A New Public Key Cipher System Based on Image Encryption

Md. Golam Rabiul Alam, Mohammad Mahadi Hassan, *Nadir Hossain, *S. M. Moinul Quadir
International Islamic University Chittagong, Chittagong
*Dhaka International University, Dhaka, Bangladesh
gra9710@yahoo.com, mahadi_cse@yahoo.com, nadir_hossain@yahoo.co.in, mebond007ce@yahoo.com

Abstract

Cryptography is one of the most important security mechanisms for information security and control. Public key cipher system provides more security then any other cipher system. In this paper we have proposed a new technique of cryptosystem, which treat the information as an image then compress the image by compression algorithm after that we encrypt every pixel of the image using LCL [1] method of message encryption. Our proposed algorithm is more secured then conventional LCL method of data encryption.

Keywords: Cryptography, Public Key, Cipher System, Compression, Encryption, LCL and RSA

1. Introduction

Cryptosystem is the system where encryption and decryption techniques are used to the network and computer for the security of the data. Encryption means the change of original information (text) into another form by some operations (algorithms) and decryption means the techniques of getting the original information by some operations (algorithms) from the encrypted data. Traditional cryptography is based on the sender and the receiver of message knowing and using the same secret key: the sender uses the secret key to encrypt the message and the receiver uses the same secret key to decrypt the message. This method is known as secret key cryptography. The main problem is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a mailing system or a phone system, or other transmission system not to disclose the secret key being communicated. These problems will be solved using public key cipher system. In the public key cipher system each person gets pare of keys, called a public key and the privet key is kept secret. One of the secured public key cipher systems is LCL [1], which is based on Diophantine equations. Here we have proposed a new technique of cryptosystem, which is based on LCL[1]. At first we treat the documents or text as an image. The image takes a large amount of memory, so we need to compress the image to reduce the size. Here we use lossless JPEG[6] or JPEG-LS[7] image compression algorithm to compress the image as our image is like a continuous tone image. Secondly we encrypt every pixels of that compressed image using LCL. At the time of decryption we again use the decryption techniques of LCL. And then decompress the cipher image to get original one. Finally we convert the image to text document. Our algorithm is more secured then existing algorithm due to pixel encryption and image compression.

2. Existing Algorithms

Here we describe the algorithm of LCL [1].
Key generation Process:
First, each user picks n pairs of parameters (q_1, k_1), (q_2, k_2), ..., (q_n, k_n) such the DK-conditions are satisfied. Afterwards, we determined

$$Q_i = \prod_{j \neq i}^{n} q_j$$

and $N_i = \lceil q_i / (k_i (q_i \bmod k_i \rceil$ are computed and b_i's are integers chosen such that $Q_i b_i \bmod q_i = q_i \bmod k_i$, for i= 1, 2, ..., n. Let $P_i = Q_i b_i$ and $S_i = P_i N_i \bmod Q$ for i=1, 2, ..., n, where,

$$Q_i = \prod_{i \neq i}^{n} q_i$$

Therefore, a vector $S=(s_1, s_2, ..., s_n)$ is obtained. Then the n-tuple S of integers is published and used as the public key of the cryptosystem for enciphering the messages. The chosen parameters (q_1, k_1), (q_2, k_2), ..., (q_n, k_n) are kept and used as the private key to decipher messages received.

The key generating process for each user are shown algorithmically in the below:

1. Pick n pair of positive integers (q_1, k_1), (q_2, k_2), ..., and (q_n, k_n) such that DK conditions are satisfied.
2. Compute, $R_i=q_i \bmod k_i$ for i=1,2,3,.....,n.

   Compute, $Q_i=\prod_{j\neq i}^{n} q_j$

   and $N_i = \lceil q_i /(k_i R_i) \rceil$ for i=1,2,3,....,n and compute,

   $$Q_i=\prod_{i\neq i}^{n} q_i$$
3. Compute, b_i 's such that $Q_i b_i \bmod q_i=R_i$ for i=1, 2, 3, ..., n. This can be done by the extend version of Euclid's algorithm[5].
4. Compute, $P_i=Q_i b_i$ and $S_i=P_i N_i \bmod Q$ for i=1, 2,3, ..., n.
5. Publish the encryption key PKu = $(s_1,s_2,.....,s_n)$ for user U.
6. Keep the private decryption key PRu= $((q_1, k_1), (q_2, k_2),.....,(q_n, k_n))$ in secret.
7. Keep P_i, Q_i, b_i, N_i and Q in secret or erase them.

