THE USE OF NEURAL NETWORK FOR DATA ENCRYPTION STANDARD (DES)

Roman Zálusky[1], Daniela Ďuračkova[1], Vladimír Sedlák[1], Tomáš Kováčik[1]

[1] Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Ilkovičova 3, 812 19 Bratislava, Slovakia
E-mail: roman.zalusky@stuba.sk

Received 29 April 2013; accepted 14 May 2013

1. Intriduction

Security is a prevalent concern in information and data systems of all types. Historically, military, national security, business and private sectors issues drove the need for secure communications. One means of providing security in communications is trough encryption. By encryption, data are transformed to unrecognizable data. This data can be recovered only by decryption. Data Encryption Standard (DES) was developed in the 1970s by IBM in cooperation with the National Securities Agency (NSA), to encrypt data using a private key algorithm. This paper describe the implementation of DES encryption algorithm with use of the neural networks.

2. Theoretical part

The Data Encryption Standard (DES) has been developed as a cryptographic standard for general use by the public. DES is the most significant modern symmetric algorithm. The algorithm is designed to encrypt a decrypt blocks of data consisting of 64 bits under control of a 56-bit key. Encrypting data converts it to an unintelligible form called cipher. Encryption and decryption must be accomplished by use the same key. The encryption and decryption consists of sixteen Feistel iterations surrounded by two permutation layers. First is the initial permutation at the input, and the other one is its inverse at the output. DES relies upon techniques of confusion and diffusion. Confusion is accomplished through substitution and the diffusion is accomplished through permutation. Permutations and substitutions (S-boxes) are based upon the key and the original text. Principles of Data Encryption Standard are referred in [1-3].

The block diagram of the DES algorithm is shown in Fig.1a. In encryption, firstly the 64-bit of the plain text are subjected to initial permutation. The output of this permutation is divided to two 32-bit blocks L_0 and R_0. It is followed by 16 Feistel rounds. In each round, the second block R_i is fed to a function F and the result is added to the first block L_i. Then both blocks are swapped and the algorithm proceeds to the next iteration. The block diagram of the F function is depicted in Fig.1b. It is key dependent and is divided to four parts. Firstly, the 32-bit input block is expanded to 48 bits by duplicating and reordering half of the bits. This expanded block is XORed with a round subkey constructed by selecting 48 bits from the 56-bit secret key. In each round is used different subkey. The 48-bit result is split into eight 6-bit blocks which are substituted in eight parallel S-boxes. Each one S-box is different, but all have the same special structure. The 32-bits result is reordered with fixed permutation before being sent to the output. The modified R_i block is then XORed with L_i block and the result is fed to the R_{i+1} block. The unmodified block R_i is fed to the L_{i+1} block.

