UDC 004
DOI: 10.15587/1729-4061.2023.285261

DEVELOPING A NEW ENCRYPTION ALGORITHM FOR IMAGES TRANSMITTED THROUGH WSN SYSTEMS

Sanaa Ahmed Kadhim
PhD, Associate Professor
Department of Bioinformatic
University of Information Technology and Communications
Al-Mansoor, Baghdad, Iraq, 009647841

Ruwaida Mohammed Yas
Corresponding author
PhD, Lecturer
Department of Computer Science
Informatics Institute for Post-Graduation Studies (IIPS)/Iraqi Commission for Computer & Informatics (ICCI)
Al-Nidal str., Baghdad, Iraq, 0096478
E-mail: roueida.m.yas@iips.icci.edu.iq

Saad Abdual Azize Abdual Rahman
PhD, Associate Professor
Department of Computer Science
AL-Ma'moon University College
Al-Eskan, Baghdad, Iraq, 0096477

Sura Khalil Abd
Doctor of Network and Communication Systems Engineering, Lecturer
Department of Computer Techniques Engineering
Dijlah University College
AlMasafi str., Baghdad, Iraq, 00964

Wireless sensor networks (WSNs) have up until now faced many challenges because of their open, wide-ranging, and resource-limited nature, including security, efficiency, and energy consumption. In the military system, it is essential to provide high-level security to the significant data over wireless network which is proved to be unreliable public communications. To solve the above problem, high level of security with minimum complexity should be applied to be adequate to limited capabilities of transmission system. This paper presents a new algorithm named (SRS) for encrypting transmitted military images to keep them from getting hacked or broken by WSN. The SRS algorithm is designed to be lightweight, fast, and secure, taking into consideration the limited capabilities of the transmission system. It is implemented as a public key cryptosystem specifically designed for image encryption. The algorithm consists of two parts: encryption and decryption. The proposed system suggested some equations and calculations that are applied to the plain and coded images after being transmitted over the WSN. The results of testing the simulation model demonstrate the effectiveness of the system by evaluation using various metrics such as Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). Overall, the paper presents a new encryption algorithm, SRS, specifically designed for securing military images transmitted over wireless sensor networks. The algorithm aims to provide a balance between security, efficiency, and energy consumption, considering the resource-limited nature of WSNs. The simulation results indicate the improvement of the proposed system by 13 %, 10 %, and 55 % in packet delivery ratio (PDR), throughput, and dropping ratio, respectively, and it shows that the suggested SRS method increased execution time by 67 % compared to RSA based algorithm

Keywords: wireless sensor network (WSN); military system SRS algorithm image encryption

Received date 13.04.2023
Accepted date 23.06.2023
Published date 30.08.2023

<b>How to Cite:</b> Kadhim, S. A., Yas, R. M., Abdual Rahman, S. A. A., Abd, S. K. (2023). Developing a new encryption algorithm for images transmitted through WSN systems. Eastern-European Journal of Enterprise Technologies, 4 (9 (124)), 54–60. doi: https://doi.org/10.15587/1729-4061.2023.285261

1. Introduction

In recent years, the continuous evolution of wireless communication has led to evolving of wireless sensor networks in many fields like military, healthcare, environmental, monitoring and other applications. WSNs are composed of several sensor-nodes, which use radio frequencies to communicate with one another. Wireless networks are proved to be unsecure for many reasons like: using old encryption protocols or weak passwords, signal broadcasting through air make it open to sniffing attack, relaying on passwords or keys for accessing data make it vulnerable to attackers, also, since wireless network is not limited by physical boundaries it become more difficult to be secured. WSN can do a variety of tasks, which include sensing, monitoring, detecting, making calculations, and analyzing [1, 2]. These wireless nodes are limited-resource devices with minimal processing-power, a small band-width, short battery-life, and restrictive memory capacities [3]. When these sensors receive WSN data, they send it to the base station (BS), which is the intended recipient. Normally, these sensors are not regularly checked and operate under unreliable circumstances. This makes WSN networks incredibly vulnerable to various threats, raising the possibility of serious security and privacy issues, as well as the simple disclosure of private information to unintended parties [1, 4]. Data sensed by sensors could be text, images, etc. Since images are such easily recognizable and noticeable objects, it is crucial and necessary to be scrambled before transmission [5, 6]. There are two different types of cryptosystems: asymmetrical and symmetrical. In symmetrical encryption and decryption process a single key (same secrete key) is used. While in asymmetrical encryption and decryption procedures, two separate keys are used. The use of public key cryptography is prevalent, for example, RSA cryptosystem, Hellman cryptosystem and El-Gamal cryptosystem [5].

