International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 247-249
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

ADVANCE CRYPTOGRAPHY ALGORITHM USING BB EQUATION AND PIXEL SHUFFLING/DE-SHUFFLING

Ishwar Lal Paliwal
MTech Scholar (DC)
Department of ECE
Shrinathji Institute of Technology & Engineering, Nathdwara

Dr. Mahesh Kumar Porwal
Professor
Department of ECE
Shrinathji Institute of Technology & Engineering, Nathdwara

Abstract— **The encrypted image is difficult in compare to the encryption of the text because of the high capacity. Recent methods are difficult to handle the image encryption. Recently, the use of chaotic signals for secure data transmission has shown significant growth in developing chaotic encryption algorithm. In a recent articlet he application of the Brahmagupta–Bhaskara (BB) equation for encryption is reported. However, a number of chaos-based algorithms are proved to be insecure in the literature. It is also shown in the literature that the BB equation based algorithm can be broken by a low complexity known as plaintext attack. Hence, in this paper, we are using pixel shuffling and then we make a new secure cryptosystem based on the BB equation and chaos is proposed for image encryption and image decryptions.**

Keywords: Image Pixel Shuffling, BB equation, Chaos Cryptosystem, Image Encryption. Image Decryptions

I. INTRODUCTION

Cryptography is a process in which we convert a plain text or clear text message to cipher text message which is based on an algorithm that both sender and receiver know, and in this way the cipher text message can be obtained to its original form. In this way, a message cannot be read by anyone but the authorized receiver. The process of converting a plain message to its cipher text form is called enciphering. Reversing this process is known as deciphering. Enciphering and deciphering are other names of encryption and decryption. There are a number of methods used to perform encryption and decryption. The most usable method uses a key. A key is a parameter of algorithm by which encryption and decryption takes place. Key-based cryptographic techniques are divided into two methods: symmetric and asymmetric. In symmetric cryptography, same key is used for encryption and decryption. In asymmetric cryptography, one key is used for encryption and another for decryption

II. PIXEL SHUFFLING

In this Paper Pixel shuffling play very important role. Pixel of image is shuffling from low intensity to high intensity in every row. , First all pixels of row 1 are arranged according to their value of intensity .Then row 2, row 3,etc. At the end we get the new shuffled image.
So, the further steps of the algorithm is done with this shuffled image

III. IMAGE PIXEL DESHUFFLING

Pixel shuffling and De-shuffling is nothing but it is a process to change the position of pixel which can be very helpful for encryption and decryption. In this concept we are doing shuffling by setting the lowest value to highest value of pixel. and de-shuffling process is reverse to shuffling. It can be done by setting the highest value to lowest value of pixel.

IV. USE OF BRAHMAGUPTA-BHASKARA EQUATION IN CRYPTOGRAPHY

The Brahmagupta-Bhaskara equation can be written as

$$(f_x{}^2+1)_p = (y^2)_p \quad \text{.....(1)}$$

Here , 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 (1) can be written as

$$(f(x^2)_p)_p +1 =(y^2)_p \quad \text{.....(2)}$$

Equation (2) can be rewritten as

$$(fq_x+1)_p = (q_y)_p \quad \text{.....(3)}$$

where q_x and q_y are the quadratic residues solution of the BB equation.
To solve the BB equation, find a possible pair (x,y) so that Equation (1) is satisfied for given f and p.
Once x and y are found, then q_x and q_y are computed as

$$q_x=(x^2)_p \text{ , } q_y=(y^2)_p \quad \text{.....(4)}$$

Given qx and qy corresponding to any root of the BB equation (fx2 + 1) p = (y2)p, it is always possible to compute uniquely the corresponding value of f, only with the knowledge of p, using the following relation:

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 247-249
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

$$f = (q\,x)^{-1}\,(q\,y - \square 1) \bmod (p) \quad .....(5)$$

The f corresponds to the clear text or plaintext in a block that is being encrypted and p corresponds to the primary secret key used in the encryption of the plaintext in a block.

V. CHAOS FUNDAMENTAL PRINCIPLE FOR CRYPTOLOGY

Sensitive dependence is one of the desired feature of the cryptographic algorithm. As, if the initial conditions that are use to encrypt any data are change even by a small amount, one bit for instance, then the encrypted text will change widely . This is one of the fundamental principles of the chaotic functions which is given by the following equation-

$$X_c(i+1)=\mu X_c(i)(1-X_c(i)) \quad .....(6)$$

When μ = 3.9, the logistic map exhibits chaotic behavior, and hence the property of sensitive dependency.

VI. THE PROPOSED ALGORITHM

The block diagram of the proposed algorithm for encryption is shown in Figure 1. In this , for a given primary key p, the root pair of
the BB equation corresponding to each pixel of the image is found. Then, according to a binary sequence generated from a chaotic system, a mod oper ation is performed on
the root pair of the BB equation corresponding to each pixel and then each root is XORed or XNORed bit-by- bit to one of the two predetermined keys, key1 and key2.

