Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.297 – 306

RESEARCH ARTICLE

Secure Crypto System for Image Encryption and Data Embedding using Chaos and BB Equation Algorithm

S.Revathy
M.E Scholar
Sri Shakthi Institute of Engineering and Technology

Abstract:

This project proposes method for image encryption and decryption, data embedding and data extraction. The content owner first encrypts image by BB equation and chaos algorithm, then the data is encrypted using data hiding key and embedded into LSB bit of specific pixels. With an encrypted image containing additional data, if a receiver has the data-hiding key, the data can be extracted without revealing original image. If the receiver has the encryption key, the original image can be extracted without disturbing data embedded. If the receiver has both the data-hiding key and the encryption key, then additional data and the original content can be recovered without any error. Since the data embedding only affects the LSB of the encrypted image, the decryption with the encryption key can result in image retrieval similar to the original version.

I. Introduction

With the rapid development of science and technology, information technology has been used widely in people's daily life. In this era of information technology, most of the confidential data and secret information is being exchanged by electronic media. The advantage of using electronic media for transferring

confidential information is that, electronic devices or components provide a high level of security, confidentiality and integrity to the data or image to be transmitted. In order to find a solution to the up to date problem of security, cryptographic algorithms are constructed to provide secure communication applications. The Cryptographic technique is process of scrambling the original message with key (set of characters) and its goal is to achieve confidentiality, integrity of data. The encryption is a process of encrypting image or data with key and decryption will reveal the original data or image by using same key which used for encryption. Data hiding is process of hiding data in any cover media like image, video etc., More techniques or algorithm is used for image encryption, decryption and for data hiding. The most common way to encrypt a data is to use XOR implementation. This paper proposes method for encryption and decryption using chaotic algorithm and BB equation and data hiding is done by simple LSB substitution method.

II. SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE

In separable reversible data hiding method the image is first encrypted using encryption key, then additional data is embedded into encrypted image by compressing LSB bit of an image. In decryption side the image will decrypted using encryption key or data will be extracted using data hiding key or both can be obtain by respected keys.

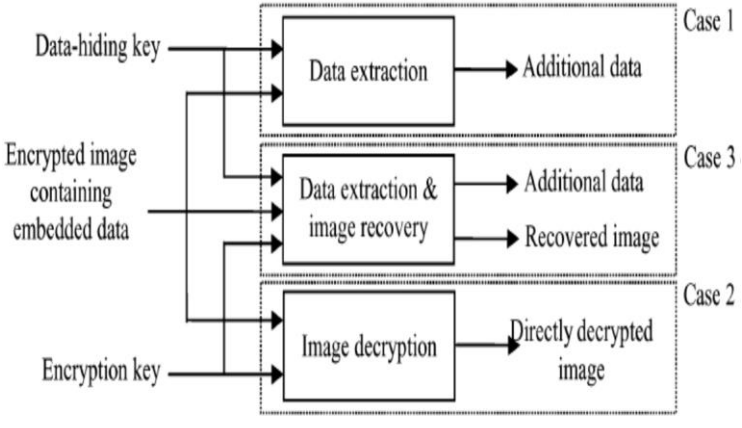

Fig 1 Separable reversible data hiding in encrypted image

In this technique data hiding is complex since it need compression of image and to place data in LSB bit of image and the key is only XORed with image to encrypt it, so it is not encrypted clearly[1] or there can be chance for revealing the image or data. To overcome above said problems this paper proposes method for double encryption of image using BB equation and chaotic algorithm and data hiding is done by simple LSB substitution method.

III. CHAOTIC ALGORITHM AND BB EQUATION

Image encryption using BB equation:

Cryptosystem based on BB equation is proposed in recent article [2]-[4]. The BB-equation in Galois Field GF (p), can be written as,

$$(n(x^2)_p)_p + 1 = (y^2)_p$$

n= original image,

p= secret key for image (odd prime).

The alternative representation for BB equation is,

$$(nq_x + 1)_p = (q_y)_p$$

Where $q\ x = (x^2)_p$, $qy = (y^2)_p$ and the subscript stands for modulo operation by p on the argument values of the expressions. The application of the BB equation for encryption depends on the following two properties.

