Proposal of Two Secure Compression Algorithms

Ahmed Tariq S.[1,a] Alaa Kadhim F.[1] Shaimaa Akram H.[2]

[1]University of Technology, Baghdad, Iraq
[2] Institute of Medical Technology, Baghdad, Iraq
[a]drahmaed_tarq@yahoo.com

ISSN: 2231-8852

ABSTRACT

In this paper two algorithms that combine compression and encryption are proposed, one is based on chaotic logistic map, and another is based on linear feedback shift register with key as a pseudo random number generators. The main idea of these algorithms is to randomize the dictionary which made the prediction of the original message is very difficult.

Keywords: secure compression, chaos theory, linear feedback shift register

1. Introduction

Data compression is the process of reducing the size of data for storage and transmission costs. Data encryption is the process of protecting information from attack. Today the security of the network communication becomes one of the most important issues due to the large amount of information that passed through various network. These large amount of information need to be compressed before encrypted and send through the network in order to reduce the time and the cost of transmission over the network (Subhamstan, R. T., et al., 2011).

LZW is dictionary based lossless data compression algorithm invented by lempd-ziv-welch as variant of LZ78 algorithm, in which its output is a code instead of a character (Kuar, S. & Sulochana, V., 2012).

Some researchers applied compression before encryption in which the practical resistance against differential cryptanalysis has been increased (Singh, A. & Gilhotra, R., 2011; Sangwan, N., 2012). Others combine compression with encryption ((Subhamstan, R. T., et al., 2011; Kelley, J. & Tamassia, R., 2014). In this paper, compression and encryption are combined together in one step by adding levels of security to LZW compression process.

The rest of the paper is organized as follows. Section 2 explains the details steps of squeeze algorithm, which includes the compression and the decompression processes. In Section 3, the chaos theory has been presented. Linear feedback shift register method that produce a set of random numbers in cryptography is reported in Section 4. Section 5 explains the details steps of the proposed secure compression algorithms. In Section 6 the result discussion of this research work is given. Conclusion remarks are outlined in the final section, 7.

2. Squeeze Algorithm

In 2014, Kelley, J. & Tamassia, R. proposed squeeze algorithm that combines compression with encryption by changing the management of dictionary. In squeeze cipher, each time the used entry was swapped with another (usually empty) random position and the new entry is inserted in position selected at a random from unoccupied cell. The random number is generated based on salsa 20 stream cipher (Kelley, J. & Tamassia, R., 2014). Fig. 1 presents the details steps of the squeeze algorithm for compression process.

```
Input: key, input stream
Output: encrypted stream
Begin
    Intialsqueeze (key, iv, g, pre, ch, D)
    While more input
    Begin
      Read next ch
      If (pre & ch) found in D
         Pre=pre & ch
      Else
         Output index ind of pre in D
         Swap ind randomly in D
         Insert (pre & ch) randomly in D
         Pre=ch
      End
          If pre <> "" then
               Output index ind of pre in D
End
      Function intialsqueeze( key, iv, g, pre, ch, D)
Begin
        Generate iv
        Compute seed=$F_{key}$ (iv)
        Put seed in g
        Pre=""    and    ch=""
        For each single character ch
             Insert ch randomly in D
End
```

Fig. 1. Squeeze algorithm for compression process

Fig. 2 illustrates the details steps of the squeeze algorithm for decompression process.

3. Chaos Theory

Chaos theory is one branch of mathematics. It deals with dynamical nonlinear system. Chaos theory is a Butterfly Effect which means that it has a sanative dependence to initial condition. For system to be a Butterfly Effect it must be nonlinear and each state must be determined by the previous state (Boing, 2015).

Random Number Generator (RNG) is used in many areas especially in cryptography for generating cryptographic keys.

Chaotic system is used to generate unpredictable sequence of random numbers in which their periodic are very long based on initial state using chaos logistic map which is written in the form (Rahal, M. & Nageb, M., 2012):

$$X_{n+1}=r\, x_n(1-x_n) \;\ldots\ldots\; \text{Eq.1}$$

Where x_n is number in between [0,1] and r between [0,4].

```
Input: key, encrypted stream E
Output: decrypted stream
Begin
  Read iv from E
  Intialsqueeze (key, iv, g, D, pre, ch, m)
  While there is more encrypted stream E
  Begin
    Read next index e
    Compute pseudo random number p of new entry
    If D[e] is undefined and (e < > p or pre="") then
      Begin
       Output fail
       If D[e] is defined and e < > p and pre < > "" then
         Begin
           Ch= Head( D[e])
            Insert (pre & ch)    randomly in D
        Else if e=r and pre < > "" then
            Ch= Head(pre)
             Insert pre & ch randomly in D
             Output D[e]
             Pre=D[e]
             Swap e randomly in D
          End
       End
    End
End
```

Fig. 2. Squeeze algorithm for decompression

4. Linear Feedback Shift Register

Linear Feedback Shift Register (lfsr) is one of the most important methods that produce a set of random numbers in cryptography based on initial seed. It uses XOR or XNOR operation to produce its sequences. If it has n input values then it produces 2^n-1 output results. The operation uses in lfsr is deterministic, in which each state is the operation of the previous state. In order to expand lfsr operation relative polynomial is used (Sharaf, M., et al., 2005; Rahimov, H., et al., 2011).

5. The Proposed Secure Compression Algorithms

In this paper two secure compression algorithms are proposed. The first proposed algorithm is based on chaotic logistic map function and the second one is based on linear feedback shift register with key as pseudo random number generators that generate unpredictable long period random numbers in which it is useful to construct a shuffled dictionary.

