Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 293–304
DOI : 10.47974/JDMSC-1883

Cryptographic image-based data security strategies in wireless sensor networks

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

D. Palanikkumar †
Department of Computer Science and Engineering
Dr NGP Institute of Technology
Coimbatore
Tamil Nadu
India

Sajja Suneel §
Department of CSE (Data Science)
Institute of Aeronautical Engineering, Dundigal
Hyderabad
Telangana
India

Satish Dekka ‡
Department of Computer Science and Engineering
Lendi Institute of Engineering and Technology
Vizianagaram
Andhra Pradesh
India

* *E-mail:* **dankan.v@bmsit.in (Corresponding Author)**
† *E-mail:* **palanikkumard@gmail.com**
§ *E-mail:* **sajja.suneel@gmail.com**
‡ *E-mail:* **satishmsc4u@gmail.com**

T. Thiruvenkadam [@]
School of Computer Science & Information Technology
JAIN (Deemed-to-be University)
Bengaluru
Karnataka
India

K. D. V. Prasad [#]
Department of Research
Symbiosis Institute of Business Management
Hyderabad
India

and

Department of Research
Symbiosis International (Deemed University)
Pune
Maharashtra
India

Abstract

There is need to develop and create new data protection mechanisms aimed at the compensating for the lack of security of WSNs. This paper introduces new cryptographic image-based techniques aimed at improving data security in WSNs. The solution also integrates imaging processing techniques with advanced cryptographic principles to merge a two-layered security architecture. This work provides a new WSN-specific encryption algorithm that delivers low energy consumption and smaller computational burden. Likewise, this is connected to an image-based authentication approach which employs steganographic methods in the information hiding technique. Intensive simulations allow the approach that supports methodology, naming increased security metrics obtained without decreasing in network performance. This study seeks to fill the gap in current practice in WSN security and provides a foundation for future research on image-based techniques integrated with cryptographic algorithms aiming at more secure data protection under limited resources.

Subject Classification: *(2010) 94A60, 20C05, 20C07.*

Keywords: *Wireless sensor networks (WSN), Cryptographic security, Image-based encryption, Data protection in WSN, Steganography, Network security, Encryption algorithm.*

[@] *E-mail:* **mailone.thiru@gmail.com**
[#] *E-mail:* **kdv.prasad@sibmhyd.edu.in**

1. Introduction

The emergence of WSNs has significantly transformed the realm of data gathering and communication in all sectors, such as environmental monitoring, smart grid management. But the growing dependence on these networks has also made data security more urgent at the same time[1]. WSNs, characterized by their limited computational power, energy constraints, and susceptibility to physical and cyber threats, present a unique set of challenges for data security [2,3]. Traditional cryptographic methods often prove inadequate, primarily due to the resource-intensive nature of conventional encryption algorithms and the complex requirements of network security.