1. Given n and p, with p>n>O, it is always possible to obtain q x and q y corresponding to the roots of the BB equation $(nx^2 + 1)_p = (y^2)_p$

2. Given qx and qy corresponding to any root of the BB equation $(nx^2 + 1)_p = (y^2)_p$, it is always possible to compute uniquely, the corresponding value of n, only with the knowledge of p.

The encryption process based on the BB equation is as follows,
1.) n corresponds to the clear text or 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 (qx, qy) of the corresponding BB equation.

Image encryption using chaotic algorithm:

The chaotic function that used is the well-known logistic map given by,

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

Where $\mu = 3.9$. Let f denote an image of size M x N pixels and f(x, y), $0 \leq x \leq M-1$, $0 \leq Y \leq N-1$, be the gray level f at position (x, y).In this algorithm qx, qy are computed using the BB equation-based encryption procedure, then a nonlinear operation (mod operation) on the added value of qx, qy and key in addition to the operations of the CKBA.

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 using chaotic sequence generator. Binary sequence is generated using binary sequence generator.

Step 3:

For x= 0 to M-1
For y = 0 to N-I

Obtain qx(x, y), qy(x, y) for chose n, p and given f(x, y) from the solution of the BB equation [5]-[6].

Case 3:
qxe(x,y) = mod((qx(x,y) +key l), 2n-l)
qxe(x,y) = qxe(x,y)XOR key l
qye(x,y) = mod((qy(x,y) +key l), 2n-1)
qye(x,y) = qye(x,y)XOR key l

Case 2:
qxe(x,y) = mod((qx(x,y) +key l), 2n-1)
qxe(x,y) = qxe(x, y) XNOR key l
qye(x,y) = mod ((qy(x,y) +key l), 2n-1)
qye(x,y) = qye(x,y)XNOR key l

Case 1:
qxe(x,y) = mod((qx(x,y) +key2), 2n-l)
qxe(x,y) = qxe(x.y)XOR key2
qye(x,y) = mod((q(x,y) +key2), 2n-1)
qye(x,y) = qye(x,y)XOR key2

Case 0:
qxe(x,y) = mod((qx(x,y) +key2), 2n-1)
qxe(x,y) = qxe(x,y)XNOR key2
qye(x,y) = mod((q(x,y) +key2), 2n-l)
qye(x,y) = qye(x, y) XNOR key2
j = j + 2
End;
End;

Step 4: The result qxe(x, y), qye(x, y) is obtained and stop the algorithm. The basic criterion to select key1 and key 2 is

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

Where Key1 $=\sum_{i=0}^{m-1} ai * 2i = m/2$, Key 2 $=\sum_{i=0}^{m-1} di * 2i = m/2$.

The Decryption Algorithm is as follows:

Steps 1 and 2 are the same as in the above encryption algorithm. Steps 3 and 4 for the decryption are as follows.

Step3:

For x=0 to M-l
For y = 0 to N-I
Switch (2xb (j)) + b(j)+ I))

Case 3:
qx(x, y) = qxe(x, y)XOR key l
qx(x, y) = mod((q x(x, y)–key l),2n-l)
qy(x, y) = qye(x, y)XOR key l
qy(x, y) = mod((q y(x, y)-key l),2n-1)
$f(x, y) = (qx(i))^{-1} (qy(i) -l) \bmod(p)$.

Case 2:
qx(x, y) = qxe(x, y)XNOR key l
qx(x, y) = mod((qx(x, y)-key l),2n-l)
qy(x, y) = qye(x, y)XNOR key l
qy(x, y) = mod((qy(x, y)-key l),2n-1)
$f(x, y) = (qx(i))^{-1} (qy(i)-I) \bmod(p)$.

Case 1:
qx(x, y) = qxe(X, y)XOR key2
qx(x,y) = mod((qx(x, y) -key2),2n-l)
qy(x,y) =qxe(x,y)XORkey2
qy(x, y) = mod((qy(x, y)-key2),2n-1)
$f(x, y) = (qx(i))^{-1}$ (qy(i) -1)mod(p).

Case 0:
qx(x,y)=qxe(x,y)XNORkey2
qx(x, y) = mod((qx(x, y) -key2),2n-l)
qy (x ,y) = qye(x, y)XNOR key2
qy(x, y) = mod((qy(x, y) -key2),2n-l)
$f(x, y) = (qx(x, y)^{-1}$ (qy(x, y)- l)mod(p).
j = j+ 2
End; End

Step 4: The result f is obtained and stop the algorithm.

