Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032838
Article

Tech Science Press

Split-n-Swap: A New Modification of the Twofish Block Cipher Algorithm

Awny Sayed[1,2], Maha Mahrous[3] and Enas Elgeldawi[1,*]

[1]Computer Science Department, Faculty of Science, Minia University, Minia, 61519, Egypt
[2]Faculty of Computing and Information Technology, Information Technology Department, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Computer Science Department, Faculty of Computers and Information, Minia University, Minia, 61519, Egypt
*Corresponding Author: Enas Elgeldawi. Email: enas.elgeldawi@mu.edu.eg
Received: 31 May 2022; Accepted: 04 July 2022

Abstract: Securing digital data from unauthorized access throughout its entire lifecycle has been always a critical concern. A robust data security system should protect the information assets of any organization against cybercriminal activities. The Twofish algorithm is one of the well-known symmetric key block cipher cryptographic algorithms and has been known for its rapid convergence. But when it comes to security, it is not the preferred cryptographic algorithm to use compared to other algorithms that have shown better security. Many applications and social platforms have adopted other symmetric key block cipher cryptographic algorithms such as the Advanced Encryption Standard (AES) algorithm to construct their main security wall. In this paper, a new modification for the original Twofish algorithm is proposed to strengthen its security and to take advantage of its fast convergence. The new algorithm has been named Split-n-Swap (SnS). Performance analysis of the new modification algorithm has been performed using different measurement metrics. The experimental results show that the complexity of the SnS algorithm exceeds that of the original Twofish algorithm while maintaining reasonable values for encryption and decryption times as well as memory utilization. A detailed analysis is given with the strength and limitation aspects of the proposed algorithm.

Keywords: Twofish; advanced encryption standard (AES); cryptography; symmetric key; block cipher

1 Introduction

Data security has become a burning issue in the past decade as the amount of data over the Internet increases exponentially every day especially after the introduction of cloud computing technologies. Critical transactions and sensitive data are required to traverse daily over the Internet. All data platforms such as e-banking platforms [1,2], cloud computing service platforms [3,4], and social networks platforms [5–8] have become vulnerable to various types of attacks.

Various symmetric key block cipher cryptographic algorithms provide a good level of security and have been adopted by many platforms, but with the enormous introduction of new technologies, new levels of security should be introduced as well. Previous security algorithms may not be the best choice for todays' needs. Either new cryptography algorithms should be developed, or extra complexity should be added to existing algorithms.

Twofish is a symmetric key cryptography algorithm developed by Bruce Schneier and was one of the five finalists of the Advanced Encryption Standard contest. Over the past years Twofish has been used in a number of firms to secure their infrastructure. However, other cryptography algorithms such as AES or Rivest's cipher (RC) are considered more favorable and much appealing because of their better security. While such algorithms may be of better security, their slow convergence is still an issue. Twofish has proven to be one of the fastest cryptography algorithms.

In this paper, a modification for the Twofish algorithm have been proposed, namely Split-n-Swap (SnS), to strengthen the security via increasing the complexity of the algorithm. Several metrics have been used to test the performance of the proposed algorithm. The paper is organized as follows: Related work is given in Section 2. An overview of the Twofish algorithm is given in Section 3. An explanation of Split-n-Swap algorithm is given in Section 4. Experimental results and conclusion are given in Sections 5 and 6 respectively.

2 Related Work

Since the introduction of new technologies and platforms such as cloud computing, Internet of Things (IoT), and social networking as an important paradigm to access and share data and resources over this huge network, an emergent security issue has raised to secure such data. And despite of other major concerns of these technologies such as performance and cost [9,10], security became the burning concern that must be achieved. The literature is rich of related work reviewing and comparing different block cipher algorithms. This section surveys previous work done in symmetric block cipher and the modifications made to different block cipher algorithms including Twofish modification.

A number of reviews has been introduced to compare between various symmetric and non-symmetric cryptography algorithms [11–19].

Several modifications have been done to enhance some block cipher algorithms. In [20], the authors tried to make alterations to the Blowfish algorithm by enlarging the block to be 128-bits block size instead of 64-bits through rounds determination in a random way. Experimental results showed that the modifications improved the performance and execution time.

