

# Signal multiple encodings by using autoencoder deep learning

Ammar Sameer Anaz<sup>1</sup>, Moatasem Yaseen Al-Ridha<sup>2</sup>, Raid Rafi Omar Al-Nima<sup>2</sup>

<sup>1</sup>Basic Education College, University of Mosul, Mosul, Iraq

<sup>2</sup>Technical Engineering College, Northern Technical University, Mosul, Iraq

---

## Article Info

### Article history:

Received Jun 10, 2022

Revised Sep 1, 2022

Accepted Sep 21, 2022

### Keywords:

Autoencoder deep learning

Decryption

Encryption

Security

---

## ABSTRACT

Encryption is a substantial phase in information security. It permits only approved persons to get private information. This study suggests a signal multi-encryptions system (SMES) technique for coding and decoding signals created by a deep autoencoder network (DAN). The DAN of four layers is employed for a coding package of signals multiple times before decoding or restructuring the original signals again. The suggested SMES offers a high level of security as it can produce and exploit multiple encryptions for signals. Many statistical calculations are applied to measure the reliability of the system. The outcomes are promising where noteworthy encryptions-decryptations are obtained.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



---

## Corresponding Author:

Ammar Sameer Anaz

Basic Education College, University of Mosul

Mosul, Iraq

Email: ammars.anaz@uomosul.edu.iq

---

## 1. INTRODUCTION

Encryption is a form of transforming information where the generated data cannot be detected by unauthorized persons. Decryption is a way to restore encrypted data into its original structure [1], [2]. The proper decryption key is required to reconstruct the contents of the encrypted information. The function of the key is to reverse the work of the encryption process. The more complex the encryption technology, the more demanding it is [3]. Encryption and decryption are both included in a big field called cryptography [4]–[7], which is also be concentrated in this paper.

Encryption was studied in many papers [7]–[11]. According to Qin *et al.* [12] studied deep learning applications in physical layer communications for systems with and without block structures. Authors here used the block structure to show how deep learning can be used for signal compression and identification in deep learning-based communication systems. They also discussed ongoing efforts for building end-to-end communication networks based on deep learning [12]. In the same year, Fadhil *et al.* proposed forward artificial neural network encoder with a main structure built by the self organizing feature map (SOM). The forward neural network dimension is initially chosen based on the number of bits in a code word and source bits. The code word uniqueness was checked to ensure that it matched existing data. For decoding, a spike neural network was used. Its performance depended on the size of the source dimension or the amount of bits in the code word [13]. Ye *et al.* [14] suggested to use a conditional generative adversarial network for representing channel effects and bridges between the transmitter deep neural networks (DNN) and receiver DNN. From results, the suggested method was active in additive white gaussian noise (AWGN) channels, frequency-selective channels and rayleigh fading channels [14]. Sassi *et al.* [15] modified posterior decoding algorithm to solve hidden Markov models by machine learning algorithms which deal with big data tasks. The authors succeeded in improving an algorithm to reduce time complexity and yield effective outcomes in

speedup, running time and high data volume parallelization efficiency. Kadum *et al.* [16] proposed a system that avoided unofficial access and spy by using dual adapted Hebbian neural network for encrypting data. Machine learning and deoxyribonucleic acid (DNA) were used to compress and growth data confusion. The method succeeded by transferring data in a secure manner and short time [16]. In the same year, Maalood *et al.* [17] suggested a lightweight stream cipher method. Then, it was tested for numerous video samples to check its suitability and authentication in encryption and decryption procedures. After testing many characteristics such as differential analysis, correlation analysis, information entropy and histogram analysis, their method showed a higher security and lower calculation time compared with state-of-the-art encoding methods [17]. From the literature, it can be noticed that the strength of encryption and the time of encryption and decryption are very important factors in cryptography. Here, both factors are considered.

