Implementation of Chaotic based Image Encryption Algorithm with the application of Bhramgupta-Bhaskara equation

Sanjay.R.chaudhari, Prof. Himanshu Arora, Prof. Dipak Dembla

Abstract— **Cryptography is just about presence of an adversary. It encompasses many problems like encryption, authentication, and key distribution to name a few. The field of modern cryptography provides a theoretical foundation based on which one can understand what exactly these problems are, how to evaluate algorithm that purport to solve them and how to build algorithm in whose security one can have confidence.**

Advanced digital technologies have made multimedia data widely available. Recently, multimedia applications become common in practice and thus security of multimedia data has become main concern.

The basic issues pertaining to the problem of encryption has been discussed and also a survey on image encryption techniques based on chaotic schemes has been dealt in the present communication. The chaotic image encryption can be developed by using properties of chaos including deterministic dynamics, unpredictable behavior and non-linear transform. [3].Generally chaotic based cryptography is not suitable for practical application [1][3]. It does not secure algorithm due to dependency of initial condition, which can be easily broken. So this algorithm optimize by using (Brahmagupta-Bhaskara) equation for finding out the roots of pixel values. This gives unique values for different pixels. This concept leads to techniques that can simultaneously provide security functions and an overall visual check, which might be suitable in some applications. Digital images are widely used in various applications, that include military, legal and medical systems and these applications need to control access to images and provide the means to verify integrity of images [3]. This algorithm proved insecure against plain-text attack by brute force way of an attack [3].this problem subsequently resolve in [10].

Index Terms— **BBequation, Chaos, Cryptography, Image encryption, Image Decryption.**

I. INTRODUCTION

The major concern while transmitting signals is the security. The security concerns are growing due to illegal data access. To protect the valuable information in many applications like medical imaging, military image database, communications and confidential video conferencing, there is a need to secure the images by the use of encryption and decryption algorithms. In such a scenario, to avoid information leakage to both active and passive attackers, encryption of the medical images is very important [4].

The chaotic based image encryption can be developed by using properties of chaos including deterministic dynamics, unpredictable behavior and non-linear transform. Generally chaotic based cryptography is not suitable for practical application. It does not secure algorithm due to dependency of initial condition [1-3]. It can be easily broken. So this algorithm is optimized by using BB (Brahmagupta-Bhaskara) equation for finding out the roots of pixel values [4]. This gives unique values for different pixels.To deal with the technical challenges, the two major image security technologies are under use: (a) Image encryption techniques to provide end-to-end security when distributing digital content over a variety of distributions systems, and (b) Watermarking techniques as a tool to achieve copyright protection, ownership trace, and authentication. In this paper, the current research efforts in image encryption techniques based on chaotic schemes are discussed.

II. AN IMPLEMENTATION OF CHAOTIC BASED CRYPTOGRAPHY

A Introduction

. One of the fundamental principles of chaotic systems is sensitive dependence or sensitivity to initial conditions [4]. Sensitive dependence is a very valuable property for cryptographic algorithms because one of the desired features of a cryptographic algorithm is that if the initial conditions used to encrypt data are changed by just a small amount, one bit for instance, the encrypted text would be widely different [5]. The chaotic function that is used is the well-known equation is $Xc(i+1) = \mu\, Xc(i)\,(1 - Xc(i))$ ------------------- (1) When $\mu=3.9$, the logistic map exhibits chaotic behavior, and hence the property of sensitive dependency. The map is one dimensional, which is good because it generates scalars to do the encryption and the chaotic properties of the logistic map are well known.

B Proposed Cryptosystem for Encryption and Decryption

The block diagram of the proposed cryptosystem for encryption and decryption is shown in figure 1. In this cryptosystem, for a given primary key p, the root pairs of the BB equation corresponding to each pixel of the image are found [4]. Then, according to a binary sequence generated from a chaotic system, a mod operation is performed on the root pair of the BB equation corresponding to each pixel and

Manuscript received April 30, 2013

Sanjay.R.chaudhari, Computer Science Engineering, AIET College, jaipur, Rajasthan, India, Phone/ Mobile No. 09824016586.

Prof. Himanshu Arora, Computer Science Engineering AIET College, jaipur, Rajasthan, India, Phone/ Mobile No 09982621591.

Prof. Dipak Dembla, Computer Science Engineering AIET College, jaipur, Rajasthan, India, Phone/ Mobile No. 095294082.

each root is XORed or XNORed bit-by-bit to one of the two predetermined keys, key1 and key2.