Another try by [21], the author suggests a new S-box generation process of Blowfish algorithm based on Self Synchronization Stream Cipher (SSS) algorithm. These alterations resulted in extra difficulty for the analysis of P-array and S-box. To generate the subkeys a total of 272 iterations is required by the suggested algorithm compared to 521 iterations. The algorithm has showed to improve memory size as it does not store the subkeys saving approximately 4 kB of memory.

A new idea was published by [22], they presented what is called Inter Bit Exchange and Merge (IBEM) for data before it is used as an input to S-Boxes. IBEM pattern of data prohibits the intruders from finding the mechanism of generating key that the user actually sends to improve the security level of Blowfish. A modification for the AES algorithm is presented in [23]. The authors tried to optimize the standards of cryptography already used for the encryption of images and text data. They borrowed the Initial permutation step, from Data Encryption Standard (DES), to reach a more encryption performance. The main objective of modifying AES is to attain better secured data and

higher encryption speed by less computation. To supersede the challenge of high calculation, the modified algorithm exchanged the MixColumn step with permutation step. This permutation step and its tables are got from the DES algorithm.

In [24], they are aiming to address the low diffusion rate at early rounds of the AES which altered by the addition of supplementary primitive operations such as exclusive OR and modulo arithmetic in the cipher round. Moreover, byte substitution and round constant addition were added to the key schedule algorithm. This modification of AES was evaluated by methods of avalanche effect and frequency test to determine the confusion and diffusion properties. The avalanche effect evaluation results show an increasing average of diffusion in many rounds, and also frequency test results show a progress in the randomness of the cipher text.

In [25], the authors implemented the Twofish algorithm using Xilinx xst-6.1 and Model-Sim Simulator, the language used for their implementation was Very High-speed integrated circuit hardware Description Language (VHDL). They have modified both the Maximum Distance Separable (MDS) and Pseudo-Hadamard Transform (PHT) functions, the resulting algorithm showed better performance than the original Twofish algorithm.

In [26], a sequential and parallel implementation have been tested over the IMAN1 Supercomputer using Message Passing Interface (MPI). The parallel Implementation has been evaluated in terms of execution time, speedup, and efficiency. According to their results, parallel Twofish implementation has better execution time for large date size than small data size. However, using a large number of processors on small data size will increase running time as the amount of communication between processors will be huge. The experimental results show that the running time decreased as well as the speed-up of encryption and decryption processes increased when eight processors is used.

The authors in [27] introduced a modified Twofish algorithm by adding a new module based on a new function called cyclic group extended. This function is added to turn up the algorithm randomness. This Function uses 8-bits and 30 tables structured with cyclic group and multiplication in Galois Field. They used two keys, the first key is used to choose a table among the 30 tables, and the second key is used for the encryption and decryption processes. The statistical analysis shows that the proposed algorithm gives more complexity than the original Twofish algorithm.

The authors in [28] proposed a model for cloud database storage of a healthcare system using the Twofish algorithm as the main data security system for encrypting and decrypting data. The paper employs Twofish algorithm for encryption to protect the integrity of the patients' data from unauthorized access and attacks.

3 Overview of the Twofish Algorithm

Twofish is considered one of the symmetric key block cipher cryptography algorithm.

It is designed by Bruce Schneier [29–32] and has chosen to be one of the five finalists of the Advanced Encryption Standard contest. Twofish is a varied key size algorithm with 128 bits block size. Twofish follow the Feistel network design which means that in each round, half of the text block is sent through an F function, and then XORed with the other half of the text block. A typical structure of Feistel network is show in Fig. 1. One of the strength of Twofish is that its implementation is publicly available for free to use by anyone with no copyright restrictions.