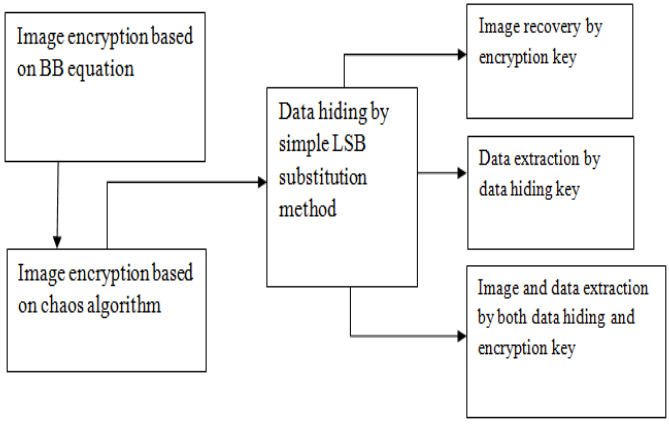

Fig 2 Block diagram of encryption, decryption and data hiding

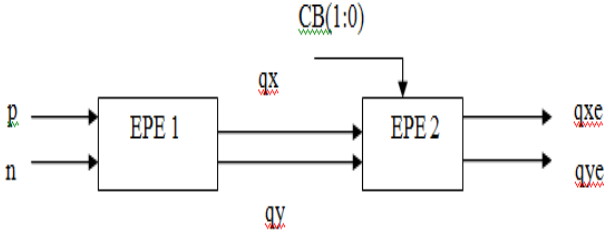

Fig 3 Block diagram for encryption unit

The architecture of EPE 1 is shown in Figure 4, which consists of three multipliers, one adder, two mod operators and one comparator. The architecture of EPE2 is shown in Figure 5 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.

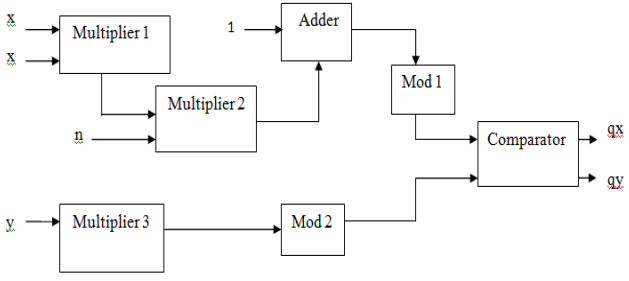

Fig 4 Block diagram of EPE1 module

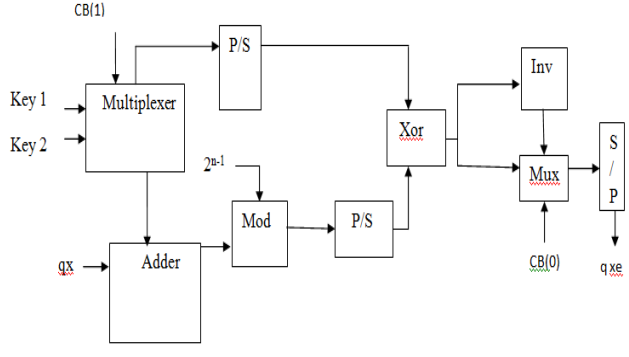

Fig 5 Block diagram of EPE 2 module

The decryption unit is shown in a Figure 6. The DPE 1 shown in Figure 7, uses key 1, key 2, CB(1), CB(0), 2^{n-1} as an input. It have two multiplexer, two parallel to serial convertor, one xor unit, one serial to parallel convertor, one subtractor, one modulo operator unit. The output of decryption unit 1 is qx,qy. The DPE 2 shown is Figure 8, uses qx, qy, 1 as an input. It has one mod inverse

unit, one subtractor, one multiplexer, one modulo operator unit. The output of decryption unit 2 is f, i.e... Input data.