Our work contributes to the field of security by proposing an intelligent algorithm for encrypting multiple signals called the deep autoencoder network (DAN). The generated codes are difficult to be predicted by unreliable people. The goal here is to build a highly secured encryption system called the signal multi-encryptions system (SMES). The remaining sections will be provided as follows: section 2 illustrates the theory of the overall cryptography algorithm; section 3 states the results and discussion, and section 4 concludes the paper.

## 2. METHOD

The main SMES concept is encrypting signal information multiple times, it is based on a DAN. Firstly, the input signal is converted into a one-dimensional (1D) matrix of size  $1 \times n$  elements, where  $n$  is the number of elements in any original signal and it is here equal to 172,890 values. Then, it is entered into the 1<sup>st</sup> hidden layer (or first encryption layer), and the weights between the input signal and the first hidden layer can be used as the first encryption key. The encrypted data is then sent to the 2<sup>nd</sup> hidden layer (or second encryption layer) using the weights between the first and second hidden layers, which can be utilized as a second key. This process can be extended to the  $N^{\text{th}}$  number of hidden layers ( $N$  here is used equal to 3 hidden layers). To find the best number of hidden nodes (or neurons) in the encryption layers, the number of hidden nodes is equally changed for all the used hidden layers to 4, 8, 16, 32, 46, and 128 nodes. Consequently, different measurements of error ratios and training times are considered, as will be declared later. On the other hand, the output layer (last layer) is employed for the decryption. It decrypts the multi-encrypted information and reconstructs the original signal by exploiting the weights between the last hidden layer and the output layer, which represent the final key. The general structure of the suggested SMES is illustrated in Figure 1. All experiments in this study are executed under the matrix laboratory (MATLAB) software of version is R2020b (9.9.0.1467703) 64 bits.

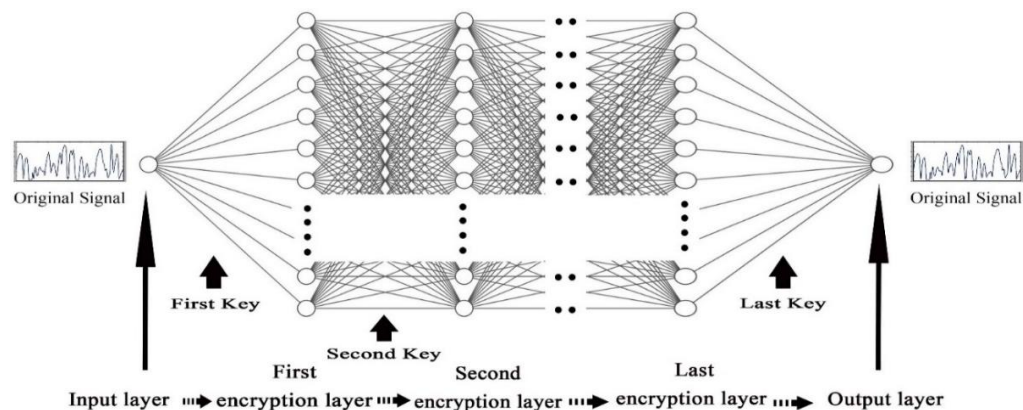


Figure 1. The general architecture of the suggested SMES

### 2.1. Deep autoencoder network

The DAN is a type of deep learning, which is advanced machine learning. Deep learning is widely employed in artificial intelligence domains such as medicine [18], images processing [19], information and sound application [20], computer vision [21], and many more applications [15], [22]–[28]. In this paper, the DAN is suggested, implemented and evaluated. It has three layers: input, many hidden layers and output layer. The backpropagation training algorithm is utilized by exploiting the input values as targets.

## 2.2. Encryption

Encryption is a method of encoding data [29]. It transforms original signals, which are the original representations of data, into coded signals. Only authorized humans are allowed to decode coded signals and view the original data.