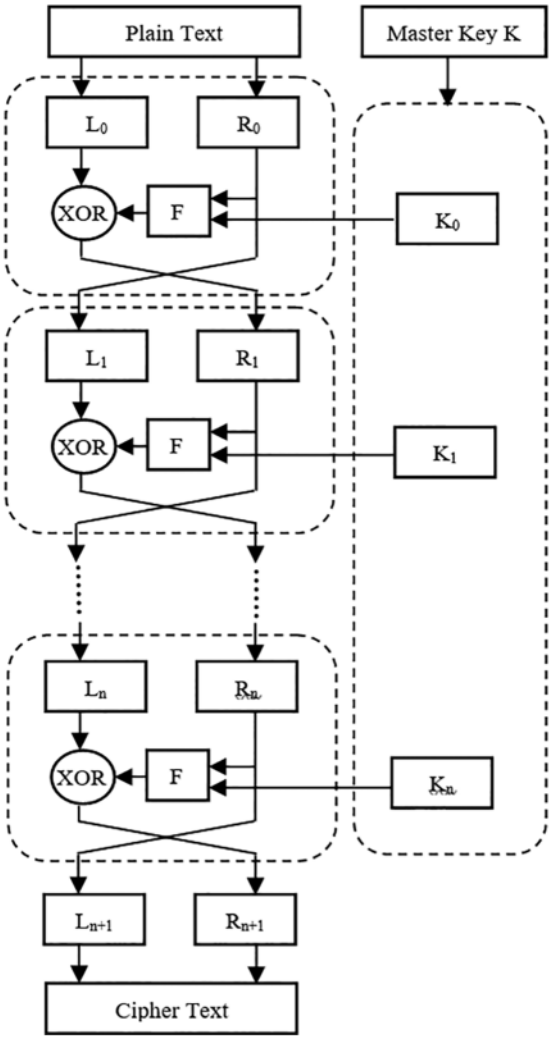

Figure 1: Feistel network

In each round of Twofish, two 32-bit words are used as an input to the F function. Each word is divided into four bytes. Those four bytes are sent to four different key-dependent S-boxes. The four output bytes (the S-boxes have 8-bit input and output) are combined using a Maximum Distance Separable (MDS) matrix to form a 32-bit word. Then the two 32-bit words are combined using a Pseudo-Hadamard Transform (PHT), added to two round subkeys, then XORed with the right half of the divided text. There are also two 1-bit rotations going on, one before and one after the XOR. Twofish also use what is so called the "prewhitening" and "postwhitening" additional subkeys are XORed into the text block both before the first round and after the last round. Fig. 2 illustrates the Twofish algorithm.