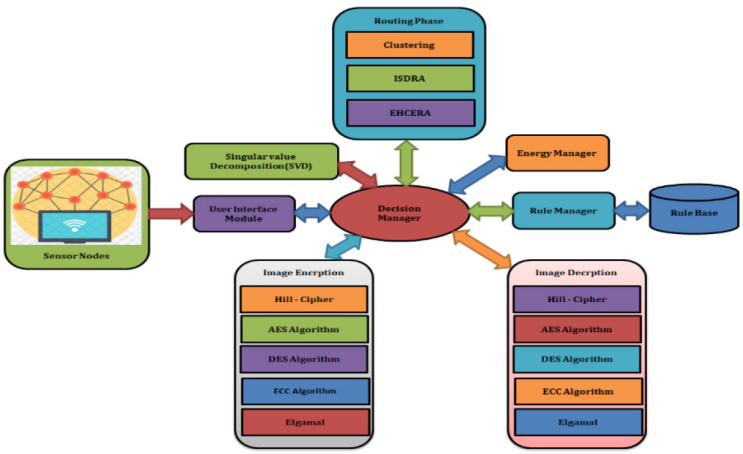

Figure 1

Design of a Secure System for Data Communication

A novel approach for secure data transmission in wireless sensor networks is proposed, centered around cryptographic methods. The architecture of this security model is detailed in Figure 1. It is built on a foundation of ten critical components[4,5]: the User Interface Module, Decision Manager, Rule Manager, Rule Base, processes for both Image Encryption and Decryption, Singular Value Decomposition, Routing, and the Energy Manager. Each component plays a vital role in the model's functionality and will be briefly explained. In the context of wireless sensor networks, sensor nodes are a standard feature[6]. In the case of experiment, a specific situation is adopted such that these nodes have minimum required energy for data communication. These nodes can

securely communicate among themselves if the previously proposed model for strictly protected data communication [7,8] is used. In this study, the Rule Manager interacts with the rule base in support of Decision Manager. It is mainly used for pulling a number of rules from the rule base on command by the Decision Manager. Besides, the Rule Manager has a significant responsibility in regard to adding new rules to the rule base that must guarantee constant maintenance of system operation updates and improvement using the latest criteria and scenarios[9,10]. Given these challenges, this study intends to design a new image-based crypto data security technique for WSNs. The goal here is to establish a security system that not only removes the WSN weaknesses but also enhances data protection against modern cyber threats. The approach that is being proposed is unique in the fact that it incorporates cryptographic processes with image-related security measures, such a combination of concepts has been hardly investigated when talking about WSNs.

2. Literature Review

This field has been researched by many scholars over the years. Based on their findings, reversible data hiding techniques are categorized into two basic types. The first one is the difference expansion technique and two, the idea of histogram shifting. Sample data schemes from both approaches have been designed and verified. Data security in wireless sensor networks (WSNs) literature is abundant which indicates the vital role of these network to various applications[11,12]. The early research was largely confined to the traditional approaches of cryptography. For example, the author's work in [13] focused on a symmetric key approach for WSNs by highlighting its easiness and lesser computational demands as opposed to asymmetric methods. But they were aware of this complexity in terms of key distribution and management that the situation demands in WSN, which is a dynamic environment. Analogously, as reported in [14] notable authors focused on public-key infrastructures for WSNs indicated that such solutions bring better security yet with the price of computational load growth which is unacceptable for limited sensor nodes. Some of the more recent studies have tried to focus on other forms. In [15], author's addressed the use of light embedded cryptographic algorithms and its potential in reducing high energy costs while minimizing time execution on processors. Yet, these algorithms often compromise on the level of security, making them unsuitable for high-risk applications. On the other hand, author's in [16] explored the integration

of steganographic techniques with traditional encryption, showing promising results in terms of covert communication but leaving the aspect of robust encryption relatively unaddressed. In this case, the sender uses the cover-image to produce an encrypted picture, which the data hider then inserts with the intended message. As soon as the recipient receives the encrypted picture, they may decode it and get back the original, unmodified cover image as well as the plaintext containing the hidden message[17,18]. In order to bridge this gap, the present study proposes an original cryptographic image based WSNs security framework which is likely to deliver a balanced trade off between security efficiency and energy performance that suits the different operational environments associated with WSNs.

3. Proposed System

The proposed research describes a novel image encryption system, which exploits the ElGamal method of the curve and is based on an ElGamal blocking pattern. This solution aims to ensure that all communications are carried out using securely encrypted methods provided by executing the encryption in a public key. The model's unique structure not only supports image encryption and data concealing but also significantly increases security. This new approach is an important progress towards the secure technique as it does not only hide intemperate data but also encrypts photos, creating strong framework.