For the previously mentioned and other reasons, it is important to improve strong, fast, and light encryption strategy to secure transmitted data through WSN system [7, 8]. Therefore, studies that are devoted about secured data transmission over WSN are scientific relevance in recent years.

2. Literature review and problem statement

Numerous studies based on symmetric, public key, or hybrid encryption mechanisms have been put forth in the literature to provide cryptographic protection for small devices in constrained environments like WSN. In [9] onetime encryption key was suggested to secure transmitted data through WSN, they suggested a method with a minimum storage space usage to be applicable with WSN limited capabilities but they needed to improve their method to suite WSN refreshment. Another proposal was made in [10] using Bloom scheme and PRNG for managing and creating keys respectively, the method reduces the frequency of transmitted data during key controlling procedure. The method was applied on medical images transmission. They didn't prove the security of images and they used a heavy-weight key. In [11] a method with two parts was proposed, one for creating keys with length to be chosen depending on some criterial using fussy methods, and the second to distribute created keys. The suggested model's drawback is that it takes longer to disseminate the key. A system was designed in [1] to be flexible and fast to encrypt data with minimum complexity and reasonable authenticity. In their work, they focused on WSN's lifetime, and they didn't determine the type of transmitted data. In [12] authors proposed an innovative information-hiding-based method for securing the transmission of sensor data; for WSN-encrypted images they applied the RSA algorithm. Here, the authors proved that their methods achieved short time for encryption but they have not proven the performance of the WSN while transmitted the encrypted images. Paper [13] suggested a novel method for securing the data transmission in WSN which based on Elliptic Curve Cryptography (ECC) and homomorphic encryption. They used ECC for public and private keys exchange Due to its capability to offer high security with a small key size. The ECC key, node identification number, and distance to the cluster head (CH) are all combined to create the 176-bit encryption key that is being proposed. By aggregating the encrypted data without first having to decrypt it, homomorphic encryption helps save energy. Some nodes (cluster-Head nodes) are not in charge of encrypting messages. They proved that their method can be used for text and image encryption, but they did not consider the encryption time. In [14] another public algorithm is used for image encryption in WSN was proposed. This work proposes a new key selection method based on Elliptic Curve and a new encryption method based on the Hill cipher, which use key permutation for enhancing the key size and for suiting the image's matrix size, resulting in secure transmission by the use of robust image encryption across wireless sensor networks. In their work they used two methods, one for key generation and the other for image encryption, thus the encryption process will be long, also they didn't prove the security of the algorithm on the images. In [15] the researcher considers both data and images when developing a crypto processor with hardware implementations. The researchers suggested the binary field GF (2m) for designing and embedding messages on elliptic curve points. The method deals with variable text-length and different image sizes as inputs. Instead of using a static size data input, it makes use of a stream-oriented approach. Their method achieved good results in terms of encryption and decryption times, but they didn't prove their method in terms of WSN's performance. The authors in [16] apply a more effective symmetric image encryption technique using an improved logistic map. The image must first be bit-scrambled in order to prevent interference between nearby pixels. Next, the image must be encrypted using non-linear diffusion operations. This paper uses the public key method for encryption and develops a new hash function for completing the security identity authentication process. The researchers examined the proposed system's security level but not its performance in terms of throughput or packet delivery ratio. In [17], the authors suggested a hybrid security algorithm. It makes use of both symmetric and asymmetric key techniques to offer high-security encryption and decryption processes that are quick. Additionally, it offers integrity, authentication, and confidentiality. For encryption, it uses Blowfish, Rivest Cipher 4 (RC4), and the Advanced Encryption Standard (AES), for integrity, it uses Message Digest 5 (MD5), finally, for authentication, it uses the Elliptic Curve Diffie Hellman. They use six algorithms for securing the transmission through WSN; thus, there will be a big delay during data transmission. A Low Energy Adaptive Clustering Hierarchy (LEACH) with RSA encryption was presented by the researchers in [18] for secure data transmission between the nodes in a wireless sensor network. At first, energy is supplied to each node in the WSN. The setup and steady phases are the first two phases of implementation. When the cluster head is chosen in a WSN, Data is encrypted using the RSA algorithm before being transferred from one source node to the other destination node. The data is once again decrypted at the destination node. When all of the rounds are finished, the number of dead nodes is displayed. Finally, in addition to the encrypted and decrypted messages, the amount of energy used is also shown. Here, the authors used the traditional RSA, which was not secure enough and was slow.

