International Journal of Engineering & Technology, 7 (2.9) (2018) 71-73

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An application data security with lempel-ziv welch and blowfish

Robbi Rahim [1] *, Danadyaksa Adyaraka [2], Sulfikar Sallu [3], Eri Sarimanah [4], Arif Hidayat [5], Anwar Sewang [6], Sitti Hartinah [7]

[1] *School of Computer and Communication Engineering, Universiti Malaysia Perlis, Kubang Gajah, Malaysia*
[2] *Komunitas Kolaborasi Publikasi Indonesia, Medan, Indonesia*
[3] *Faculty of Information Technology, Universitas Sembilanbelas November Kolaka, Kolaka, Indonesia*
[4] *Faculty of Teaching and Education, Universitas Pakuan, Bogor, Indonesia*
[5] *Universitas Muhammadiyah Metro, Lampung, Indonesia*
[6] *Institut Agama Islam Negeri Parepare, parapare, Indonesia*
[7] *Universitas Pancasakti, Tegal, Indonesia*
**Corresponding author E-mail: usurobbi85@zoho.com*

Abstract

This research uses Blowfish algorithm which is part of Algorithm Encryption in cryptography. The Blowfish algorithm is part of symmetric cryptography, which is the key used for encryption equal to the key used for decryption. Besides the security of the file, the size problem of a file is also a calculation. Large files can be compressed by performing the LZW compression process is one of the compression algorithms that use dictionary. The merger between the cryptographic algorithm and the compression algorithm ensures that files cannot be viewed by unauthorized users, ensuring files can be stored in low-capacity media all of which lead to faster delivery.

Keywords: *Encryption; Data Security; Application Security; Blowfish; LZW.*

1. Introduction

Secure and secure network transmission and connectivity is a priority when communication is made especially if there is a confidential data transmission process then security is a top priority [1]–[6]. Such information shall remain confidential during transmission and shall remain original upon receipt at the destination. To fulfill this, the process of encryption and decryption of information are required. Data encryption is a special technique undertaken to secure data from third parties or from other parties who are not entitled to such data or information by using a particular algorithm, the encryption process transforms the original data form into a form of password that is not easily known by the layman and requires an algorithm or specific methods for reading the data [7]–[10], so the information transmitted [11], [12] during the sending process is on the form of encrypting, so that the original information cannot be known by the unauthorized parties. The original information can only be known by the recipient by using a secret key [13]–[16].

Security by using cryptography is good enough but from the speed of delivery [17]–[20] as well as reducing the size of the original data, this combination is expected to increase the speed of data transmission and improve the security of the data to be transmitted. Blowfish and Lempel-Ziv Welch (LZW) algorithms were used in this study [13].

Blowfish is a symmetric key cryptography where is function that use S-Box and XOR for secure message [21]–[23]. Furthermore, in terms of compression, LZW is a lossless type compression and use dictionary method for its process. In general the LZW compression algorithm will form a dictionary during the compression process then immediately after completion the dictionary is not stored in the compressed file. So it can be explained that the general principle of LZW algorithm work is to check every character that appears and then combine with the next character into a string if the new string is not in the dictionary or not indexed then the new string will be indexed into the dictionary [24]–[26].

2. Methodology

Cryptography is the science and art of keeping messages safe by applying secret techniques in writing, with special characters, using letters and characters outside of their original form, or by other methods that can be understood only by certain parties [27]–[29].

Blowfish algorithm has a work like the following [30], [31]:

a) Key expansion (Key-expansion), it functions to change the key (minimum 32-bit, maximum 448-bit) into multiple sub-key arrays with a total of 4168 bytes (18x32-bit for P-array and 4x256x32-bit for S-box so that the total is 33344 bits or 4168 bytes).
b) Initialize the first P-array as well as four S-boxes, sequence with a definite string. The string consists of the hexadecimal digits of phi, excluding the three in the beginning.
c) XOR-P1 with 32-bit initial key, XOR P2 with next 32-bit of key, and so on for all key bits. Repeat the entire cycle of the key bits in sequence until the entire P-array is XOR with the key bits.
d) Encrypt the all-zero string with the Blowfish algorithm, using the sub-key that has been described in steps 1 and
e) Replace P1 and P2 with output from step 3.
f) Encrypt step 3 output using Blowfish algorithm with modified sub-key.
g) Replace P3 and P4 with output from step 5.

h) Continue the above steps, replace all P-array elements and then the fourth S-box in sequence, with the results of Blowfish algorithm output constantly changing.