5.1. The First Algorithm: Secure Compression Algorithm Based on Chaotic Logistic Map Function as a PRNG

The first proposed algorithm is the secure compression algorithm based on chaotic system. As it is discussed previously, chaotic system is used to generate long period of unpredictable random numbers based on its logistic map. In this algorithm, the current dictionary entry is swapped with a random position, and the new string is inserted in random position in dictionary. These random positions are generated from chaotic logistic map function. Fig. 3 illustrates the details steps of the compression algorithm.

```
Input: stream of character, initial seed.
Output: codes or indices
Begin
   Generate an array of random numbers using Chaotic_rand Function
   Initialize the shuffled dictionary D that contain ASSCII code for every single character with
initial permutation
   While there is more input
   Begin
     Read the next character ch
     W=previous & ch
     Check w if it is in D then
     Previous=w
   Else
     Begin
       Output=output &the code of the previous in D
       Swap the position of the previous with random number position generated from
       Chaotic-rand function in D
       Insert w in random number position generated from Chaotic-rand function in D
   End
   If previous <> "" then
       Output=output & the code of the previous in D
End
Function Chaotic-rand
Input: radius r, seed X(0)
Output: array of random numbers
Begin
   Chaotic_rand(0)=X(0)
   For i=0 to last value -1
         X(i+1)=r * X(i) * (1- X(i))
         Chaotic_rand(i+1)=X(i+1)
         Next i
End
```

Fig. 3. The compression algorithm

Fig. 4 shows the details steps of the decompression process.

```
Input: sequence of codes (indices), initial seed
Output: string of character
Begin
   Generate an array of random numbers using Chaotic_rand Function
   Initialize the shuffled dictionary D that contain ASSCII code for every single character with initial
       permutation
      Read a code k
      W=k
      While there is a character
        Begin
          If k is found in D then
          Begin
             Entry=Dictionary entry for k
             Output entry
             Insert w& entry[0]    in random position in D using chaotic_rand function
             W=entry
                Swap the position of the w with random position in D using chaotic_rand function
            End
          Else
                Output and insert in a random position in D the previous output and previous output first
                character
        End
End
```

Fig. 4. The decompression algorithm

5.2. The Second Algorithm: Secure Compression Algorithm Based on LFSR with Key as a PRNG

Linear feedback shift register is used to generate a sequence of random numbers. In this algorithm lfsr with key is used, in which the initial key is entered in binary and the bits are shifted and the new bit is computed based on feedback polynomial function, then bits in the lfsr is converted to decimal to compute the random value and use it as random number and the new key for the next step. This process continue until 2^n -1 values are generated (n represents the number of bits).

```
Input: initial seed in binary
Output: array of random numbers
Begin
  Key= initial seed in decimal
  lfsr_key (0)=key
  For i=1 to last value
    Begin
      X1= Shift initial seed one bit to left
      Apply lfsr feedback polynomial function
      Key= Add the bit generated in previous step instead of last bit after the shifting
            lfsr_key (i)=key in decimal
      Next i
    End
End
```

Fig. 5. Linear Feedback Shift Register, LFSR algorithm.

The secure algorithm for compression and decompression based on lfsr with key is same as the secure compression and decompression based on chaotic system except in the function of generating random numbers. Instead of using Chaotic_rand function the following lfsr_key function is used. Fig. 5 shows the details steps of the lfsr_key algorithm.

6. Discussion

This section provides some experiment on the two proposed algorithm. These two algorithms are implemented based on 2^{12} dictionary size and are compared with LZW and gzip. In the first algorithm which is based on chaotic system the following logistic map is used: $\mathbf{X_{n+1}=r\ x_n(1-x_n)}$ and the used value of r is 3.795.

In the second algorithm which is based on lfsr, the feedback $X^{12}+X^{11}+X^{10}+X^{4}+1$ is used to generate the new bit that added after shifting. The speed of LZW and gzip is higher than the proposed algorithms this is due to the permutation process done with each insertion process. The compression ratio achieved by the proposed algorithm is comparable to LZW and gzip. The proposed algorithms provide a level of security compered to LZW and gzip.

7. Conclusions

In current work, compression and encryption are combined together by implementing a random permutation process based on chaotic system and lfsr. This will allow doing compression with encryption at the same time in order to speed up the process of implementing one after another which it is useful especially in network transmission._In this paper two algorithms proposed to achieve that aim in which they are simple to implement and give good result.

References

Subhamstan, R. T., Soujanya, M., Hemalatha, T., and Revathi, T.(2011). Simultaneous Data Compression and Encryption, International Journal of Computer Science and Information Technologies (IJCSIT), 2369-2374.

Kuar, S. and Sulochana, V. (2012) .Design and Implementation of LZW Data Compression Algorithm**,** , International Journal of Information Science and Technologies (IJISST), vol.2, no.4.

Singh, A. and Gilhotra, R. (2011) .Data Security Using Private Key Encryption System Based on Arithmetic Coding, International Journal of Network Security and Its Application (IJNSA),vol3, no.3.

Sangwan, N.(2012). Text Encryption with Huffman Compression", , International Journal of Computer Applications, 0975-8887, vol 54, no.6.

Kelley, J. and Tamassia, R.(2014). Secure Compression: Theory and Practice.

Boing,(2015). Chaos Theory and the Logistic Map.

Rahal, M. and Nageb, M. (2012). Pseudo-Random Number Generator using Deterministic Chaotic System", , International Journal of Scientific and Technology Research, vol.1, Issue 9.

Sharaf, M., Mansour, H., and Zayed, H. (2005). A Complex Linear Feedback Shift Register Design for the A5 Key Stream Generator, Proceedings of the Twenty Second National Radio Science Conference.

Rahimov, H., Babaei, M., and Farhadi, M. (2011). Cryptographic PRNG Based on Combination of LFSR and Chaotic Logistic Map, Applied Mathematics, 2, 1531-1534.