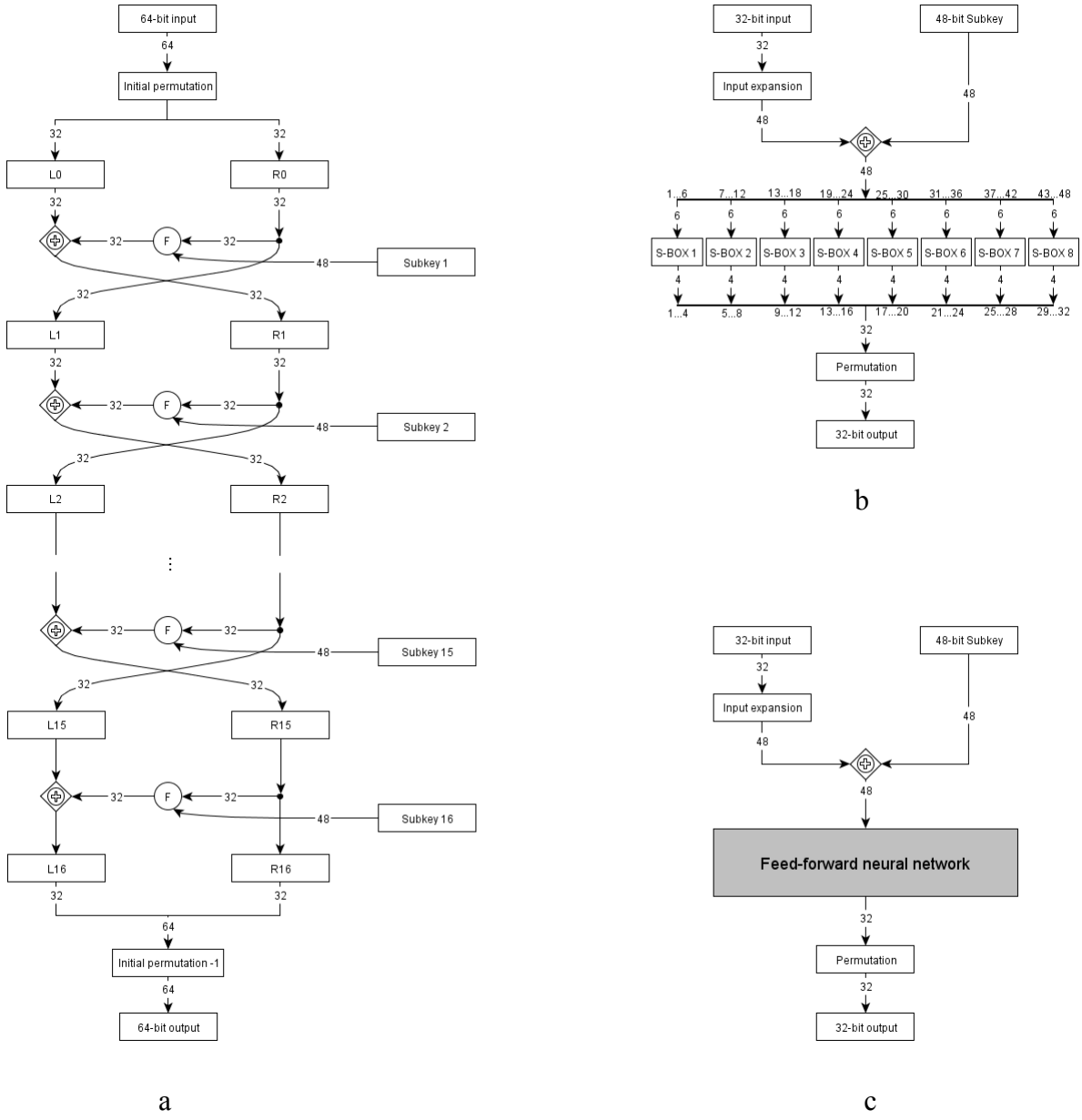

Fig. 1: *Block diagrams of Data Encryption Standard (DES)*

a) DES core algorithm

b) Standard cipher function F

c) Cipher function F with use the neural network

The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations [4].

3. Experimental part

This paper proposed a implementation of Data Encryption Standard (DES) algorithm with the neural network. Basic principles of neural networks are referred in [5–7]. In proposed DES algorithm, the neural network performs the substitutions with S-boxes. In standard DES algorithm, each unique S-box (S-box$_1$, S-box$_2$,..., S-box$_8$) takes a 6-bit block as

input and yields a 4-bit block as output in *F* function (Fig.1b). Standard S-boxes are defined by tables. Table 1 represents the S-box$_1$. Output of the S-box is obtained as follows: The first and the last bit of 6-bit input represent in base 2 a nuber in the range 0 to 3. This number select the row in the table. The middle 4-bits of input represent in base a number in the range 0 to 15 which select the column in the table. Output of the S-box is then the 4-bit number on seleted row a column.