The LZW compression algorithm has the following workings:

a) The Dictionary is initialized with all the basic characters present: {'A' .. 'Z', 'a' .. 'z', '0' .. '9'}.
b) P the first character in the character stream.
c) C the next character in the character stream.
d) Is the string (P + C) contained in the dictionary? If yes, then P = P + C (combine P and C into a new string).

If not, then:

a) Output a code to replace string P.
b) Add a string (P + C) to the dictionary and give the number/code that has not been used in the dictionary for the string.
c) P C
d) Are there any subsequent characters in the character stream?

If yes, then go back to step 2.

3. Results and discussion

Application of blowfish and LZW algorithm can be seen in Figure 1 below.

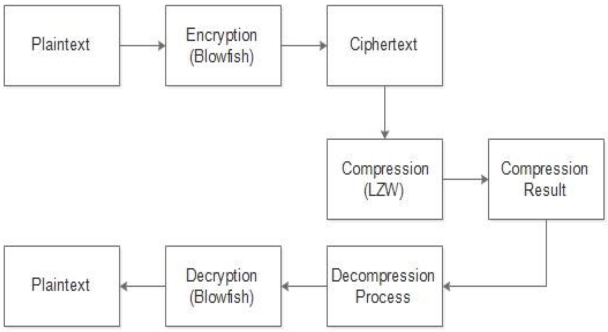

Fig. 1: Blowfish and LZW Process Diagram.

Cryptography process using Blow-fish algorithm begins by determining the plaintext and the key that will be used, then encryption process is done. The key forming process in the Blowfish algorithm can be seen in the following pseudo-code:

```
Public WriteOnly Property KeyGenerate() As String
Set(ByVal Value As String)

Dim datar, dataX, j, i, K, datal, PanjKunci As Integer
Dim Key() As String
If (Nilakunci = Value) Then Exit Property
Nilakunci = Value
PanjKunci = Len(Value)

datal = 0 : datar = 0
For i = 0 To (ROUNDS + 1) Step 2
Call Encryption(datal, datar)
Next
End Set
End Property
```

The encryption and decryption process is done by using the following pseudocode:

```
Private Sub Encryption(ByRef Xl As Integer, ByRef Xr As Integer)
        Static j, i, Temp As Integer
        Xr = Xl Xor m_pBox(ROUNDS)
        Xl = Temp Xor m_pBox(ROUNDS + 1)
End Sub

Private Sub Decryption(ByRef Xl As Integer, ByRef Xr As Integer)
        Static j, i, K As Integer
        K = Xr
        Xr = Xl Xor m_pBox(ROUNDS + 1)
        Xl = K Xor m_pBox(ROUNDS)
        j = ROUNDS - 2
End Sub
```

Encryption process using blowfish can be seen as follow:
Plaintext= DRAGONSS
Key= 3116
Step calculation is done as follows:

a) The initialization of P-Array (P1, P2... P18) is 32 bits, like Table 1.

Table 1: P-Array Conversion to Biner

P-array	Hexa	Biner (32 bit)
P1	243F6A88	00100100 00111111 01101010 10001000
P2	85A308D3	10000101 10100011 00001000 11010011
P3	13198A2E	00010011 00011001 10001010 00101110
P4	3707344	00000011 01110000 01110011 01000100
P5	A4093822	10100100 00001001 00111000 00100010
P6	299F31D0	00101001 10011111 00110001 11010000
P7	82EFA98	00001000 00101110 11111010 10011000
P8	EC4E6C89	11101100 01001110 01101100 10001001
P9	4,53E+11	01000101 00101000 00100001 11100110
P10	38D01377	00111000 11010000 00010011 01110111
P11	BE5466CF	10111110 01010100 01100110 11001111
P12	34E90C6C	00110100 11101001 00001100 01101100
P13	C0AC29B7	11000000 10101100 00101001 10110111
P14	C97C50DD	11001001 01111100 01010000 11011101
P15	3F84D5B5	00111111 10000100 11010101 10110101
P16	B5470917	10110101 01000111 00001001 00010111
P17	9216D5D9	10010010 00010110 11010101 11011001
P18	8979FB1B	10001001 01111001 11111011 00011011

b) Initialization of S-Arrays totaling 255 each in the form of hexadecimal which is then converted to binary, like Table 2.