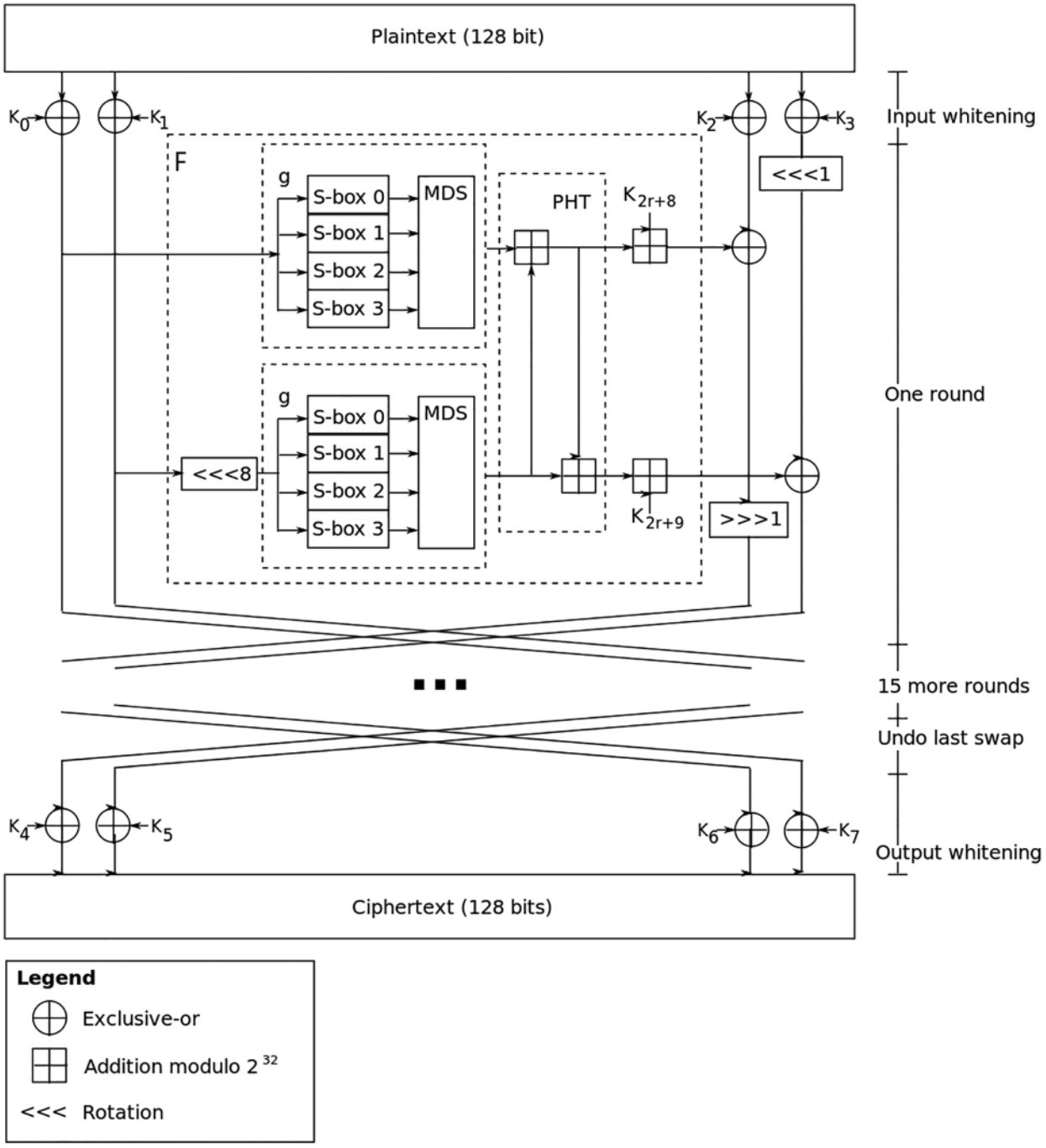

Figure 2: Twofish algorithm

4 The Proposed Algorithm: Split-n-Swap (SnS)

The g function of the Twofish Algorithm receives 32-bits data divided into four 8-bits. In the original Twofish the four 8-bits are fed directly to the S-boxes. In the modifying proposed algorithm,

a Split and Swap operation is made to the four 8-bits prior to the entry of S-boxes, as shown in Fig. 3. That is very helpful to withstand the differential attacks and the man-in-the middle (MitM) attacks. The following pseudo code illustrates how the Split-n-Swap algorithm works.

1. Let's divide the 32-bits input to the g function into four bytes X_1, X_2, X_3, and X_4
2. Split each X into odd and even bits, such that X_i^{odd} is the 4 odd bits of X_i. Similarly, X_i^{even} is the 4 even bits of X_i
3. Constitute new four bytes Y_1, Y_2, Y_3, and Y_4, such that:

$$Y_1 = X_1^{odd} \leftrightarrow X_3^{even}$$

$$Y_2 = X_2^{odd} \leftrightarrow X_4^{even}$$

$$Y_3 = X_3^{odd} \leftrightarrow X_2^{even}$$

$$Y_4 = X_4^{odd} \leftrightarrow X_1^{even}$$

where $\leftrightarrow$ Empty equation removed! is the swap operator which combines one odd bit from the first operand and one even bit from the second operand and so on.