Various approaches for secure data exchange in WSNs have been suggested and deployed in the past. Each system is effective in a wide range of scenarios and applications. Regardless, no model provides high-level data security when interacting through WSNs with short execution times and high throughput, and no model test the effectiveness of the encryption algorithm in terms of SNR, MES and PSNR. For this reason, a new security algorithm for efficient data transmission with high security, fast, and high throughput is proposed.

3. The aim and objectives of the study

The aim of this study is to present a new method for creating keys using proposed mathematical equations and implement the suggested keys in encrypting images transmitted through WSN.

To achieve this aim, the following objectives are accomplished:

– to create strong keys using the proposed equations;

– to use the generated keys in encrypting sensed images to secure the transmitted data in the NW;

– to decrypt encoded received image at the Base-station;

– to provide a high-speed encryption algorithm;

– to provide better evaluation performance of the proposed system.

4. Materials and methods of research

4. 1. Object and hypothesis of the study

The object of the study is system for the encryption and decryption of the images during transmission over WSN. The system was built using MATLAB R2019b compiler, tested using Windows 10 with processor Core(TM) i7-8550U CPU, and 128 GB RAM. The images used to test the system were chosen from internet with different rang of quality to ensure the applicability of the system. The results were calculated for over than 30 images, only four random images were used to clarify the procedure and the results.

The system has many steps starting with generating keys to be used later within the suggested SRS and ending with a decrypted text (image).

4. 2. Proposed SRS steps

The following steps are used to create the SRS algorithm's keys, encryption process and decryption process:

– Key selection (From BS view):

1. Select n as a set of prime numbers, each referred to as p_i, such that: $n=\{p_i$: $i=1, 2, \dots n, p_i$ is a prime number$\}$.

2. Compute n_1 and n_2 using the product operation, as the following: the n_1 value is found from the product of the prime numbers p_i, as shown in (1):

$$n_1=\prod\nolimits_{i=1}^{n} p_i, \qquad (1)$$

where (i=1 to n).

While n_2 value is found from the product of the prime numbers p_i, as shown below:

$$n_2=\prod\nolimits_{i=1}^{n-1} p_i, \qquad (2)$$

where (i=1 to n–1).

3. Choose the value of e which must be greater the 1 and less than n_1 ($1<e<n_1$) and greatest common divisor between e and n_1 must be equal to 1 (gcd (e, n_1)=1).

4. The public key of BS will be:

$P^k=(e, n_1)$.