Let f denote an image of size M × N pixels and f(i, j), $0 \le i \le M-1$, $0 \le j \le N-1$ be the gray level of f at position (i, j). The encryption algorithm for the proposed f cryptosystem is as follows.

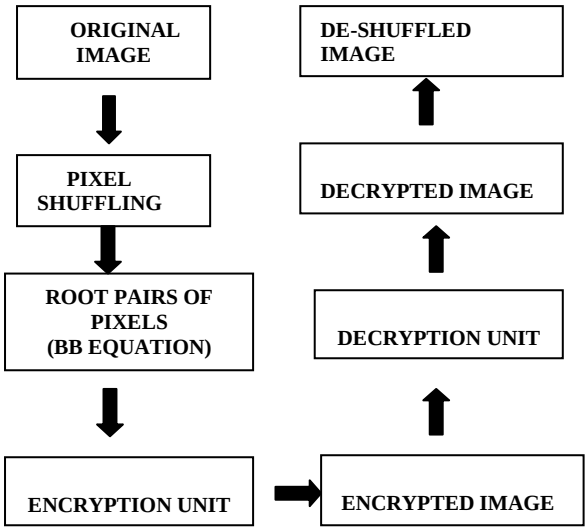

Figure 1: Block diagram of the proposed Algorithm.

VII. THE PROPOSED ALGORITHM FOR ENCRYPTION

The proposed algorithm for encryption is as follows.
Step 1:Choose p, key1 and key2 and set l = 0.

Step 2: Choose the initial point Xc (0) and generate the chaotic sequence Xc (0), Xc (1), Xc (2), …, Xc (MN/16 − 1) using Equation (4) and then create b (0), b (1), b (2), …, b (2MN − 1) from Xc (0), Xc (1), Xc (2) ,…,
Xc (MN/16 − 1) by the generating scheme such that b(32i + 0)b(32i + 1) …..... b(32i + 29)b(32i + 30)b(32i + 31)…..... is the binary representation of Xc (i) for i = 0, 1, 2, (MN/16 − 1).
Step 3: For i = 0 to M − 1
For j = 0 to N − 1, obtain Qx(i, j) and Qy(i, j) from the solution of BB equation.

VIII. THE PROPOSED ALGORITHM FOR NCRYPTION

The proposed algorithm for encryption is as follows.
Step 1:Choose p, key1 and key2 and set l = 0.

Step 2: Choose the initial point Xc (0) and generate the chaotic sequence Xc (0), Xc (1), Xc (2), …, Xc (MN/16 − 1) using Equation (4) and then create b (0), b (1), b (2), …, b (2MN − 1) from Xc (0), Xc (1), Xc (2) ,…, Xc (MN/16 − 1) by the generating scheme such that b(32i + 0)b(32i + 1) …..... b(32i + 29)b(32i + 30)b(32i + 31)…..... is the binary representation of Xc (i) for i = 0, 1, 2, (MN/16 − 1).

Step 3: For i = 0 to M − 1

For j = 0 to N − 1, obtain Qx(i, j) and Qy(i, j) from the solution of BB equation.

IX. STEPS FOR PROPOSED DECRYPTION LGORITHM

Step1: Same as Encryption Algorithm
Step 2: Same as Encryption Algorithm
Step 3: Get the values of **Qxe(i,j)** & **Qye(I,j)** for each pixel from two encrypted images.
Step 4: Decryption Process

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

Case 3: $Qx(i,j) = Qxe(i,j)$ XOR key1
$Qx(i,j) = \bmod(Qxe(i,j)+key1)$
$Qy(i,j) = Qye(i,j)$ XOR key1
$Qy(i,j) = \bmod(Qye(i,j)+key1)$
$f(i,j) = (Qx(I,j))^{-1}\,(Qy(I,j)-1) \bmod P$

Case 2: $Qx(i,j) = Qxe(i,j)$ XNOR key1
$Qx(i,j) = \bmod(Qxe(i,j)+key1)$
$Qy(i,j) = Qye(i,j)$ XNOR key1
$Qy(i,j) = \bmod(Qye(i,j)+key1)$
$f(i,j) = (Qx(I,j))^{-1}\,(Qy(I,j)-1) \bmod P$

Case 1: $Qx(i,j) = Qxe(i,j)$ XOR key2
$Qx(i,j) = \bmod(Qxe(i,j)+key2)$
$Qy(i,j) = Qye(i,j)$ XOR key2
$Qy(i,j) = \bmod(Qye(i,j)+key2)$
$f(i,j) = (Qx(I,j))^{-1}\,(Qy(I,j)-1) \bmod P$

Case 0: $Qx(i,j) = Qxe(i,j)$ XNOR key2
$Qx(i,j) = \bmod(Qxe(i,j)+key2)$
$Qy(i,j) = Qye(i,j)$ XNOR key2

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 8, ISSN No. 2455-2143, Pages 247-249
Published Online June - July 2016 in IJEAST (http://www.ijeast.com)

$$Qy(i,j) = \mathrm{mod}(Qye(i,j)+key2)$$
$$f(i,j) = (Qx(I,j))^{-1}\,(Qy(I,j)-1) \bmod P$$

Step 5: Finally it generates decrypted image.