4. Feed the resulting Y_1, Y_2, Y_3, and Y_4 to the S-boxes of the g function.

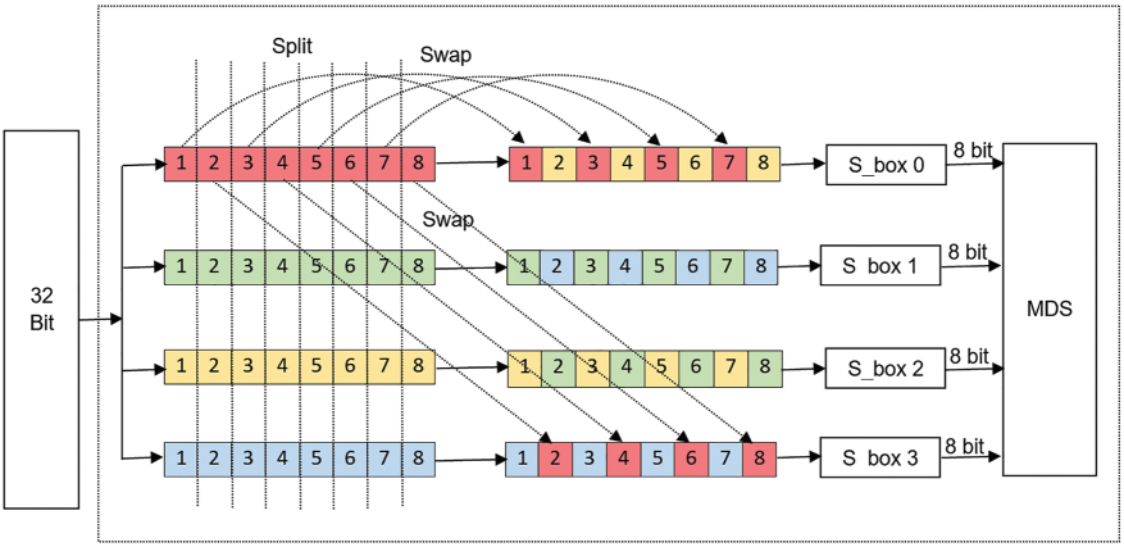

Figure 3: Split-n-Sawp (SnS) model

5 Experimental Results

In this section, computational analysis is given to measure the performance of the Split-n-Swap algorithm compared to the original Twofish algorithm. Four performance metrics have been examined which are: Encryption/Decryption Time and Encryption/Decryption memory utilization.

5.1 Encryption/Decryption Time

Encryption/Decryption Time can be defined as the amount of time needed by the cipher algorithm to encrypt or decrypt the cipher text. Both Tab. 1 and Fig. 4 depicts the encryption time for the original

Twofish algorithm and SnS algorithm. From Fig. 4 and the corresponding tabular representation, it can be seen that although SnS has much higher complexity than the original Twofish algorithm, it gave a slightly higher encryption time. Moreover, from Tab. 1, SnS has proven to gave better results than AES algorithm when dealing with text and image files. Similarly, Tab. 2 and Fig. 5 show the result of decryption time.

Table 1: Encryption time in milliseconds

File type	File size	Encryption time in msec		
		Towfish	SnS	AES
JPG	96 KB	565.63	499.11	552.67
TXT	116 KB	646.12	660.29	756.4
PDF	324 KB	1646.31	2136.45	1668.18
PPT	1.29 MB	6700.8	8875.93	6593.46
MP3	2.04 MB	10641.16	13290.57	10450.02
MP4	2.13 MB	11053.33	13906.69	10797.49

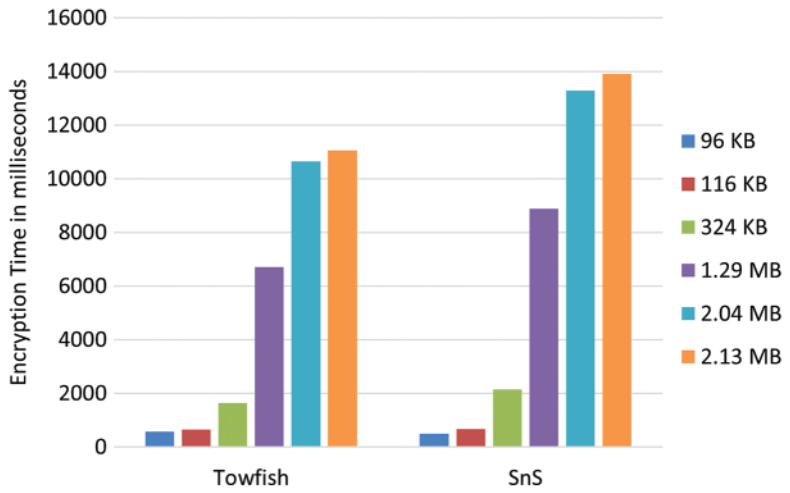

Figure 4: Encryption time

Table 2: Decryption time in milliseconds

File type	File size	Decryption time in msec		
		Towfish	SnS	AES
JPG	96 KB	485.12	594.02	492.23
TXT	116 KB	588.11	798.02	615.84
PDF	324 KB	1617.94	2650.39	1660.3

(Continued)

Table 2: Continued

File type	File size	Decryption time in msec		
		Towfish	SnS	AES
PPT	1.29 MB	6408.95	8471.77	6667.7
MP3	2.04 MB	10330.41	12515.73	10449.53
MP4	2.13 MB	10699.38	13073.78	10966.1