5. Choose the value of d to be the multiplication of e with d mod(n_2) equivalence to as shown in (3):

$$e\times d\, mod\left(n_2\right)=1. \qquad (3)$$

6. The Private key of BS will be: $S^k=(d, n_2)$.

7. The BS sends its public key to sensors:

– From sensors' view (encryption process):

1. The sensor senses the image (I), where (I) is an array of numbers that contains original plain image.

2. The sensor encrypts the plain image using BS's public key to get the ciphered image:

$$\text{Plain image}\left(I\right)= \text{Cj}\times\text{d mod}\left(n_2\right), \qquad (4)$$

where (j=1 to size (I)).

3. The sensor sends the ciphered image to BS:

– From BS view (decryption process):

1. The BS gets the ciphered image (C) from the sensors.

2. BS Decrypts the received image by using its private key=(d, n_2), where the plain image (I) can be found by multiplying the array (Cj) with the private key d mod (n_2):

$$\text{Plain image}\left(I\right)= Cj\times d\ \text{mod}\left(n_2\right), \qquad (5)$$

where (j=1 to size(C)).

4. 3. Keys generation using the proposed SRS

Suppose n contains six prime numbers to be used as input for the generation of n_1 and n_2. Instead of using the same number to be part of both the private and the public key, two different numbers are used one for encryption and the other for decryption. The two numbers (n_1, n_2) were calculated by the proposed method such that they satisfy the encoding\decoding process. This process will raise the complexity of discovering the keys or even part of them.

4. 4. Image encryption and decryption for WSN framework

In this paper, a new public key cryptosystem is proposed in which encryption procedure completely switches a decipherable image to a picture that is not straightforward to keep the first picture secret between clients, resulting in a secure transmission by effectively encrypting images through Wireless Sensor Networks (WSNs). The suggested algorithm makes use of smaller keys, which take up less memory, increase network throughput, and reduce encryption, decryption, and overall execution times. It is ideal for long-distance or covert communications involving large amounts of information because the order in which the cryptographic algorithms are used is determined by the time required for encoding and decoding. The process of encrypting and decrypting an image is shown in Fig. 1.

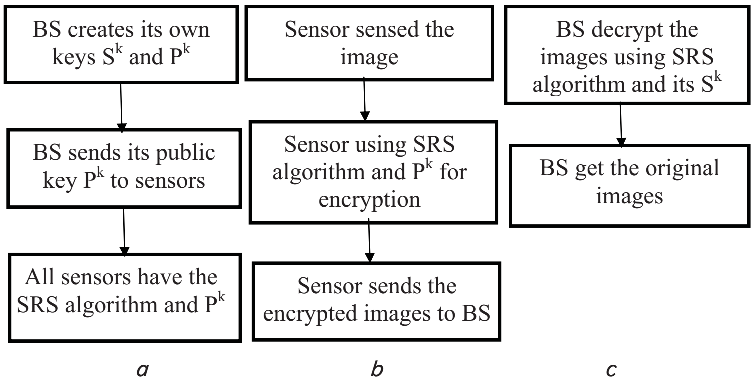

BS creates its own keys S^k and P^k
BS sends its public key P^k to sensors
All sensors have the SRS algorithm and P^k
Sensor sensed the image
Sensor using SRS algorithm and P^k for encryption
Sensor sends the encrypted images to BS
BS decrypt the images using SRS algorithm and its S^k
BS get the original images
a
b
c

Fig. 1. The proposed approach: *a* — key generation and distribution; *b* — image encryption and transmission; *c* — image decryption

In Fig. 1, *a*, the BS creates its keys and distribute the public key to all neighboring sensors. In Fig. 1, *b*, any sensor receives an image will use the SRS algorithm and the public key of the BS to encrypt the image and send it to the BS. Fig. 1, *c*, BS will decrypt the received encoded image using SRS algorithm and its own private key.