X. RESULTS

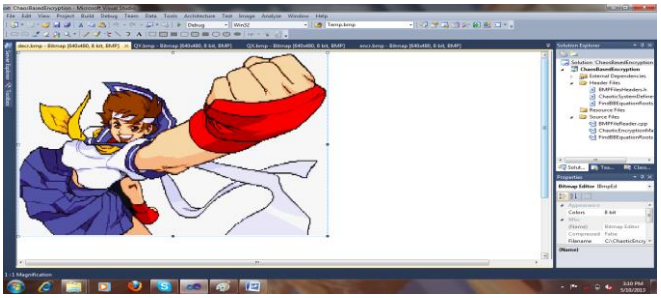

Figure 1: Original image

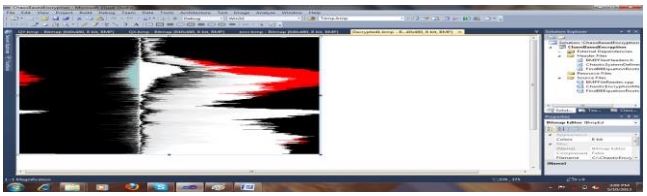

Figure 2: Shuffled image

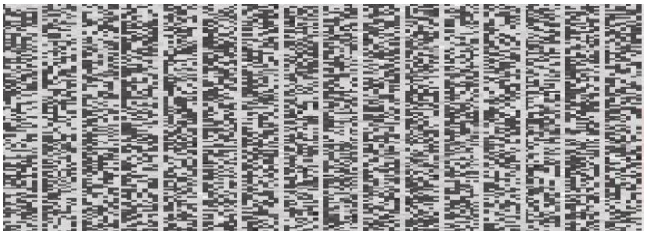

Figure 3: Encrypted Qx of the Shuffled image

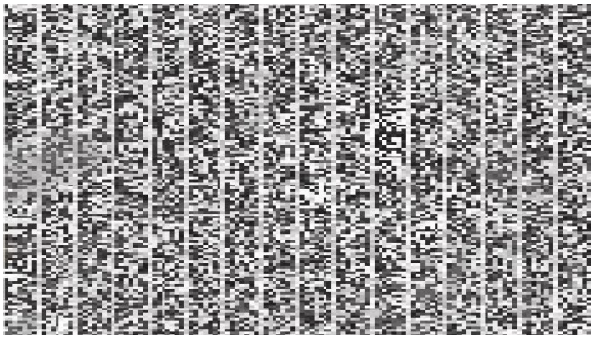

Figure 4: Encrypted Qy of the Shuffled image

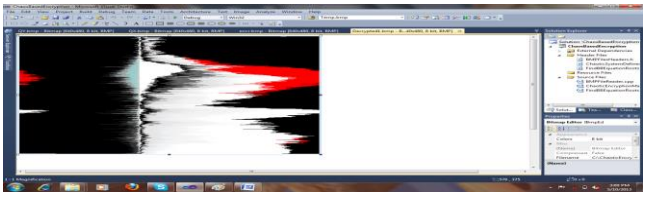

Figure 5: Decrypted image

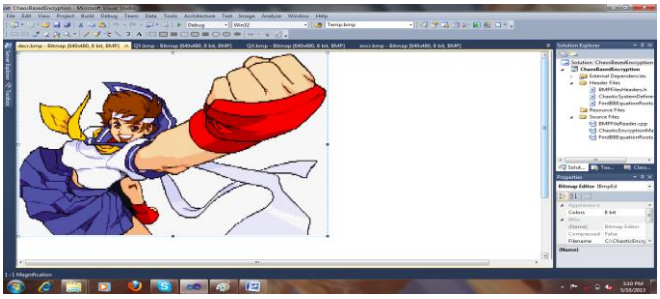

Figure 6: DeShuffled image

XI. CONCLUSION

In this paper, a secure algorithm based on Brahmagupta–Bhaskara equation is design for image encryption. From the result, it is concluded that the proposed algorithm is effective for secure image encryption.

XII. REFERENCES

1. S 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

2. 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.

3.T Seidel D Socek, and M Sramka, Cryptanalysis of video encryption algorithms," In Proceedings of the 3rd Central European Republic, June 26-28 (2003), Tatra Mt. Mathematical publications, Vol. 29, pp. 1-9, 2004.

4. G Alvarez ,L H Encinas, and J M Masque, "Known-Plaintext Attack to Two Cryptosystems Based on the BB Equation," IEEE Transactions on Circuits and Systems II: Express Briefs Vol. 55, Issue 5, pp. 423-6, 2008.

5. A M Youssef, A comment on "Cryptographic applications of Brahmagupta-Bhakara equation", IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, no. 4, pp. 927-8, 2007.

6.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.