generating the chaotic binary sequence, thus improving speed. Figure 5 shows the binary sequence generator used so that the key space is independent of processors. Here, register r_i store wxp bits, p is the computing precision used in logistic mapping and w is a parameter used to control key space. The Logistic mapping is the same as equation (3) and the discretization rule is given as equation (5)

$$a_i = 1(x_i > 0.5)$$
$$0(x_i < 0.5)$$

B. Generation of q_x and q_y

The BB equation is used to find q_x and q_y values. Initially the x and y values are to be known, for that the BB equation is is solved for different values of n. The n value corresponds to the each and every pixel value obtained after conversion of image. Hence for various n(x,y),0 ≤ x ≤ M-1,0 ≤ y ≤ N-1,be the gray level n at (x,y) qx, qy are computed using the BB equation.

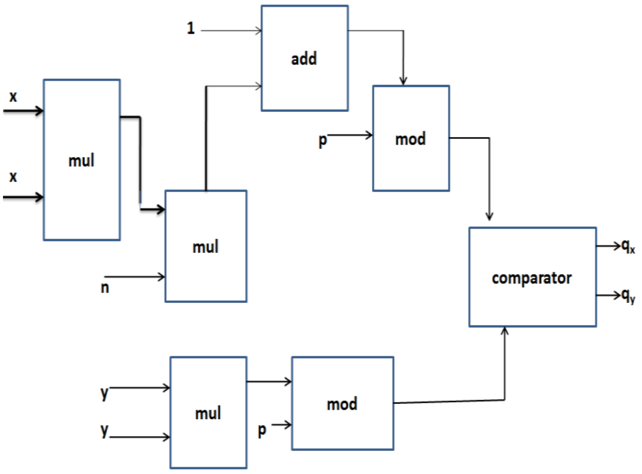


Figure 3 Architecture of EPE1

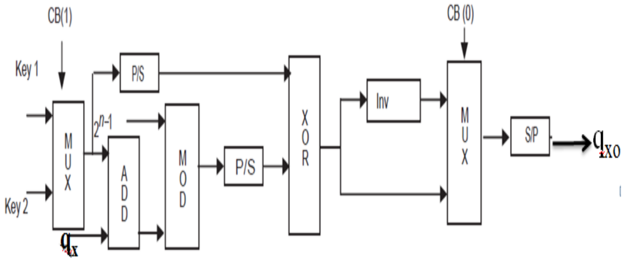
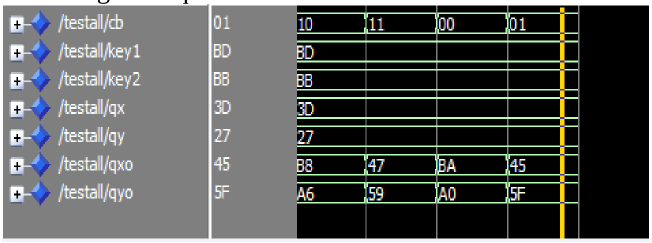


Figure 4 Architecture of EPE2

VI. SIMULATION RESULTS

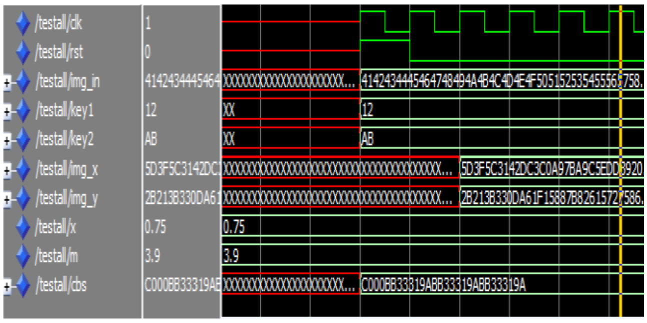
The entire architecture is modeled using VHDL. The coding is done on Xilinx ISE13.2 on Spartan 3. Simulation can be done using ModelSim SE 6.3f simulator.

Figure 5, Figure 6, shows the simulation result of encrypted data using BB Equation.



```
/testall/cb    01  10  11  00  01
/testall/key1  BD  BD
/testall/key2  BB  BB
/testall/qx    3D  3D
/testall/qy    27  27
/testall/qxo   45  B8  47  BA  45
/testall/qyo   5F  A6  59  A0  5F
```

Figure 5 Simulation result of Encrypted Data obtained from EPE2



```
/testall/clk     1
/testall/rst     0
/testall/img_in  414243444546 4  XXXXXXXXXXXXXXXXXXXXXX...  4142434445464748494A4B4C4D4E4F505152535455565758.
/testall/key1    12              XX                           12
/testall/key2    AB              XX                           AB
/testall/img_x   5D3F5C3142DC1   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX...  5D3F5C3142DC3C0A97BA9C5EDD3920.
/testall/img_y   2B213B330DA61   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX...  2B213B330DA61F15887B8261572 7586.
/testall/x       0.75            0.75
/testall/m       3.9             3.9
/testall/cbs     C000BB33319AE   XXXXXXXXXXXXXXXXXXXXXX...  C000BB33319ABB33319ABB33319A
```

Figure 6 Simulation result of encrypted data using BB Equation.