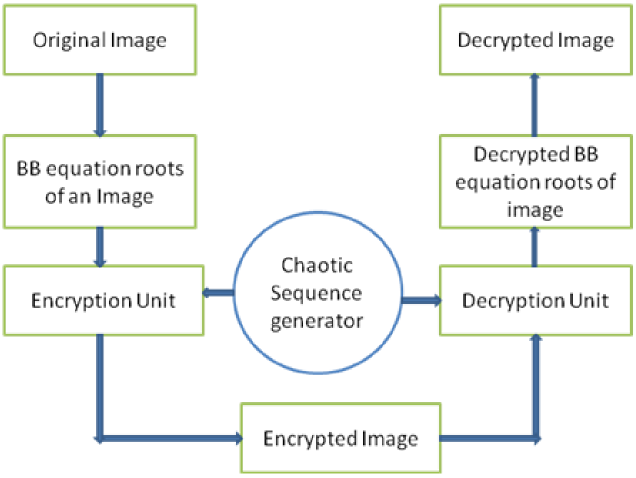
Original Image
Decrypted Image
BB equation roots of an Image
Decrypted BB equation roots of image
Chaotic Sequence generator
Encryption Unit
Decryption Unit
Encrypted Image

Fig-1 Block Diagram of Proposed Encryption algorithm

The chaotic function that is used is the well-known logistic map given in equation (1) with μ = 3.9. Let f denote an image of size MxN pixels and f(i,j), 0<i<M-1, 0<i<N-1 be the gray level of f at position (i,j). The encryption algorithm for the proposed cryptosystem is as follows.

C Chaotic system Using B.B Equation.

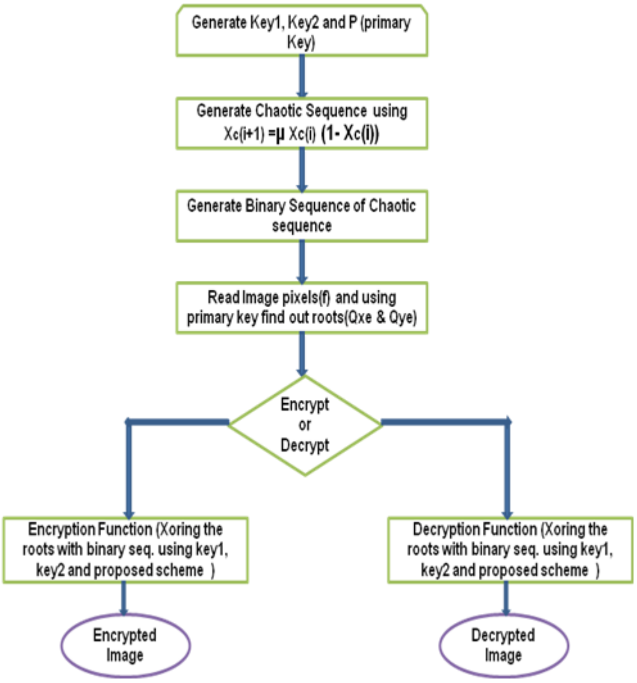
Generate Key1, Key2 and P (primary Key)
Generate Chaotic Sequence using Xc(i+1) =μ Xc(i) (1- Xc(i))
Generate Binary Sequence of Chaotic sequence
Read Image pixels(f) and using primary key find out roots(Qxe & Qye)
Encrypt or Decrypt
Encryption Function (Xoring the roots with binary seq. using key1, key2 and proposed scheme)
Decryption Function (Xoring the roots with binary seq. using key1, key2 and proposed scheme)
Encrypted Image
Decrypted Image

Fig-2 Flow Chart of Proposed Encryption algorithm.

In this Algorithm Flow chart it has shown process of encryption and decryption. First step is to generate the primary key, Key1, Key2. Then it will generate the chaotic sequence (chaotic variables) Using equation.x_c (i+1) =μx_c (i) (1-x_c (i)) (2) Second step is to convert the chaotic sequence to binary sequence. It generates 32 bits for every chaotic variable. Third step is to read the values of pixels and using keys it Find out the roots. So finally BB equation is $\{f_x{}^2+1\}_p=\{y^2\}_p$ (3)

