Journal of Engineering and Applied Sciences
MEDWELL PUBLICATIONS

A New Operation in Cryptology (Noise-Injection)

Y. Benlcouiri, M. Benabdellah, M.C. Ismaili and A. Azizi
Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University, Oujda, Morocco

Key words: Cryptology-By-Noise-Injection (CBNI)

Corresponding Author:
Y. Benlcouiri
Laboratory of Arithmetic, Scientific Computing and Applications, Faculty of Science, Mohamed First University, Oujda, Morocco

Page No.: 237-238
Volume: 16, Issue 7, 2021
ISSN: 1816-949x
Journal of Engineering and Applied Sciences

Abstract: The existing operations in cryptology are substitution and permutation. The main idea of this study consist to define a new operation in cryptology.

INTRODUCTION

The most methods of encryption based on two principles: substitution and transposition substitution means that replacing some letters by symbols or others. Transposition means that permuting the letters of the message to make it unintelligible. Over the centuries, many systems of cryptographic TMIS have developed more perfection more clever[1, 2].

The existing stegano-system by secret key[3] have touch the idea of noise injection. We assume that if the principle of key is existing in hidden information that can be considered as a crypto-system[4].

The body of the present work will be organized as follow. In the second section, we present the CBNI principle in encryption and decryption. Then, in the third section, we conclude this work by redefining Shannon's definition[5].

Noise-injection operation: The principle of noise-injection operation is to add an information to the clear message for encryption and eliminate it to decryption. This operation can be schematized as follow (Fig. 1).

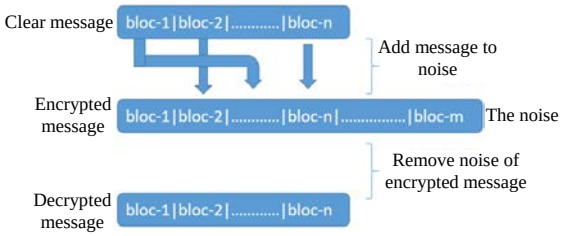

Fig. 1: Noise-injection operation

Inject the message in noise product an encrypted message; several method can be realize that such as pseudo-random generator when the results is the emplacement of message in the noise. Then, the decryption is the inverse of operation of encryption[6].

CONCLUSION

The Shannon definition of cryptology seams that substitution and/or permutation. Then, we add noise-injection. The redefinition of operation of cryptology is substitution and/or permutation and/or noise-injection.

REFERENCES

01. Schneier, B., 1997. Cryptographie Appliquee. 2nd Edn., Wiley and International Thomson Publishing, New York, USA.,.
02. Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2013. Encryption of ultrasound images using the permutation on the (Z/pZ) fields. Int. J. Applied Math. Sci., 7: 2093-2102.
03. Benlcouiri, Y., M. Ismaili, A. Azizi and M. Benabdellah, 2012. Securing images by secret key steganography. Applied Math. Sci., 6: 5513-5523.
04. Das, D. and R.R. Mary, 2017. Real time noise filtering for low cost IMU sensors. Asian J. Inf. Technol., 16: 536-543.
05. Ojha, S.K., O.P. Singh, G.R. Mishra and P.R. Vaya, 2018. Effect of threshold roll-off on static noise margin of sram cell. J. Eng. Applied Sci., 13: 5801-5806.
06. Serrezuela, R.R., A.L.P. Salazar, J.B.R. Zarta and L.A.C. Pinilla, 2018. Industrial application of optimal filtering for states polynomials incompletely measurable with cross noise. J. Eng. Applied Sci., 13: 2536-2543.