The main strength of the suggested model comes from its utilization of an undeletable data hiding approach. This strategy remarkably simplifies computationally and ensures a high level of security, which makes secure communication easier. As shown in Figure 2, the model uses

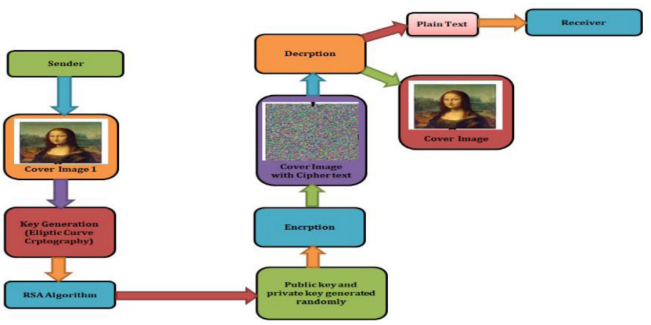

Figure 2

Design of Encrypted Image Concealment Systems

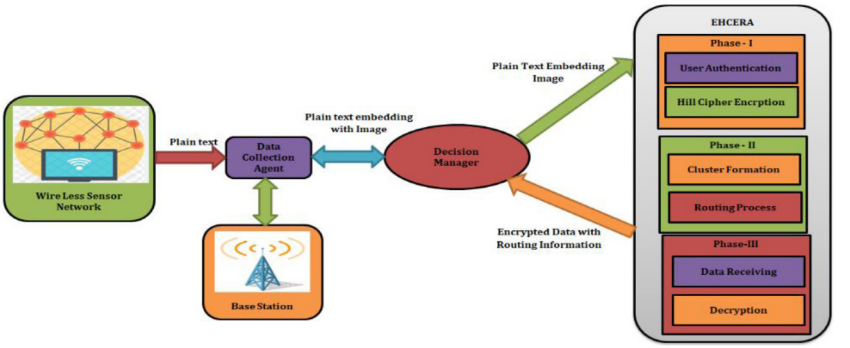

Figure 3

Design of Data Transmission with a Cluster-Based System

the RSA algorithm to obtain public and private keys. These keys are then used in the encryption that is carried using the Elgamal algorithm. This proposed architecture not only represents the performance of the frame but also manifests the aptitude for recovering images without loss, which ensures the high suction and accuracy of this system. Figure.3. depicts the framework of cluster-based data transmission, used in this study. First, the process involves a data collection agent collecting information from nodes forming part of the network environment and communicating this to a decision manager. This information goes through different procedures in the proposed EHCERA structure, along with encryption, decryption, clustering and routing.

The model is structured into three distinct phases:

Phase 1: Applies the Hill-cipher encryption algorithm.

Phase 2: It conducts clustering and routing operations.

Phase 3: Contains data reception and decryption algorithm application.

Original image is encrypted first in this system. After different processing steps, the image is decrypted and returned to the user; it is reconstructed[19,20]. This comprehensive ISA framework guarantees error-free, fast and safe data transmission which preserves the quality of an original image throughout this whole process. The architecture of the proposed system highlights twin-layer security on the data, retaining its safety and invulnerable nature.

Algorithm:

A ECB homomorphic encoding scheme based on ElBamal cryptography used to implement encryption processes is used in this research paper. The scheme unfolds in the following steps:

Step 1: Initial Setup

Input: Plaintext message P

Output Goal: Encrypted messages C1 and C2.

Step 2: Preparation Phase

Select a 256-bit prime number p.

Read the plaintext P and the cover image I.

Step 3: Elliptic Curve Configuration

Apply the elliptic curve equation $y^2 = x^3 + ax + b$

Compute $(x^3 + ax + b) \bmod p$.

Identify two specific points *a* and *b* on the curve.

Step 4: Group Formation and Key Selection

From the group $G = \langle Z_p^*, X \rangle$.

Select a member *d* from *G*, ensuring $1 \le d \le p - 2$.

Step 5: Public and Private Key Generation

Choose e_1 as a primitive root in G.

Calculate $e_2 = e_1^d \bmod p$.

Assign (e_1, e_2, p) as the public key and *d* as the private key.