The subscript p stands for modulo operation by p on the argument values of the expressions. For obtain a valid quadratic residues solution of the BB equation. Now equation (3) can be written as $\{f(_x{}^2)_p\}_p+1=\{y^2\}_p$ (4)
Equation (4) can rewritten as $\{fq_x+1\}_p=\{q_y\}_p$ (5)
Where q_x and q_y are the quadratic solution of the BB equation. To solve the BB equation finds a possible pair (x, y) so that equation (3) is satisfied for given f and p.Fourth step is to decide either it has to encrypt or decrypt the data. Then it calls the encryption function or decryption function. And it performs encryption.TheBrahmagupta–Bhãskaraequation is a quadratic Diophantine equation of the form
$N*X^2+k=Y^2$ (6)
Where is an integer (positive or negative) and N is a positive integer such that √N is irrational. A particular case of the above BB equation with k = 1 given below $N*X^2+1=Y^2$ (7)
is also known as Pell equation in the literature. We refer to a pair of positive integers X_i and Y_i (i.e. $X_{i,}$ Y_i € 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 $\{r\}_m$ denote the least positive (or nonnegative) remainder of modulo m, in GF (p). With this notation, the BB equation in (1) takes the form $(n*x^2+1)_p= (y^2)_p$ [4] (8)
Where n = $\{N\}_p$ and 1≤ n ≤ (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 0 < x_i, y_i < (p-1) satisfying the (2) denoted as (x_i, y_i) is referred to as its root. Clearly, $x_i = \{X_i\}_p$ and $y_i = \{Y_i\}_p$.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 ≤ j ≤ (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 quadratic non residue of p.2) Given a root of the equation and the value of p, it is possible to determine uniquely the value of n. 3) For 0 < n1, n2 < p and n1 ≠ n2, equations {n1*x2 + 1} p = {y2} p do not share common root(s). The BB equation can be written for key k=1 $N*X^2+k=Y^2$

III. PROPOSED CRYPTOGRAPHY ALGORITHM

A The Proposed Encryption algorithm

1 Choose Key1 (8 bit), Key2 (8 bit), P (Primary Key of 8 bit) and set l

2 Choose the Initial point Xc (0) and generate the chaotic sequence Xc (1), Xc (2), Xc (3),……… Xc (MN) using equation

Xc (i+1) =µXc (i) (1-Xc(i)) (2)

Then generate binary sequence using scheme b (32i+0), b (32i+1), b (32i+2),………. b (32i+3) and it is binary representation of chaotic scheme.

3 Generate the roots Qx(i,j) & Qy(I,j) for each pixel Using B.B equation for root finding.

4 Encryption Process

```
        Switch (2xb (1) +b (1+1))
        Case 3: Qxe(i,j) = mod(Qx(i,j)+key1)
          Qxe(i,j) = Qxe(i,j) XOR key1
                 Qye(i,j) = mod(Qy(i,j)+key1)
          Qye(i,j) = Qye(i,j) XOR key1
        Case 2:  Qxe(i,j) = mod(Qx(i,j)+key1)
          Qxe(i,j) = Qxe(i,j) XNOR key1
                 Qye(i,j) = mod(Qy(i,j)+key1)
          Qye(i,j) = Qye(i,j) XNOR key1
        Case 1:  Qxe(i,j) = mod(Qx(i,j)+key2)
          Qxe(i,j) = Qxe(i,j) XOR key2
                 Qye(i,j) = mod(Qy(i,j)+key2)
          Qye(i,j) = Qye(i,j) XOR key2
        Case 0:  Qxe(i,j) = mod(Qx(i,j)+key2)
          Qxe(i,j) = Qxe(i,j) XNOR key2
                 Qye(i,j) = mod(Qy(i,j)+key2)
          Qye(i,j) = Qye(i,j) XNOR key2
```