5. Results of applying the proposed method

5. 1. Key generation

The process of selecting the keys to be used in encryption and decryption will be clarified by the following example:

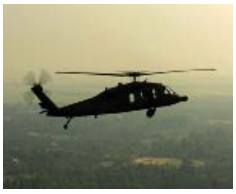
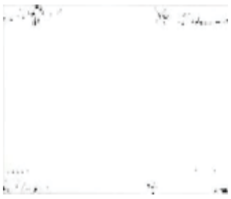
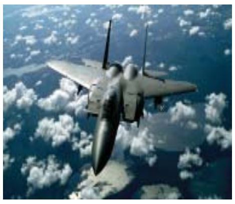
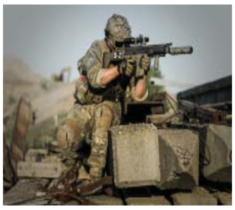
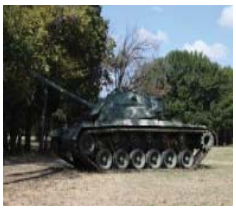
1. Let i=6, and the p s' values are: $p1$=3: $p2$=7: $p3$=11: $p4$=13: $p5$=17: $p6$=19.
2. n={3, 7, 11, 13, 17, 19).
3. n_1=$p1$*$p2$*$p3$*$p4$*$p5$, n_1=51051.
4. n_2=$p1$*$p2$*$p3$*$p4$, n_2=3003.
5. e=23 , gcd(e, n_1)=1.
6. The public key of BS will be: P^k=(23, 51051).
7. d*e mod n_2=1, d=914.
8. The Private key of BS will be: S^k=(914, 3003).
9. The BS sends its public key to sensors.

5. 2. Image encryption

The experimental results of the suggested algorithm, which provides encryption process (using (4)) for the chosen images, are shown in Table 1.

Table 1

The experimental results for encryption of the selected images

Image	Plain image	Encrypted image
Image 1		
Image 2		
Image 3		
Image 4		

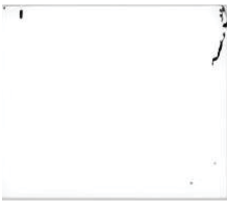
As shown from the above table, the plain images were scrambled in a way that all the features in the images have been distorted as illustrated in the third column (encrypted image). Comparing the original image with the encrypted image, they should have no common features (or having maximum differences between them).

5. 3. Image decryption

Using the created keys decrypt the encoded image (using (5)) to recover the original one. The experimental results of the decryption process using the proposed method is shown in Table 2 below.

Table 2

The experimental test for decryption

Image	Encrypted image	Decrypted image
Image 1		
Image 2		
Image 3		
Image 4		

As shown from the above table, the ciphered images were unscrambled in a way that all the features in the images have been retrieved as illustrated in the third column (decrypted image).

During the evaluation process, the quality of the reconstructed image is measured by calculating the SNR, MSE, and PSNR between the original image and the retrieved image, which are metrics utilized to evaluate the quality of an image following its reconstruction. The MSE represents the average squared difference between the original and retrieved images. The PSNR is a measurement of the peak signal-to-noise ratio, expressed in decibels, between the two images. The SNR used to compute the difference between the original and encrypted images by measuring the level of protection on encrypted images. Table 3 shows the comparative results of PSNR, MSE, and SNR.

Table 3

Comparative analysis

Images	SNR	MES	PSNR
Image 1	–27.23448	7402422.95723	–20.5629
Image 2	–27.23452	10166672.56357	–21.9410
Image 3	–27.23449	7238597.05454	–20.4657
Image 4	–27.23452	7327764.17455	–20.5189

As seen from Table 3, the lower values of the PSNR the original images and encrypted images means a better result, because it shows a less similarity between the original and the encrypted images. The higher values of the MES mean a better result, because it shows dissimilarity between the original and the encrypted images. The more negative the SNR (Signal-to-Noise Ratio) value, the more robust the scheme is.