## 2.3. Decryption evaluation

To evaluate the decryption's reliability, many measurement equations have been used to calculate the errors between original signals and restored (or decrypted) signals. Low error values show high performances. Whereas, high error values show low performances. Such equations include:

### 2.3.1. Mean square error

Mean square error (MSE) measures the errors of mean squares. This measurement is represented by the following [30]:

$$MSE = \frac{1}{n} \sum_{i=1}^n (I_i - O_i)^2 \quad (1)$$

where  $MSE$  is the MSE error,  $n$  is the number of elements in any original or restored signal,  $I$  is the original signal and  $O$  is the restored signal.

### 2.3.2. Peak signal to noise ratio

Peak signal to noise ratio (PSNR) is the ratio of the maximum possible signal power to the power of the corrupting noise. It is usually measured in decibel. The following is an example of PSNR computation [30]:

$$PSNR = 10 \log \frac{l^2}{MSE} \quad (2)$$

where PSNR is the PSNR error and  $l$  is the maximum peak value.

### 2.3.3. Average difference

Average difference (AD) considers the mean between the original and restored signals. AD can be represented as follows [30]:

$$AD = \frac{1}{n} \sum_{i=1}^n |I_i - O_i| \quad (3)$$

where  $AD$  is the AD of error.

### 2.3.4. Maximum difference

Maximum difference (MD) measures the maximum absolute difference between the original and restored signals. MD is denoted as follows [30]:

$$MD = \text{Max}(|I_i - O_i|) \quad (4)$$

where  $MD$  is the MD error.

### 2.3.5. Normalized absolute error

This technique measures exactly what is the difference between the processed signal and the original signal. Normalized absolute error (NAE) is defined as follows [30].

$$NAE = \frac{\sum_{i=1}^n (|I_i - O_i|)}{\sum_{i=1}^n (I_i)} \quad (5)$$

where  $NAE$  is the NAE error.

## 3. RESULTS AND DISCUSSION

Database of DIVERse 2K (DIV2K) is used. It can be considered as a set of signals [31]. In this study, we tried to encode signals using the suggested deep learning. We have tested and compared the results of outputs and inputs. The system achieved good results for complex coding with more than one stage. Three hidden layers are used for our experiments. The proposed DAN is checked for the appropriate size of nodes

in the hidden layers in order to achieve the most acceptable performance by giving the lowest results of error rates. The number of hidden neurons in all three hidden layers is changed for the values of 4, 8, 16, 32, 64 and 128 nodes. Each of these sizes is evaluated by applying the error measurement equations of the MSE, PSNR, AD, MD, and NAE. Table 1 shows the DAN performances of errors for the different numbers of hidden neurons. While Table 2 measures the training time for each case of changing the number of hidden neurons.

Table 1. DAN performances of errors for the different numbers of hidden neurons

Error Type	4	8	16	32	64	128
	hidden neurons	hidden neurons	hidden neurons	hidden neurons	hidden neurons	hidden neurons
MSE	0.17	$5.42 \times 10^{-10}$	0.17	$3.22 \times 10^{-9}$	$3.19 \times 10^{-10}$	0.17
PSNR	55.71	140.78	55.71	133.04	143.08	55.71
AD	0.36	$2.18 \times 10^{-8}$	0.35	$8.37 \times 10^{-8}$	$2.06 \times 10^{-8}$	0.35
MD	0.89	$1.21 \times 10^{-4}$	0.89	$99 \times 10^{-4}$	$59 \times 10^{-4}$	0.89
NAE	1	$2.39 \times 10^{-5}$	1	$4.36 \times 10^{-5}$	$5.22 \times 10^{-6}$	1

This table shows that the PSNR error attained a good value for 64 neurons in the hidden layers, because higher value means more quality of output reconstructions. The results in the values of AD errors show that the lowest value is for the number of 64 neurons in the hidden layers too. NAE error values also show that 64 neurons in the hidden layers have the minimum value. Only the MD error obtained the minimum value for 8 neurons. After comparing the error values and considering that the more complex code causes greater strength, the number of 64 neurons in the hidden layers seems the best choice for our multi-stage code generations.