VII. CONCLUSION AND FUTURE WORK

In this paper, a secure Cryptosystem based on the BB equation and chaos is proposed for image encryption. The values are generated in Xilinx ISE and the RTL schematic of EPE unit is obtained. In future the exact reverse process shall be carried out to decrypt the encrypted data. The proposed cryptosystem is illustrated with implementation results, from the results, it is concluded that the proposed Cryptosystem is effective for secure data encryption

REFERENCES

[1] P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications', IEEE Transactions on Consumer Electronics,

[2] 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 2S-31, 2000, Geneva, Switzer; and, vol.IV, pp.49-52..

[3] L.H. Zhang, X.F. Liaom and X.B. Wang, "An Image Encryption Approach Based on Chaotic maps", Chaos, Solitons and Fractals, vo1.24, pp.759-765, may 2005.

[4] SJ. Xu, Y.L. Wang, J. Z. Wang and M.Tian, "Cryptanalysis of TwoChaotic Image Encryption Schemes Based on Permutation and XOR operations", 200S International Conference on Computational Intelligence and Security, voI.2,pp.433-437, Dec.200S.

[5] M.I. Sobhy, and A.R.Shehata,"Methods of attacking chaotic encryption and countermeasures,"Proc.lEEE International ConfAcoustics, Speech, and signal processing (ICASSP 200 I), vol.2, pp.1001-1004.

[6] S.I.Li and X.Zheng,"Cryptanalysis of a Chaotic Image encryption Method", IEEE International Symposium on circuits and Systems (ISCAS 2002), voL2, pp.708-7II, 2002.

[7] G.Alvarez, F.Montoya, M.Romera, and G. Pastor, "Cryptanalysing a discrete time chaos synchronization secure communication systems," Chaos, Solitons and fractals, 2003, voL2I, no.3, pp.689-694.

[8] N.Rama Murthy and M.N.S.Swamy,"Cryptographic Applications of Brahmagupta Bhaskara Equation", IEEE Transactions on circuitS-I, Regular papers, voL53, July2006, pp.I565-I571.

[9] A.M. Youssef, A comment on "Cryptographic applications of Brahmaguptha Bhaskara equation, IEEE Trans.Circuits Syst, 1, Reg papers, voL54, no.4, pp.927-928.

[10] G. Alvarez, L.H. Encinas, and J.M. Masque, "Known Plaintext Attack To Two Cryptosystems Based On The BB Equation", IEEE Transactions on Cicuits and Systems II: Express Briefs Volume 55, Issue 5, May 2008 page(s): 423-426.

[11] B. Dutta and A. N. Singh, *History of Hindu Mathematics: A Source Book*. Bombay, India: Asia Publishing House, 1962.

[12] M. N. S. Swamy, “Brahmagupta’s theorems and recurrence relations,”*The Fibonacci Fibonacci Quarterly*, vol. 36, no. 2, pp. 125–128, May 1998.

[13] T. S. Bhanu Murthy, *A Modern Introduction to Ancient Indian Mathematics*. New Delhi, India: Wiley Eastern Ltd., 1994.

[14] L. E. Dickson, *History of the Theory of Numbers*. NewYork: Chelsea, 1952, vol. II, ch. XII, p. 341.

[15] M. R. Schroeder, *Number Theory in Science and Communication*, Second Enlarged Edition ed. New York: Springer-Verlag, 1990, pp.201–202.

[16] N. R. Murthy and M. N. S. Swamy, “On the Solutions of the Congruences $nx^2 \pm 1 \equiv y^2 (\bmod p)$,” , to be published.

[17] S. Barnard and J. M. Child, *Higher Algebra*. London, U.K.:Macmillan and Co, 1960, ch. XXXIII, p. 535.

[18] G. Chrystal, *Algebra—An Elementary Text-Book, Part II*. New York:Dover, 1961, ch. XXXIII, pp. 478–479.

[19] R. A. Mollin, *Fundamental Number Theory with Applications*. Boca Raton, FL: CRC, 1998, p. 102.

[20] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source code in C*. New York: Wiley, 1996.

Suvarna.M pursuing 4th semester M.Tech VLSI Design and Embedded System in B.G.S. Institute of Technology, B.G.Nagar, Mandya, Karnataka, India. She completed her B.E. from Karnataka in 2011. Her area of interest includes Cryptography, Embedded system, Low power VLSI and Image Processing.