5. 4. Speed of the proposed algorithm

The proposed system proved to be fast and light which are very adequate to the limited potential WSN. This was proved by comparison with RSA system, where RSA is a public key cryptosystem uses three different algorithms to provide asymmetric encryption. Such that: Key generation algorithm, $Gen(1^k)$: Given a security parameter k, outputs a pair of keys, namely public key p^k and secret key s^k respectively. Encryption algorithm, Enc (p^k, m): Given the input p^k and message m, outputs the ciphertext c. Decryption algorithm, Dec (s^k, c): Given the input s^k and ciphertext c, outputs the message m. the compression between the two systems (the proposed SRS system and the RSA) [18] as shown in Table 4.

Table 4

Execution time

Image	RSA	SRS
Image 1	13.081314 seconds.	5.720398 seconds
Image 2	75.198161 seconds.	6.614578 seconds.
Image 3	81.020421 seconds	7.311440 seconds.
Image 4	89.115245 seconds	8.244410 seconds.

Table 4 shows the differences of the execution time between the public key (RSA) algorithm and the proposed algorithm. As seen that the proposed algorithm takes less execution time than RSA algorithm.

5. 5. Performance analysis

For performance evaluation of the proposed system, three parameters are considered which are: packet delivery ratio, throughput, dropping ratio.

From Fig. 2 below it illustrates the improvement of the packet delivery ratio of our proposed algorithm compared with the RSA based method in [18], this is due to the use of the new mathematical equations used in the proposed method. Packet Delivery Ratio (PDR) represents the number of packets received successfully to the total number of packets sent by source node.

Fig. 3 below shows the evaluation of the throughput which counts the amount of transmitted data in a given amount of time. Comparing our suggested approach to the RSA-based method in [18], the amount of data delivered per unit of time is noticeably higher.

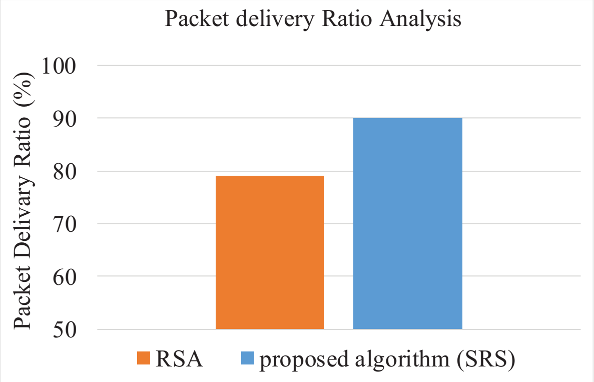


Fig. 2. Packet delivery ratio analysis

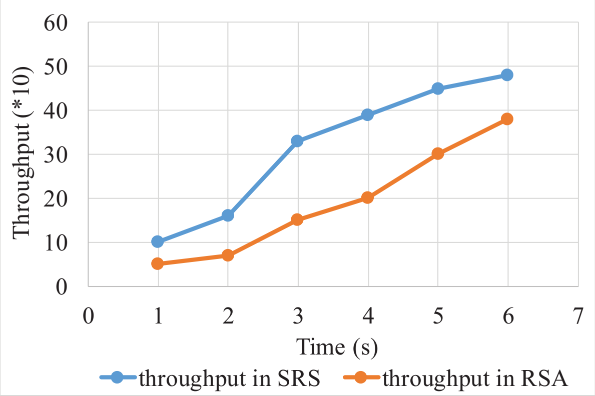


Fig. 3. Throughput performance analysis

In Fig. 4 it is possible to notice the enhancement of dropping ratio of our proposed algorithm compared with the RSA based method. Dropping ration can be defined as the amount of dropped data packets divided by the total number of transmitted data packets.