The training time increases with the number of hidden neurons in the hidden layer, see Table 2. The fundamental reason for a large number of hidden layers is that each point in the signal has its own neurons on the processing line from the input layer to the output layer in DAN, which allows for a complicated encryption scheme. In the Table 2, it is clear that increasing the number of neurons leads to an increase in the training time by assuming a constant data size this must be taken into account if this system is implemented in real-time systems.

Table 2. Training time of each DAN according to its number of hidden neurons

Numbers of hidden neurons	4	8	16	32	64	128
Time in seconds	15.47	41.53	38.40	113.86	318.96	555.18

#### 4. CONCLUSION

An MES system based on DAN was proposed in this study. Several encryption layers make up the proposed system. To begin, the input layer is established to read signal data and generate the initial key and encryption procedure on the signal input. From the input encoded signal, each encryption layer generates its own keys. The last layer decrypts the encoded signal and reconstructs the original signal using its key and inputted signal to it. Signals are successfully tested using the  $N^{\text{th}}$  encryption procedure once the system is constructed. Many error measurement formulas were used to calculate the optimal system performance after changing concealed size layers. This reliable technology may be used to deliver a critical notification while maintaining a high level of security. When you're concealed, you'll obtain the finest results.

#### ACKNOWLEDGEMENTS




Authors would like to thank the Basic Education College/University of Mosul/Iraq and Technical Engineering College/Northern Technical University/Mosul/Iraq. Also, thanks to Mr. Eirikur Agustsson and Mr. Radu Timofte for their available database.

#### REFERENCES




- [1] H. Grari, S. Lamzabi, A. Azouaoui, and K. Z-Dine, "Cryptanalysis of Merkle-Hellman cipher using ant colony optimization," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 2, pp. 490-500, Jun. 2021, doi: 10.11591/ijai.v10.i2.pp490-500.
- [2] R. Al-Jawadi and R. Al-Naima, "Hybridization of genetic algorithm with neural networks to cipher english texts," *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 7, no. 3, pp. 77-90, Dec. 2010, doi: 10.33899/csmj.2010.163928.