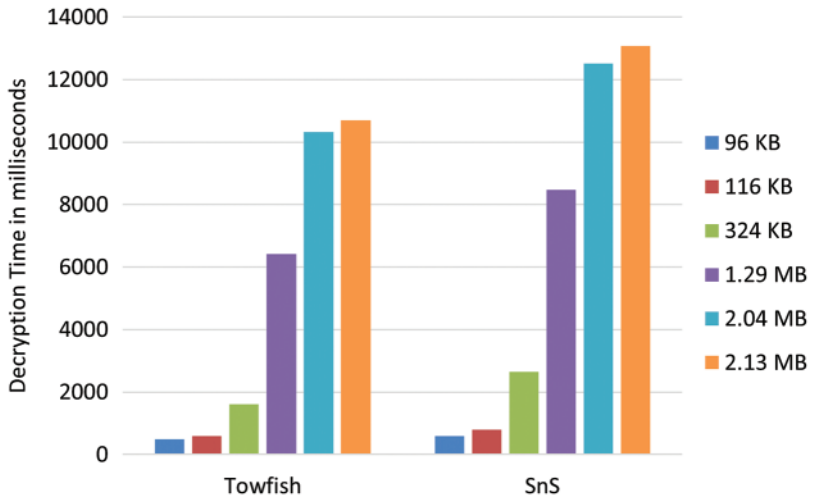

Figure 5: Decryption time

5.2 Encryption/Decryption Memory Utilization

Encryption/Decryption memory utilization is another important metric that should be taken into account when designing a cipher model. Tabs. 3 and 4, give a tabular representation of memory utilization of both Twofish and SnS algorism in encryption and decryption operation respectively. Similarly, Figs. 6 and 7 depicts the memory utilization for both algorithms in encryption and decryption operation respectively.

Table 3: Encryption memory utilization in kilobytes

File type	File size	Memory utilization in KB		
		Towfish	SnS	AES
JPG	96 KB	176.63	151.67	134.34
TXT	116 KB	142.31	255.705	225.68
PDF	324 KB	717.81	861.26	340.29
PPT	1.29 MB	138.92	870.89	1463.37
MP3	2.04 MB	3556.91	2198.02	2251.3
MP4	2.13 MB	3710.92	2406.44	2353.59

Table 4: Decryption memory utilization in kilobytes

File type	File size	Memory utilization in KB		
		Towfish	SnS	AES
JPG	96 KB	325.60	356.81	124.13
TXT	116 KB	436.42	209.15	225.66
PDF	324 KB	562.15	747.96	450.3
PPT	1.29 MB	487.16	613.41	1463.37
MP3	2.04 MB	3719.82	3716.50	2200.21
MP4	2.13 MB	3344.24	3342.31	2328.07