5 Finally it generates two encrypted images (Qxe & Qye).

B *The Proposed Decryption algorithm*

1 Same as Encryption Algorithm

2 Same as Encryption Algorithm

3 Get the values of Qxe(i,j) & Qye(I,j) for each pixel from two encrypted images.

4 Decryption Process

```
        Switch (2xb(1)+b(1+1))
        Case 3:    Qx(i,j) = Qxe(i,j) XOR key1
          Qx(i,j) = mod(Qxe(i,j)+key1)
                  Qy(i,j) = Qye(i,j) XOR key1
          Qy(i,j) = mod(Qye(i,j)+key1)
                f(i,j) = $(Qx(I,j))^{-1}$ (Qy(I,j)-1) mod P
        Case 2:  Qx(i,j) = Qxe(i,j) XNOR key1
          Qx(i,j) = mod(Qxe(i,j)+key1)
                 Qy(i,j) = Qye(i,j) XNOR key1
          Qy(i,j) = mod(Qye(i,j)+key1)
                f(i,j) = $(Qx(I,j))^{-1}$ (Qy(I,j)-1) mod P
       Case 1:     Qx(i,j) = Qxe(i,j) XOR key2
          Qx(i,j) = mod(Qxe(i,j)+key2)
                   Qy(i,j) = Qye(i,j) XOR key2
          Qy(i,j) = mod(Qye(i,j)+key2)
                f(i,j) = $(Qx(I,j))^{-1}$ (Qy(I,j)-1) mod P
       Case 0:     Qx(i,j) = Qxe(i,j) XNOR key2
          Qx(i,j) = mod(Qxe(i,j)+key2)
                  Qy(i,j) = Qye(i,j) XNOR key2
          Qy(i,j) = mod(Qye(i,j)+key2)
                f(i,j) = $(Qx(I,j))^{-1}$ (Qy(I,j)-1) mod P
```

5 Finally got f so it generates decrypted image and Stop the algorithm.mod stand for modulus after division. Since all secret key cannot make disorderly encryptedimage.Actually the secret key of propose algorithm is p, key1, key2, Xc (0). The key contains total 3n+32 bit because of following criteria

.N=1
∑ (ai+di) =n\2 (9)
I=0

32 n n n n
2 *2 *c*2 \ (log2 – 1) keys are available out of the key that shows complexity of an attack

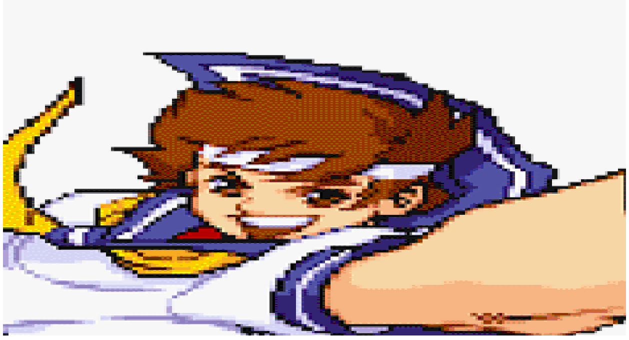

Figure 3 Original image

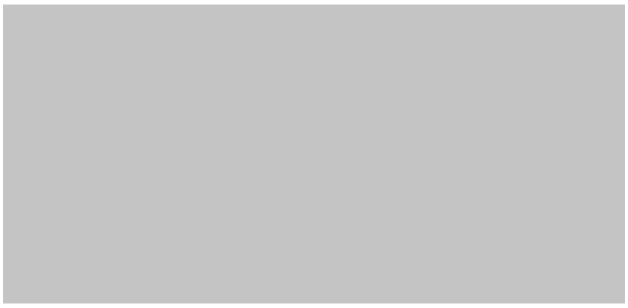

Figure: 3(a) Qx of doll image (Qx)e

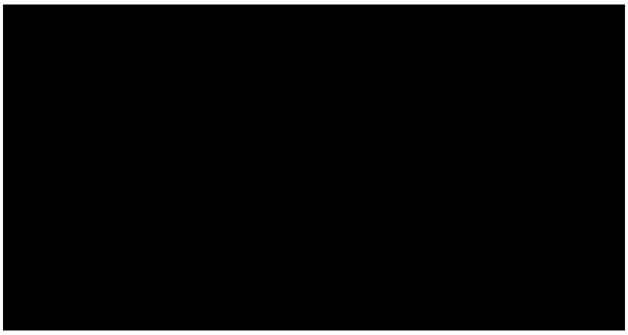

Figure: 3(b) Qx of doll image (Qy)e

IV. IMPLEMENTATION RESULTS

Table 1 Comparison result with other encryption algorithms.

Input In K.B	**AES (ms)**	**3DES (ms)**	**BLOW FISH (ms)**	**RC2 (ms)**	**Proposed Algorithm (ms)**
49	56	54	36	57	68
59	38	48	36	60	80
100	90	81	37	91	112

Table 2 Comparison of Proposed Algorithm with other encryption algorithms.