Table 2: S-Array to Biner

S-Array	Hexa	Biner
S1,0	D1310BA6	11010001 00110001 00001011 10100110
S1,255	6E85076A	01101110 10000101 00000111 01101010
S2,0	4B7A70E9	01001011 01111010 01110000 11101001
S2,255	DB83ADF7	11011011 10000011 10101101 11110111
S3,0	E93D5A68	11101001 00111101 01011010 01101000
S3,255	406000E0	01000000 01100000 00000000 11100000
S4,0	3A39CE37	00111010 00111001 11001110 00110111
S4,255	3AC372E6	00111010 11000011 01110010 11100110

c) Plaintext = DRAGONSS

Table 3 shows plaintext in hexa and biner.

Table 3: Plaintext to Biner

Character	Hexa	Biner
D	44	01000100
R	52	01010010
A	41	01000001
G	41	01000111
O	47	01001111
N	4f	01001110
S	53	01010011
S	53	01010011

d) split into 2 part, name it XL and XR

XL = 01000100 01010010 01000001 01000111
XR = 01001111 01001110 01010011 01010011

e) Key generation:

Key: 3116

Table 4: Key Conversion to Biner

Character	Hexa	Biner
3	33	00110011
1	31	00110001
1	31	00110001
6	36	00110110

Table 4 shows key conversion to biner. Biner: 00110011 00110001 00110001 00110110

f) Sub-key for first iteration:

$P_1 = P_1$ XOR key

P_1 = 00100100 00111111 01101010 10001000

XOR

00110011 00110001 00110001 00110110

P_1 = 00010111 00001110 01011011 10111111

g) Sub-key for another iteration:

$P_2 = P_2$ XOR P_1

P_2 = 10000101 10100011 00001000 11010011

XOR

00110011 00110001 00110001 00110110

P_2 = 10110110 10010010 00111001 11100101

Pseudocode and process above are part of all process from blowfish and LZW, the application is designed by using Visual Basic.Net programming language, for the results of Blowfish and LZW application testing can be seen in Figure 2.

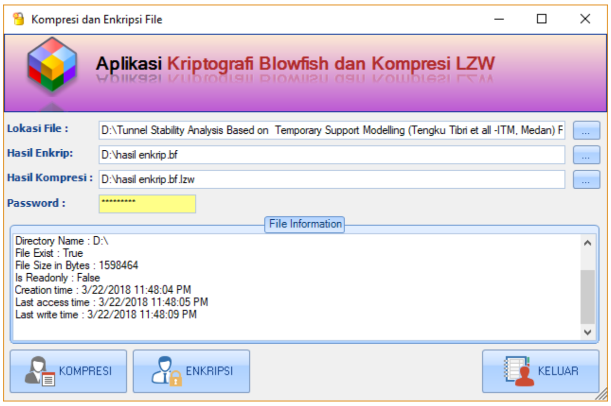

Fig. 2: Encryption and Compression Form.

Figure 2 shows the file information before the encryption and compression process, the next process is to secure data or files with the process of encryption and compression and the result will be save with filename and location that has been set before process encryption and compression.

4. Conclusion

The combination of Blowfish and LZW algorithms can manipulate and minimize data or files that user want to transmit over the network or through other media, this combination is also very likely to be developed in order to produce better security because the compression principle also changes the original form of data to other ben- not easily known by irresponsible parties.

References

[1] S. Renu and S. H. Krishna Veni, "An enhanced security tree to secure cloud data," *Int. J. Eng. Technol*., vol. 7, no. 1.1, pp. 64–70, 2018.

[2] K. Neeraja, P. Rama Chandra Rao, D. Suman Maloji, and D. Mohammed Ali Hussain, "Implementation of security system for bank using open CV and RFID," *Int. J. Eng. Technol*., vol. 7, no. 2–7, p. 187, Mar. 2018.

[3] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci*., vol. 12, no. 22, pp. 6483–6487, 2017.

[4] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," *J. Phys. Conf. Ser*., vol. 930, no. 1, p. 012005, Dec. 2017.

[5] D. Nofriansyah et al., "A New Image Encryption Technique Combining Hill Cipher Method , Morse Code and Least Significant Bit Algorithm," *J. Phys. Conf. Ser*., vol. 954, no. 1, p. 012003, 2018.

[6] R. Rahim et al., "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser*., vol. 1007, no. 1, p. 012003, Apr. 2018.

[7] S. Marrapu, S. Sanakkayala, A. kumar Vempalli, and S. K. Jayavarapu, "Smart home based security system for door access control using smart phone," *Int. J. Eng. Technol*., vol. 7, no. 1, p. 249, Mar. 2018.