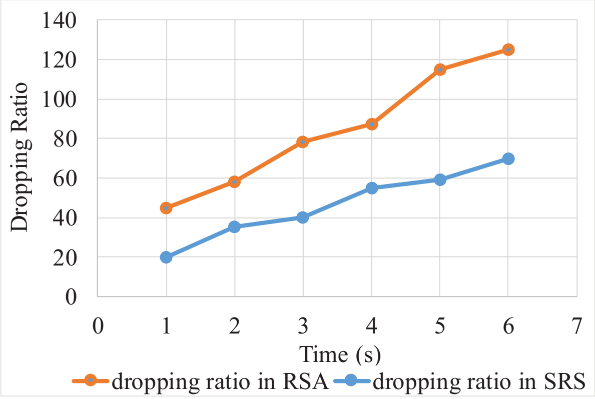


Fig. 4. Dropping ratio performance analysis

Because of the great security offered in our proposed method, the amount of the dropping data packets in our suggested SRS is significantly lower than in the RSA based method. So the suggested method guarantees data integrity while it is being transmitted.

6. Discussion of results of encrypting and decrypting military images using the proposed system

The results of applying the proposed SRS system showed that, the system is secure, light, and fast which was proven by testing and evaluating the system using different metrics. Metrics like, SNR, MSE, and PSNR were utilized to evaluate the quality of an image following its reconstruction. The secrecy of encryption was proved according to these metrics which indicate no similarity between the original and the encrypted images (Tables 1–3). While the comparison the original image with the decrypted image, indicate that they were identical (or at least had minimal differences). The testing also showed that the system was faster during implementation (Table 4), throughput, packet delivery ratio were higher (Fig. 2, 3), and dropping ratio was less (Fig. 4) when comparing with the RSA-based method in [18].

It can be noted that the results achieved by the proposed system was comparably good, which indicate the secrecy and the confidentiality in the transmission of military images over a wireless sensor network (WSN).

The proposed system works perfectly with high and middle quality images; it may have a bad reconstructed image.

As a future work, our suggested system can be modified to be applicable with different Internet of Things (IoT) applications. IoT security issues are becoming more prevalent due to their rising popularity, much like wireless networks. To solve this problem, let's intend to expand our suggested system so those real-world IoT environments can be used to implement and evaluate it.

7. Conclusions

1. Creates keys depending on selecting n prime numbers as shared secrete set used to create two numbers that maximize secrecy and confidentiality of the transmitting of the military images over WSN. The creation is fast with minimum complexity and maximum security.

2. The exchange of the keys was made through the open wireless system securely since each part will find out its key locally.

3. A new asymmetric encryption algorithm was proposed for encrypting different types of images with different sizes.

4. By testing the system using the performance metrics, it has been proven that the suggested method performs better and is more secure when used with WSN military applications. The improvements of the proposed SRS in PDR, throughput, and dropping ratio were 13 %, 10 %, and 55 % over the RSA-based algorithm, respectively.

5. Comparing the suggested SRS system with the well-known RSA system, it gave better execution time The SRS algorithm was faster than RSA by about 67 %.

Conflicts of Interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study and the results reported in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has no associated data.