- [3] R. R. Al-Nima, A. N. Hamed, and R. Y. Srdeeq, "Multiple data type encryption using genetic neural network," *Tikrit Journal of Engineering Sciences*, vol. 17, no. 2, pp. 51–57, Jun. 2010, doi: 10.25130/tjes.17.2.05.
- [4] M. Ubaidullah and Q. Makki, "A review on symmetric key encryption techniques in cryptography," *International Journal of Computer Applications*, vol. 147, no. 10, pp. 43–48, Aug. 2016, doi: 10.5120/ijca2016911203.
- [5] S. Adamovic, M. Sarac, D. Stamenkovic, and D. Radovanovic, "The importance of the using software tools for learning modern cryptography," *International Journal of Engineering Education*, vol. 34, no. 1, pp. 256–262, 2018.
- [6] D. A. Q. Shakir and A. J. Dawood, "3D chaos graph deep learning method to encrypt and decrypt digital image," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, pp. 941–951, Feb. 2022, doi: 10.11591/ijeecs.v25.i2.pp941-951.
- [7] C. Yuan, C. Wu, D. Cheng, and Y. Yang, "Deep learning in encoding and decoding of polar codes," *Journal of Physics: Conference Series*, vol. 1060, no. 1, 2018, doi: 10.1088/1742-6596/1060/1/012021.
- [8] N. Yu, Z. Li, and Z. Yu, "Survey on encoding schemes for genomic data representation and feature learning—from signal processing to machine learning," *Big Data Mining and Analytics*, vol. 1, no. 3, pp. 191–210, Sep. 2018, doi: 10.26599/bdma.2018.9020018.
- [9] T. Wang, C.-K. Wen, H. Wang, F. Gao, T. Jiang, and S. Jin, "Deep learning for wireless physical layer: opportunities and challenges," arXiv, Oct. 27, 2017, doi: 10.48550/arXiv.1710.05312.
- [10] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85–117, Jan. 2015, doi: 10.1016/j.neunet.2014.09.003.
- [11] H.-H. Wang, J.-M. Liu, M. You, and G.-Z. Li, "Audio signals encoding for cough classification using convolutional neural networks: A comparative study," Nov. 2015, doi: 10.1109/bibm.2015.7359724.
- [12] Z. Qin, H. Ye, G. Y. Li, and B.-H. F. Juang, "Deep learning in physical layer communications," *IEEE Wireless Communications*, vol. 26, no. 2, pp. 93–99, Apr. 2019, doi: 10.1109/mwc.2019.1800601.
- [13] M. J. Fadhil, M. A. Najj, and G. A. Salman, "Transceiver error reduction by design prototype system based on neural network analysis method," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 3, pp. 1244–1251, Jun. 2020, doi: 10.11591/ijeecs.v18.i3.pp1244-1251.
- [14] H. Ye, L. Liang, G. Y. Li, and B.-H. Juang, "Deep learning-based end-to-end wireless communication systems with conditional GANs as unknown channels," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3133–3143, May 2020, doi: 10.1109/twc.2020.2970707.
- [15] I. Sassi, S. Anter, and A. Bekkhoucha, "A spark-based parallel distributed posterior decoding algorithm for big data hidden markov models decoding problem," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 3, pp. 789–800, 2021, doi: 10.11591/ijai.v10.i3.pp789-800.
- [16] S. A. Kadum, A. Y. Al-Sultan, and N. A. Hadie, "Data protection based neural cryptography and deoxyribonucleic acid," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 2756–2764, Jun. 2022, doi: 10.11591/ijece.v12i3.pp2756-2764.
- [17] A. T. Maolood, E. K. Gbashi, and E. S. Mahmood, "Novel lightweight video encryption method based on ChaCha20 stream cipher and hybrid chaotic map," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 5, pp. 4988–5000, Oct. 2022, doi: 10.11591/ijece.v12i5.pp4988-5000.
- [18] M. Y. Al-Ridha, A. S. Anaz, and R. R. O. Al-Nima, "Expecting confirmed and death cases of covid-19 in Iraq by utilizing backpropagation neural network," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 4, pp. 2137–2143, Aug. 2021, doi: 10.11591/eei.v10i4.2876.
- [19] R. R. O. Al-Nima, S. Q. Hasan, and S. Esmail, "Exploiting the deep learning with fingerphotos to recognize people," *International Journal of Advanced Science and Technology*, vol. 29, no. 7, Jul. 2020.
- [20] A. P. Gudmalvar, C. V. R. Rao, and A. Dutta, "Improving the performance of the speaker emotion recognition based on low dimension prosody features vector," *International Journal of Speech Technology*, vol. 22, no. 3, pp. 521–531, Dec. 2018, doi: 10.1007/s10772-018-09576-4.
- [21] J. Kim, J. Ko, H. Choi, and H. Kim, "Printed circuit board defect detection using deep learning via a skip-connected convolutional autoencoder," *Sensors*, vol. 21, no. 15, p. 4968, Jul. 2021, doi: 10.3390/s21154968.
- [22] G. Lăzăroiu, M. Andronie, M. Iatagan, M. Geamănu, R. Ștefănescu, and I. Dîjmărescu, "Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things," *ISPRS International Journal of Geo-Information*, vol. 11, no. 5, p. 277, Apr. 2022, doi: 10.3390/ijgi11050277.
- [23] X. Yang, S. Zhang, J. Liu, Q. Gao, S. Dong, and C. Zhou, "Deep learning for smart fish farming: applications, opportunities and challenges," *Reviews in Aquaculture*, vol. 13, no. 1, pp. 66–90, Jun. 2020, doi: 10.1111/raq.12464.
- [24] P. H. Yi *et al.*, "Can AI distinguish a bone radiograph from photos of flowers or cars? Evaluation of bone age deep learning model on inappropriate data inputs," *Skeletal Radiology*, vol. 51, no. 2, pp. 401–406, Aug. 2021, doi: 10.1007/s00256-021-03880-y.
- [25] M. Uzun, M. U. Demirezen, and G. Inalhan, "Physics guided deep learning for data-driven aircraft fuel consumption modeling," *Aerospace*, vol. 8, no. 2, p. 44, Feb. 2021, doi: 10.3390/aerospace8020044.
- [26] S. Amirian, K. Rasheed, T. R. Taha, and H. R. Arabia, "Automatic generation of descriptive titles for video clips using deep learning," in *Transactions on Computational Science and Computational Intelligence*, Springer International Publishing, 2021, pp. 17–28, doi: 10.1007/978-3-030-70296-0\_2.
- [27] M. Fu, Q. Zhong, and J. Dong, "Sports action recognition based on deep learning and clustering extraction algorithm," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–9, Mar. 2022, doi: 10.1155/2022/4887470.
- [28] R. de Q. Mendes, E. G. Ribeiro, N. dos S. Rosa, and V. Grassi, "On deep learning techniques to boost monocular depth estimation for autonomous navigation," *Robotics and Autonomous Systems*, vol. 136, p. 103701, Feb. 2021, doi: 10.1016/j.robot.2020.103701.
- [29] B. K. A. Ahmed, R. D. Mahdi, T. I. Mohamed, R. A. Jaleel, M. A. Salih, and M. M. A. Zahra, "A novel secure artificial bee colony with advanced encryption standard technique for biomedical signal processing," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 1, p. 288, Jan. 2022, doi: 10.21533/pen.v10i1.2610.
- [30] F. Memon, M. Ali Unar, and M. Sheeraz, "Image quality assessment for performance evaluation of focus measure operators," *Mehran University Research Journal of Engineering & Technology*, vol. 34, no. 4, pp. 389–386, 2015, doi: <https://doi.org/10.48550/arXiv.1604.00546>.
- [31] R. Timofte *et al.*, "NTIRE 2018 challenge on single image super-resolution: methods and results," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Jun. 2018, pp. 965–96511, doi: 10.1109/CVPRW.2018.00130.