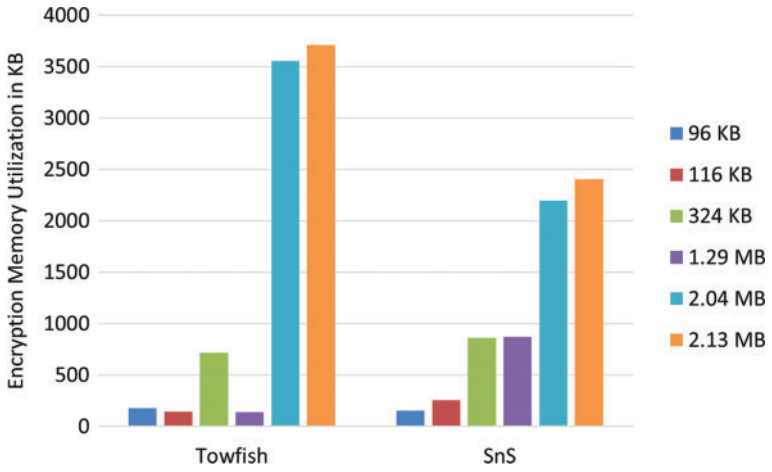

Figure 6: Memory utilization for encryption time

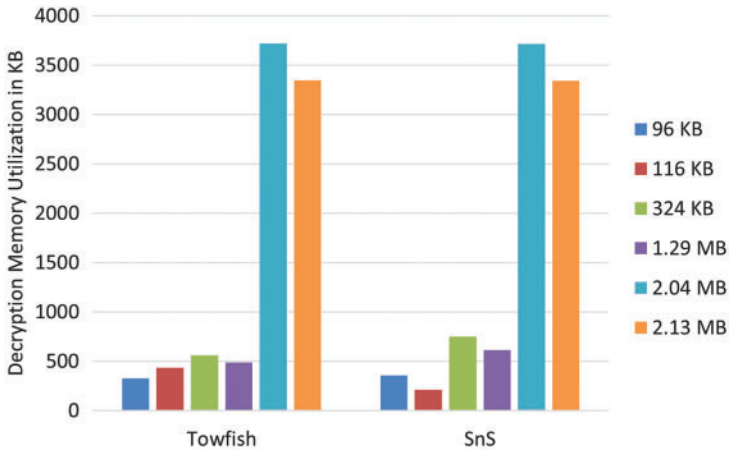

Figure 7: Memory utilization for decryption time

It can be seen from the tables and the figures that the complexity added to SnS didn't affect the memory utilization performance. Moreover, at some instances SnS performs better than both the original Twofish and AES algorithms.

6 Conclusion

Twofish has been always considered a flexible design that can be implemented over a wide range of hardware and software platforms. In this paper, Split-n-Swap, a novel modification of the Twofish algorithm has been proposed to increase its security level by increasing the complexity based on interbit exchange of the g function input. The experimental results show that the proposed model has increased the complexity of the original Twofish algorithm yet keeps a reasonable encryption/decryption times and memory utilization. Even when compared to AES algorithm, the proposed model gives better results over text and image files.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Ramadevi, K. N. Baluprithviraj, V. Ayyem Pillai and K. Subramaniam, "Deep learning based distributed intrusion detection in secure cyber physical systems," *Intelligent Automation & Soft Computing*, vol. 34, no. 3, pp. 2067–2081, 2022.

[2] D. Liao, and X. Wang, "Applications of blockchain technology to logistics management in integrated casinos and entertainment," *Informatics*, vol. 5, no. 4, pp. 44, 2018.

[3] G. Ciaburro and G. Iannace, "Improving smart cities safety using sound events detection based on deep neural network algorithms," *Informatics*, vol. 7, no. 3, pp. 23, 2020.

[4] H. El-Sofany, "A proposed biometric authentication model to improve cloud systems security," *Computer Systems Science and Engineering*, vol. 43, no. 2, pp. 573–589, 2022.

[5] A. A. Radwan, H. V. Madhyastha, F. Omara, T. M. Mahmoud and E. Elgeldawi, "Pinterest attraction between users and spammers," *International Journal of Computer Science Engineering and Information Technology Research*, vol. 4, no. 1, pp. 63–72, 2014.

[6] E. Elgeldawi, A. A. Radwan, F. Omara, T. M. Mahmoud and H. V. Madhyastha, "Detection and characterization of fake accounts on the pinterest social networks," *International Journal of Computer Networking, Wireless and Mobile Communication*, vol. 4, no. 3, pp. 21–28, 2014.

[7] E. Elgeldawi, A. Sayed, A. R. Galal and A. M. Zaki, "Hyperparameter tuning for machine learning algorithms used for arabic sentiment analysis," *Informatics*, vol. 8, no. 4, pp. 79, 2021.

[8] A. A. Sayed, E. Elgeldawi, A. M. Zaki and A. R. Galal, "Sentiment analysis for arabic reviews using machine learning classification algorithms," in *Proc. of 2020 Int. Conf. on Innovative Trends in Communication and Computer Engineering (ITCE)*, Aswan, Egypt, pp. 56–63, 2020.

[9] A. A. Radwan and E. Elgeldawi, "Solving the optimal routing problem in a packet-switching computer network using decomposition," *Egyptian International Journal*, vol. 4, no. 9, pp. 1–13, 2003.

[10] A. A. Radwan, T. M. Mahmoud and E. Elgeldawi, "Improving the efficiency of the flow deviation method for solving the optimal routing problem in a packet-switched computer network," *International Journal of Applied Mathematics*, vol. 5, no. 2, pp. 171–187, 2001.

[11] M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric algorithm survey: A comparative analysis," *International Journal of Computer Applications*, vol. 61, no. 20, pp. 12–19, 2013.