Encryption and decryption process:
Let the sending message represented by

$M=(m_1, m_2,....., m_n)$

Where m_i is a bits sub-message represented by a decimal number in the range of $[0, 2^b-1]$
Then $(m_1, m_2,....., m_n)$ is enciphered by

$$C=E(S,M)=S*M=\sum_{i=1}^{n} m_i s_i$$

into an integer C. Afterward, the integer C is send to receiver as the cipher-image of the original message M. On receiving C, the receiver is able to convert C into $(m_1, m_2,.....,m_n)$ by

$$m_i = \lfloor k_i C / q_i \rfloor \bmod k_i ,$$

$1 \le i \le n$.

The encryption and decryption process are show algorithmically in the bellow:
For Encryption,

1. Encryption $M=(m_1, m_2,....., m_n)$ by

   $$C=E(S,M)=S*M=\sum_{i=1}^{n} m_i s_i$$
2. Send out the integer C as the cipher image of message M.
3. Exit.

For Decryption

1. Computer the i^{th} component m_i of message M by computing

   $m_i=D((q_i, k_i), C) = \lfloor k_i C / q_i \rfloor \bmod k_i$,

   $1 \le i \le n$.
2. Exit.

DK-Conditions:
For n pairs of integers (q_1,k_1), (q_2, k_2), ..., (q_n, k_n) it follows that

1. q_i's are pairwise relative primes; i.e. $\gcd(q_i, q_j)=1$ for $i \neq j$.
2. $k_i>w$ for i=1,2,.....,n. where $w=2^b-1$ and b is the length of bits of each sub-message.
3. $q_i>k_i w(q_i \bmod k_i)$, and $q_i \bmod k_i \neq 0$ for i=1,2,...,n.

The above three conditions are known as DK-conditions as they are used to generate as deciphering keys. This n integer pair (q_i, k_i)'s will kept secret and used as private key for user U for decryption of the encrypted message.

3. Proposed Algorithm

Encryption Algorithm:

Step 1: Covert the text to an image.

Step 2: Covert the image to gray scale image.

Step 3: Compress the image using lossless JPEG compression algorithm.

Step 4: Apply encryption (LCL) algorithm to each pixels of 4X4 matrix of the image and calculate the cipher image.

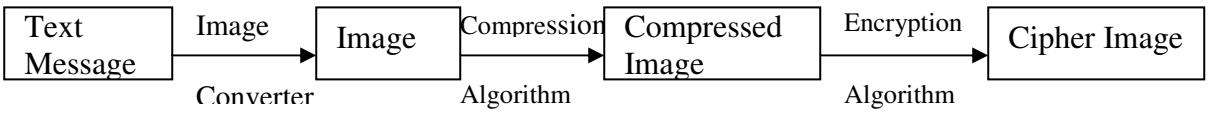

Figure: Encryption Technique

Decryption Algorithm:

Step 1: Apply the decryption (LCL) algorithm to the compressed image.

Step 2: Decompress the image.

Step 3: Covert the image to text.

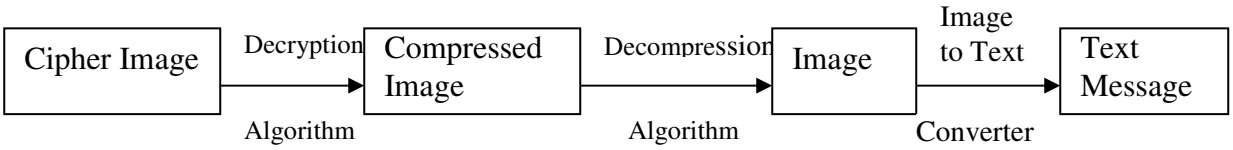

Figure: Decryption Technique

4. Example

Suppose we encrypt "CSE". At first we convert it to a gray scale image. After compression we consider each character of image as 12X12=144 pixels. So the total number of pixels are 144X3(for 3 characters)= 432. We encrypt each pixel. And found cipher image.