**BIOGRAPHIES OF AUTHORS**

**Ammar Sameer Anaz**    received the B.Sc and M.Sc degrees in Technical Computer Engineering in 2006 and 2018, respectively. During 2018, he worked as an Assistant Lecturer in the Basic Education College in University of Mosul, Iraq. His research interests are in the fields of real time applications, artificial intelligence, and image processing. He can be contacted at email: ammars.anaz@uomosul.edu.iq.



**Moatasem Yaseen Al-Ridha**    received the B.Sc degrees in Technical Computer Engineering in 2006. In 2013, he accomplished his master's degree in the School of Electrical and Computer Engineering at Southern Illinois University-USA. His research interests are in the fields of image processing, signal processing, pattern recognition, security, and artificial intelligence. He can be contacted at email: moatasem@ntu.edu.iq.



**Raid Rafi Omar Al-Nima**    received the B.Sc and M.Sc degrees in Technical Computer Engineering in 2000 and 2006, respectively. During 2006, he worked as an Assistant Lecturer in the Technical College of Mosul, Iraq. In 2011, he obtained the Lecturer scientific title in the same college. In 2017, he accomplished his Ph.D in the School of Electrical and Electronic Engineering at Newcastle University, UK. In 2020, he achieved the title of Assistant Professor in the Northern Technical University. His research interests are in the fields of pattern recognition, security, artificial intelligence, and image processing. He can be contacted at email: raidrafi3@ntu.edu.iq.