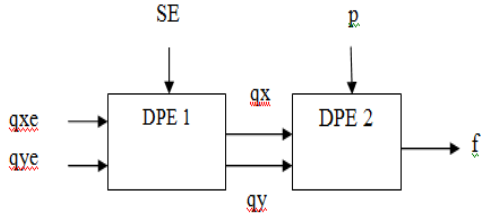

Fig 6 Block diagram of Decryption module

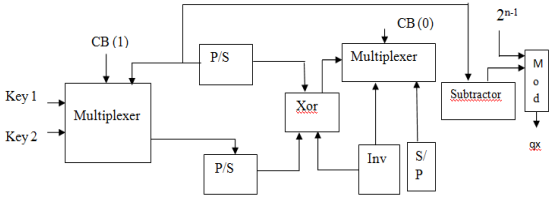

Fig 7 Block diagram of DPE 1 module

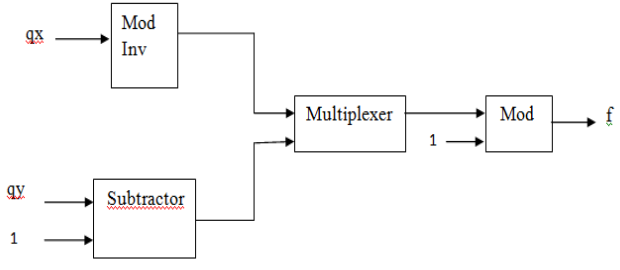

Fig 8 Block diagram DPE2 module

Data Hiding:

In the data embedding phase, the data is first converted into cipher text by adding with data hiding key. Then the cipher text form of data is embedded into LSB bit of encrypted image by simple LSB substitution method.

Data hiding by simple LSB substitution:

In this section, the general operations of data hiding by simple LSB substitution method is described[7].
Let C be the original 8-bit grayscale cover-image of Mc × Nc pixels represented as

$$C = \{xij \mid 0 \leq i < Mc,\ 0 \leq j < Nc,$$

$$xij \in \{0,1,\ldots\ldots,255\}\} \quad (1)$$

M be the n-bit secret message represented as
$M = \{mi \mid 0 \leq i < n,\ mi \in \{0; 1\}\}$ (2)

The n-bit secret message M is need to be embedded into the k-rightmost LSBs of the cover-image C. The subset of n pixels $\{x_{l1}; x_{l2}; : : : ; x_{ln}\}$ is chosen from the cover-image C in a predefined sequence. The embedding process is completed by replacing the k LSBs ofx_{li} by m_i.

The mathematical equation to denote this is as follows:

$$x_{li}' = x_{li} - x_{li} \bmod 2^k + m_i$$

The x_{li}' denotes pixel value after the data is embedded. The pixel for data to be embedded is given by LFSR, where its ouput generates a specific value in that value will be used as an pixel value for data embedding. After data embedding the data extraction is done by giving values of pixel where data is embedded. The mathematical representation for data extraction is given by:

$$m_i = x_{li} \bmod 2k :$$

IV. Conclusion and Future Scope

In this paper a secured cryptosystem for image encryption and decryption is proposed based on VLSI architecture of chaotic algorithm and BB equation and data embedding process is done by simple LSB substitution method. This technique provides high level of security because image is double encrypted by BB equation and chaotic algorithm. In future steganographic technique can be used as a part of encryption and decryption process to improve the secrecy of image or data.

REFERENCES

[1]Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Imag**e"** IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, april 2012
[2] A. M. Youssef, A comment on "Cryptographic applications of Brahmagupta Bhakara equation ", IEEE Trans. Circuits Syst. I, Reg Papers, vo1. 54,no. 4,pp. 927-928
[3] Rama Murthy N. and Swamy M.N.S, " Cryptographic Applications of Brahmagupta-Bhaskara Equation",IEEE Transactions on circuits -I, Regular Papers, Vo1.53, July 2006, pp. 1565-1571.
[4] G. Alvarez, L. H.Encinas, and .l.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.
[5] Suvarna M., Prabhavathi K., Anandaraju M. B., Nuthan A. C., (2013) 'Design and Implementation of Highly Secure Cryptosystem for Image Encryption' (IJIES) ISSN: 2319–9598, Volume-1, Issue-7.
[6] Deergha Rao K. and Gangadhar Ch., (2011) 'VLSI Realization of a Secure Cryptosystem for Image Encryption and Decryption' IEEE.
[7] Chi-Kwong Chan, Cheng L.M. (2003). 'Hiding data in images by simple LSB substitution' Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong.