As for example, we want to encrypt 15 of the 432 pixels.

The pixel values, M=(67,83,69,32,68,105,115,99,105,112,108,105,110,101,46)

The generated private key corresponding 15 pixels are.

$(q_1,k_1)=(16711427,257)$, $(q_2,k_2)=(16711429,258)$, $(q_3,k_3)=(16711431,259)$, $(q_4,k_4)=(16711431,260)$, $(q_5,k_5)=(16711435,261)$, $(q_6,k_6)=(16711439,262)$, $(q_7,k_7)=(16711441,263)$, $(q_8,k_8)=(16711447,264)$, $(q_9,k_9)=(16711451,265)$, $(q_{10},k_{10})=(16711459,266)$, $(q_{11},k_{11})=(16711463,267)$, $(q_{12},k_{12})=(16711477,268)$, $(q_{13},k_{13})=(16711481,269)$, $(q_{14},k_{14})=(16711483,270)$, $(q_{15},k_{15})=(16711489,271)$.

By using these private keys we generate public keys for encryption and calculate cipher image.

C=146932247935318936779860548515413135323428510084238309325673625991485335494053143817307612457451121729011955250

The receiver has received the cipher image C and decrypts each pixel and gets 15 integer values of compressed image.

M=(67,83,69,32,68,105,115,99,105,112,108,105,110,101,46)

After decompression the original image is found. Then an image to text converter is used to recover the plain text.

5. Performance Analysis

The goal of computer security consists of maintaining three characteristics: confidentiality, integrity and availability.

Security Issue	Proposed Algorithm	LCL[1]	RSA[8]
Confidentiality	Most	More	More
Integrity	Most	More	More
Availability	Available	Available	Available

Table 1: Performance comparisons table

Our proposed algorithm is most confidential because LCL and RSA use character wise encryption unlike we use (12x12) 144 pixels for encrypting a single character. We like to say that our algorithm is also most reliable then LCL & RSA because our algorithm provides two level securities for documents. At first level we convert the text as image. And at the second stage we calculate the private key for every pixels of the image rather than every character. Again as our algorithm based on public key cipher system it is also available like RSA and LCL. Though our algorithm is complex then the existing algorithms but it provides more security of data than the existing.

6. Conclusion

The security of data is very much important for both the sender and receiver. Encryption provides security for data. The most important factor to implement a cryptosystem is calculating public key for the users of the system, which provide high level of security but the calculating process should be less complex. Our proposed public key cipher systems based upon the Diophantine equations provide high level of security but its implementation procedure is more complex. Decryption procedure of this public key system is relatively easy. If our algorithm can be implemented we believe that it can provide more security than existing.

References

[1] C. H. Lin, C. C. Chang and R. C. T. Lee, January 1995. A New Public Key Cipher System Based Upon the Diophantine Equations, IEEE Transactions on Computers. ISSN:0018-9340 Volume 44 , Issue 1 (January 1995) Pages: 13 - 19

[2] Michael J. Wiener, Summer 1998. CryptoBytes: Performance comparison of public key cryptosystem, vol. 4, no. 1, pp. 1-5.

[3] Oded Goldreich, Autumn 1997. CryptoBytes: On the Foundation of Modern Cryptography, vol. 3, no. 2, pp-1-5

[4] B. Chor and R. L. Rivest, 1998. Knapsack Type Public Key Cryptosystem Based on Arithmetic in Finite Field, IEEE Transaction on Information Theory, vol.34, no-5, pp-901-909.

[5] D. E. Knuth, 1980, "The Art of Computer Programming", vol.1 Fundamental Algorithm, 2nd Edition, MA: Addition- Wesley.

[6] ISO/IEC 10918-1 Digital image compression and coding of continuous-tone still images.

[7] ISO/IEC 14495-1 Lossless and near-lossless and coding of continuous-tone still images (JPEG-LS).

[8] R. L. Rivest , A. Shamir , L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978