ALGORITHM	**ENCRY. RATIO**	**SECURITY**	**SPEED**
AES	**>37.5%**	**LOW**	**FAST**

XOR	50-60%	LOW	FAST
PROPO.ALGO.	ABOUT 70%	VERY HIGH	ACHIEVE HIGH SPEED USING DEDICATED HARDWARE

V. CONCLUSION

In this project, the various genetic algorithm & chaos based of information security has been discussed, and a new approach has been proposed. For transmitting the secured data over the channel there is requirement of the high throughput, in these cases the conventional encryption techniques are not a feasible solution for this reason a high throughput and secure encryption technique is proposed for real time data transmission like over the telephone link or video transmission. The concept of Genetic Algorithms used along with the randomness properties of chaos. Limitation of The concept of Genetic Algorithms used along with the randomness properties of chaos. Limitation of Chaotic cryptography is improved by using Brahmagupta-Bhaskara equation.This total way of transferring secret information is highly safe and reliable. The simulation results have indicated that the encryption results are (1) completely chaotic by the sense of sight, (2) very sensitive to the parameter fluctuation.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to my honourable guide Prof. Himanshu Arora and Prof. Dipak Dembla for their valuable guidance and constant encouragement. They encouraged my ideas, provided me a platform to establish them. I am also thankful to all the faculty members of the Computer Science Engineering Department for helping me directly or indirectly in bringing this piece of work to a successful completion.I must reserve a special thanks to my parents as this work would have been impossible without their blessings. I owe my deepest gratitude to them. Above all, I express my thanks to the "ALMIGHTY" for all his blessing and kindness.

REFERENCES

[1] N Masuda and K Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Trans. on Circuits and Systems -I:* Fundamental Theory and Applications, vol. 49, no. 1, pp. 28-40, 2002.

[2] DouS Li, G Chen and X Zheng, "Chaos-based encryption for digital images and videos," In: B. Furht and D. Kirovski, editors. Multimedia Security Handbook of Internet and Communications Series, Ch. 3, CRC Press, Vol. 4, 2004.

[3] N. Rama Murthy and M. N. S. Swamy, "Cryptographic Applications of Brahmagupta-Bhaskara Equation ", IEEE Transactions on Circuits and Systems-I Regular Papers, VOL.53, NO. 7, JULY 2006 I

[4] K. Deergha Rao, K. Praveen Kumar and P.V. Murali Krishna, "A New and Secure Cryptosystem for Image Encryption and Decryption", IETE Journal of Research, VOL. 57, ISSUE 2, Mar-Apr 2011

[5] Wenbo Mao, "Modern Cryptography: Theory and Practice", Publisher: Prentice Hall PTR, Copyright: Hewlett Packard, 2004.

[6] D. S. Abdul. Elminaam, Higher Technological Institute, 10th of Ramadan City, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMAVolume 8, 2009 ISSN: 1943-7765

[7] J C Yen and J I Guo, "A New Chaotic Key -Based Design for Image Encryption and Decryption," Proc. IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, vol. 4, pp. 49-52, 2000.

[8] S Li, G Chen and X Zheng, "Chaos-based encryptionfor digital images and videos," In: B. Furht and D. Kirovski, editors. Multimedia Security Handbook of Internet and Communications Series, Ch. 3, CRC Press, Vol. 4, 2004.

[9] S J Li and X Zheng, "Cryptanalysis of s Chaotic Image Encryption Method," IEEE International Symposium on Circuits and Systems (ISCAS 2002), vol. 2, pp.708-11,2002

[10] N Rama Murthy and M N S Swamy, "Author's reply", IEEE Trans. Circuits Syst. I, Reg. Papers, vol.54, no. 4, pp. 928-9, 2007.

[11] A M Youssef, A comment on "Cryptographic applications of Brahmagupta-Bhaskara equation", IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, pp. 927-8, 2007.

[12] Jolly Shah and Dr. Vikas Saxena, " Performance Study on Image Encryption Schemes", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[13] Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption

[14] Daniel Socek_, Shujun Liy, Spyros S. Magliverasz and Borko Furhtx

BOOKS

[15] Ljupco Kocarev, shiguo Lian, "Chaos-based Cryptography", springer, 2011

[16] Wade trappe, Lawrence C. Washington, " Introduction to cryptography with Coding Theory", Pearson education.

[17] Oded Goldreich, "Foundations of Cryptography: Basic Applications", Cambridge University, 2004, vol. 2.

WEBSITES

[18] "Different Cryptography Algorithms", available online at http://en.wikipedia.org/wiki/.

[19] "Data Encryption Techniques", available online at www.mrp3.com/encrypt.html

[20] "Encryption Algorithms", available online at ftp-software-review.toptenreviews.com/encryption-algorithms.html

[21] http://en.wikipedia.org/wiki/Automatic_Number_Plate_recognition,Retrieved