Tab. 1. Example of representation of the S-box (S-box$_1$)

	Column Number															
Row No.	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

The block of the Feed-forward neural network performs all partial substitutions (Fig.1c). Neural network has eight 6-bit inputs and eight 4-bit outputs. It contains two hidden layers with 160 hidden neurouns in the first hidden layer and 40 hidden neurons in the second hidden layer. We verified the functionality of proposed DES algorithm. Both algorithms standard and proposed were realized in Matlab. Algorithms works with ASCII text or hexadecimal representation. For better readability, we present data in the hexadecimal form.

Input data consists of 64-bit random generated numbers in hexadecimal format. Firstly, we performs data encryption with standard DES algorithm and the decryption with proposed DES algorithm containing the feed-forward neural network. For all operations was used the same key. We have done 100 encryption and decryption proceses for different input data. Part of the obtained result are presented in Table 2. All decrypted data coincides with the input data. Next, we tested the proposed algorithm in the reverse order. Plain data are encrypted with DES algorithm, which use the neural network and decrypted with standard algorithm. In this test, we also performed 100 encryption and decryption proceses for the same input data as in the previous test and with the same key. Table 3 shows a part of achieved data. Both tests have demonstrated proper functionality of proposed DES algorithm with feed-forward neural network.

Tab. 2. Data encryption with standard DES and decryption with DES using neural network with key AB12C4DF679EE5A4 in hexadecimal form

Plain data (HEX)	**Encrypted data (HEX)**	**Decrypted data (HEX)**
1234567812345678	05AFCF7A9D025E53	1234567812345678
76D6E788DC5A99E5	664A4F0A6D0528A3	76D6E788DC5A99E5
3546739DACFE65FF	A3AF6A0FC3127C84	3546739DACFE65FF

Tab. 3. Data encryption with DES using the neural network and decryption with standard DES algorithm with key AB12C4DF679EE5A4 in hexadecimal form

Plain data (HEX)	**Encrypted data (HEX)**	**Decrypted data (HEX)**
1234567812345678	05AFCF7A9D025E53	1234567812345678
76D6E788DC5A99E5	664A4F0A6D0528A3	76D6E788DC5A99E5
3546739DACFE65FF	A3AF6A0FC3127C84	3546739DACFE65FF

4. Conclusion

A modified algorithm of Data Encryption Standard (DES), which uses the neural network has been designed. The neural network was used to perform the substitutions with S-boxes in function *F*. The proposed DES algorithm was compared with standard algorithm and its encryption and decryption capability was evaluated. We have done two tests. In first test was data encrypted with stadndard DES algorithm and decrypted with proposed algorithm. The other test was performed in reverse order. We have tested on 100 randomly generated 64-bit blocks. Both tests have demonstrated proper functionality of proposed DES algorithm with feed-forward neural network.

Acknowledgement
This work supported in part by the Research and Development Operational Programme from the ERDF under "Competence Center for SMART Technologies fo Electronics and Informatics Systems and Services, ITMS 26240220072", ENIAC-JU project MAS (Agreement no. 120228), and the Ministry of Education, Science, Research and Sport of the Slovak Republic under grants VEGA 1/0987/12 and VEGA 1/0823/13.

References:

[1] E. Biham and A. Shamir: Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New-York (1993).
[2] NIST: Data Encryption Standard. Technical Report FIPS PUB 46-3, National Institute of Standards and Technology, Washington DC (1977).
[3] D. Coppersmith: The Data Encryption Standard (DES) and its Strength Against Attacks. IBM Journal of Research and Development (1994).
[4] B. Scheier: Applied Cryptography: Protocols, Algorithms and Source Code in C. John WIley & Sons (1995).
[5] V. Kvasnička, Ľ. Beňušková, I. Farkaš, A. Kráľ, J. Pospíchal and P. Tiňo: Introduction into the neural networks (In Slovak), IRIS, Bratislava, (1997).
[6] Sinčák and G. Andrejková: Neural Networks (The engineering methodology) part 1. (In Slovak), Elfa s.r.o., Košice (1996).
[7] C. R. Alavala: *Logic and Neural Networks: Basic concepts and applications*, New Age Publications , (2007).