References

1. Khashan, O. A., Ahmad, R., Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Networks, 115, 102448. doi: https://doi.org/10.1016/j.adhoc.2021.102448
2. Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., Liu, J. (2019). A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network. IEEE Access, 7, 53079–53090. doi: https://doi.org/10.1109/access.2019.2911395
3. Khashan, O. A. (2020). Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment. IEEE Access, 8, 66878–66887. doi: https://doi.org/10.1109/access.2020.2984317
4. Yas, R. M., Hashim, S. (2021). Intelligent Approaches for Enhancing Networked Routing Protocol. Iraqi Journal of Science, 4121–4147. doi: https://doi.org/10.24996/ijs.2021.62.11.32
5. Mathur, S., Gupta, D., Goar, V., Kuri, M. (2017). Analysis and design of enhanced RSA algorithm to improve the security. 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT). doi: https://doi.org/10.1109/ciact.2017.7977330
6. Rafash, A. G. H., Saeed, E. M. H., Talib, A.-S. M. (2021). Development of an enhanced scatter search algorithm using discrete chaotic Arnold's cat map. Eastern-European Journal of Enterprise Technologies, 6 (4 (114)), 15–20. doi: https://doi.org/10.15587/1729-4061.2021.234915
7. Khashan, O. A., Zin, A. M., Sundararajan, E. A. (2014). Performance study of selective encryption in comparison to full encryption for still visual images. Journal of Zhejiang University SCIENCE C, 15 (6), 435–444. doi: https://doi.org/10.1631/jzus.c1300262
8. Kadhim, S. A., abdual Rahman, S. A. A. (2021). A proposed method for encrypting and sending confidential data using polynomials. Global Journal of Engineering and Technology Advances, 8 (2), 082–087. doi: https://doi.org/10.30574/gjeta.2021.8.2.0133
9. Szalachowski, P., Kotulski, Z. (2012). One-Time Broadcast Encryption Schemes in Distributed Sensor Networks. International Journal of Distributed Sensor Networks, 8 (3), 536718. doi: https://doi.org/10.1155/2012/536718
10. Muhajjar, R. A., Flayh, N. A., Al-Zubaidie, M. (2023). A Perfect Security Key Management Method for Hierarchical Wireless Sensor Networks in Medical Environments. Electronics, 12 (4), 1011. doi: https://doi.org/10.3390/electronics12041011

11. Wazery, Y. M., Ali, M. A. S. (2018). An Intuitionistic Fuzzy Sets Implementation for Key Distribution in Hybrid Message Encryption Over Wsns. International Journal of Advances in Applied Sciences, 7 (3), 273. doi: https://doi.org/10.11591/ijaas.v7.i3.pp273-285
12. Zhao, G., Yang, X., Zhou, B., Wei, W. (2010). RSA-based digital image encryption algorithm in wireless sensor networks. 2010 2nd International Conference on Signal Processing Systems. doi: https://doi.org/10.1109/icsps.2010.5555601
13. Elhoseny, M., Elminir, H., Riad, A., Yuan, X. (2016). A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. Journal of King Saud University - Computer and Information Sciences, 28 (3), 262–275. doi: https://doi.org/10.1016/j.jksuci.2015.11.001
14. Ramasamy, J., Kumaresan, J. S. (2020). Image Encryption and Cluster Based Framework for Secured Image Transmission in Wireless Sensor Networks. Wireless Personal Communications, 112 (3), 1355–1368. doi: https://doi.org/10.1007/s11277-020-07106-7
15. Leelavathi, G., Shaila, K., Venugopal, K. R. (2020). Message and Image Encryption Embedding Data to GF(2m) Elliptic Curve Point for Nodes in Wireless Sensor Networks. EAI/Springer Innovations in Communication and Computing, 329–338. doi: https://doi.org/10.1007/978-3-030-19562-5_33
16. Li, H., Ge, B., Xia, C., Wang, T. (2021). Image Encryption for Wireless Sensor Networks with Modified Logistic Map and New Hash Algorithm. Wireless Algorithms, Systems, and Applications, 29–37. doi: https://doi.org/10.1007/978-3-030-86137-7_4
17. Abdulhameed, H. A., Abdalmaaen, H. F., Mohammed, A. T., Mosleh, M. F., Abdulhameed, A. A. (2022). A Lightweight Hybrid Cryptographic Algorithm for WSNs Tested by the Diehard Tests and the Raspberry Pi. 2022 International Conference on Computer Science and Software Engineering (CSASE). doi: https://doi.org/10.1109/csase51777.2022.9759589
18. Aruna Deepthi, S., Aruna, V., Leelavathi, R. (2022). Image Transmission Using Leach and Security Using RSA in Wireless Sensor Networks. Advances in Intelligent Systems and Computing, 39–51. doi: https://doi.org/10.1007/978-981-16-9573-5_3