[8] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur, vol*. 38, no. October 2013, pp. 97–102, 2013.

[9] D. Coppersmith, J. Stern, and S. Vaudenay, "The security of the birational permutation signature schemes," *J. Cryptol., vol*. 10, no. 3, pp. 207–221, 1997.

[10] R. Rahim et al., "Searching Process with Raita Algorithm and its Application," *J. Phys. Conf. Ser*., vol. 1007, no. 1, p. 012004, Apr. 2018.

[11] D. Abdullah et al., "A Slack-Based Measures for Improving the Efficiency Performance of Departments in Universitas Malikussaleh," *Int. J. Eng. Technol*., vol. 7, no. 2, pp. 491–494, Apr. 2018.

[12] H. Hartono, D. Abdullah, and A. S. Ahmar, "A New Diversity Technique for Imbalance Learning Ensembles," *Int. J. Eng. Technol*., vol. 7, no. 2, pp. 478–483, Apr. 2018.

[13] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, "Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression," *World Trans. Eng. Technol. Educ*., vol. 15, no. 3, pp. 292–297, 2017.

[14] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, pp. 366–371.

[15] E. Kartikadarma, T. Listyorini, and R. Rahim, "An Android mobile RC4 simulation for education," *World Trans. Eng. Technol. Educ*., vol. 16, no. 1, pp. 75–79, 2018.

[16] R. Rahim, A. S. Ahmar, A. P. Ardyanti, and D. Nofriansyah, "Visual Approach of Searching Process using Boyer-Moore Algorithm," *J. Phys. Conf. Ser*., vol. 930, no. 1, p. 012001, Dec. 2017.

[17] M. Trinath Basu and J. K. R. Sastry, "A fully security included cloud computing architecture," *Int. J. Eng. Technol*., vol. 7, no. 2.7 Special Issue 7, pp. 807–812, 2018.

[18] B. Prema Sindhuri and M. Kameswara Rao, "IoT security through web application firewall," *Int. J. Eng. Technol*., vol. 7, no. 2–7, p. 58, Mar. 2018.

[19] A. E. S. Kacaribu and Ratnadewi, "Multiplying cipher images on visual cryptography with ElGamal algorithm," in 2015 *2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2015, pp. 159–162.

[20] Ratnadewi, R. P. Adhie, Y. Hutama, A. Saleh Ahmar, and M. I. Setiawan, "Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC)," *J. Phys. Conf. Ser*., vol. 954, no. 1, p. 012009, Jan. 2018.

[21] R. Rahim, H. Winata, I. Zulkarnain, and H. Jaya, "Prime Number: an Experiment Rabin-Miller and Fast Exponentiation," *J. Phys. Conf. Ser*., vol. 930, no. 1, p. 012032, Dec. 2017.

[22] D. Abdullah, R. Rahim, D. Apdilah, S. Efendi, T. Tulus, and S. Suwilo, "Prime Numbers Comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 978, no. 1, p. 012123.

[23] R. Rahim, D. Hartama, H. Nurdiyanto, A. S. Ahmar, D. Abdullah, and D. Napitupulu, "Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm," *J. Phys. Conf. Ser*., vol. 954, no. 1, p. 012008, 2018.

[24] D. Salomon, Data *Compression the Complete Reference FourthEdition*, vol. 53, no. 9. Springer, 2007.

[25] R. Gonzalez and R. Woods, *Digital image processing*. 2002.

[26] Y. U. Zheng, "Trajectory Data Mining : An Overview," *ACM Trans. Intell. Syst. Technol*., vol. 6, no. 3, pp. 1–41, 2015.

[27] H. Li and P. Liu, "An Identification System Combined with Fingerprint and Cryptography," in *First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06)*, 2006, pp. 105–108.

[28] R. I. Al-Khalid, R. A. Al-Dallah, A. M. Al-Anani, R. M. Barham, and S. I. Hajir, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes," *J. Softw. Eng. Appl*., vol. 10, no. 01, pp. 1–10, Jan. 2017.

[29] S. Bruce, *Applied cryptography*. 1996.

[30] T. Nie, C. Song, and X. Zhi, "Performance evaluation of DES and Blowfish algorithms," in *2010 International Conference on Biomedical Engineering and Computer Science, ICBECS 2010*, 2010.

[31] A. Alabaichi, F. Ahmad, and R. Mahmod, "Security analysis of blowfish algorithm," in *2013 2nd International Conference on Informatics and Applications, ICIA 2013*, 2013, pp. 12–18.