[12] S. Rajesh, V. Paul, V. G. Menon and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, pp. 293–314, 2019.
[13] E. Elgeldawi, M. Mahrous and A. Sayed, "A comparative analysis of symmetric algorithms in cloud computing: A survey," *International Journal of Computer Applications*, vol. 182, no. 48, pp. 7–16, 2019.
[14] A. Dandalis, V. K. Prasanna and J. D. Rolim, "A comparative study of performance of AES final candidates using FPGAs," *Cryptographic Hardware and Embedded Systems Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, vol. 1965, pp. 125–140, 2002.
[15] M. Akram, M. W. Iqbal, S. A. Ali, M. U. Ashraf, K. Alsubhi *et al.,* "Triple key security algorithm against single key attack on multiple rounds," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 6061–6077, 2022.
[16] B. A. Y. Alqaralleh, F. Aldhaban, E. A. AlQarallehs and A. H. Al-Omari, "Optimal machine learning enabled intrusion detection in cyber-physical system environment," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 4691–4707, 2022.
[17] N. Kumar, V. M. Mishra and A. Kumar, "Smart grid security by embedding s-box advanced encryption standard," *Intelligent Automation & Soft Computing*, vol. 34, no. 1, pp. 623–638, 2022.
[18] A. A. Eshmawi, S. A. Alsuhibany, S. Abdel-Khalek and R. F. Mansour, "Competitive swarm optimization with encryption based steganography for digital image security," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 4173–4184, 2022.
[19] R. Marzouk, F. Alrowais, N. Negm, M. A. Alkhonaini, M. A. Hamza *et al.,* "Hybrid deep learning enabled intrusion detection in clustered IoT environment," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3763–3775, 2022.
[20] A. L. Reyes, E. D. Festijo and R. P. Medina, "Blowfish-128: A modified blowfish algorithm that supports 128-bit block size," in *Proc. of 2018 the 8th Int. Workshop on Computer Science and Engineering (WCSE 2018)*, Bangkok, pp. 578–584, 2018.
[21] T. S. Atia, "Development of a new algorithm for key and S-box generation in blowfish algorithm," *Journal of Engineering Science and Technology*, vol. 9, no. 4, pp. 432–442, 2014.
[22] S. S. Susilabai, D. S. Mahendran and S. John Peter, "Interbit exchange and merge (IBEM) pattern of blowfish algorithm, " *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 7, no. 5S2, pp. 129–132, 2019.
[23] V. C. Koradia, "Modification in advanced encryption standard," *Journal of Information, Knowledge and Research in Computer Engineering*, vol. 2, no. 2, pp. 356–358, 2013.
[24] E. M. De Los Reyes, D. A. M. Sison and D. R. P. Medina, "Modified AES cipher round and key schedule," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 7, no. 1, pp. 29–36, 2019.
[25] P. Gehlot, S. Biradar and B. P. Singh, "Implementation of modified twofish algorithm using 128 and 192-bit keys on VHDL," *International Journal of Computer Applications*, vol. 70, no. 13, pp. 36–42, 2013.
[26] H. Harahsheh and M. Qatawneh, "Performance evaluation of twofish algorithm on IMAN1 supercomputer," *International Journal of Computer Applications*, vol. 179, no. 50, pp. 1–7, 2018.
[27] S. M. Kareem and A. S. Rahma, "A novel approach for the development of the twofish algorithm based on multi-level key space," *Journal of Information Security and Applications*, vol. 50, no. 102410, 2020.
[28] V. Miranda and R. Karthikeyan, "An implementation of twofish algorithm in healthcare system to enhance data security," *International Journal of Innovative Science, Engineering & Technology*, vol. 5, no. 4, pp. 2348–7968, 2018.
[29] D. Gulsezim, "Two factor authentication using twofish encryption and visual cryptography algorithms for secure data communication," in *2019 Sixth Int. Conf. on Internet of Things: Systems, Management and Security (IOTSMS)*, Granada, Spain, pp. 405–411, 2019.

[30] S. Majzoub and H. Diab, "Mapping and performance analysis of the twofish algorithm on MorphoSys," in *ACS/IEEE Int. Conf. on Computer Systems and Applications*, Tunis, Tunisia, pp. 9–15, 2003.

[31] W. Sun, X. Chen, X. R. Zhang, G. Z. Dai, P. S. Chang *et al.,* "A multi-feature learning model with enhanced local attention for vehicle re-identification," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 3549–3561, 2021.

[32] W. Sun, G. C. Zhang, X. R. Zhang, X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy," *Multimedia Tools and Applications Multimedia Tools and Applications*, vol. 80, pp. 30803–30816, 2021.