Step 6: Key Transmission

Securely send the private key *d* to the intended receiver.

Step 7: Encryption Process

At the sender's end, select a random integer *r* from *G*.

Perform EIGamal encryption to obtain $C_1 = e_1^r \bmod p$ and $C_2 = (e2^r XP) \bmod p$.

Apply similar steps for both the embedded message and the cover image.

Step 8: Transmission to Receiver

Send the encrypted components C_1, C_2, C_3 and C_4 to the receiver.

Step 9: Decryption and Recovery

The receiver processes C_1, C_2, C_3 and C_4.

Decrypttoretrieve $P = [C_2 \; X \; (C_1^{\;d})^{-1}] \bmod p$ and $I = [C_4 \; X \; (C_3^{\;d})^{-1}] \bmod p$.

Extract and separate the original image *I* and message P.

4. Results and Discussion

In wireless sensor networks (WSNs), the suggested cryptographic image-based security approach improves security and efficiency significantly, according to simulation findings. A number of tests were conducted to determine the efficacy of the data concealing strategy as part of the performance assessment phase of the proposed model's implementation. Image quality and payload capacity were the two primary considerations that shaped these trials.

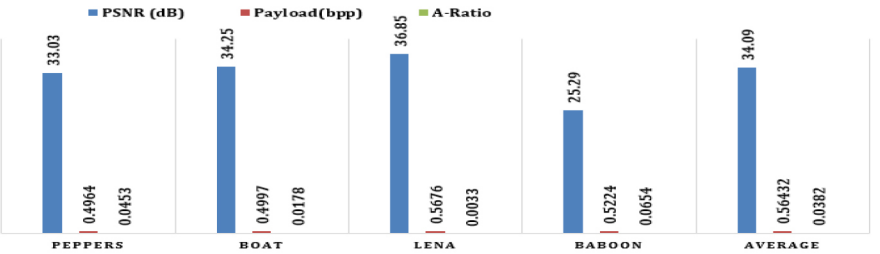

Figure 4

Analysis of PSNR, Payload, and A-Ratio

For the experimental phase, four distinct images were selected: Peppers, Boat, Lena, and Baboon. These images served as the basis for testing and analyzing the proposed model's capabilities. Figure 4. presents

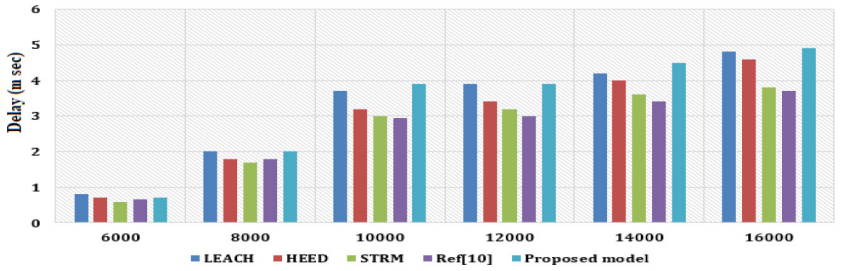

Figure 5

Delay Assessment Relative to Packet Quantity

detailed findings, showcasing the payload values (measured in bpp), the quality of the images post-encryption, and their overall availability for effective data hiding.

As seen in Figure 5, the suggested routing model has somewhat longer latency than the other three algorithms: LEACH, HEED, and STRM. Using picture data and key-image for encryption is the cause for the somewhat high latency. The current secure routing and energy-efficient routing algorithms are tested with the same collection of images in a number of different ways. Figure 6 demonstrates that the proposed model exhibits lower energy efficiency compared to existing secured routing protocols like LEACH, HEED, and STRM algorithms. Additionally, the model ensures secure data storage and transmission between source and destination nodes by implementing encryption and decryption processes. Here, the focus is on the effectiveness of the proposed model in maintaining security and reliability, even if it comes at the cost of slightly lower energy efficiency when compared to other routing protocols.

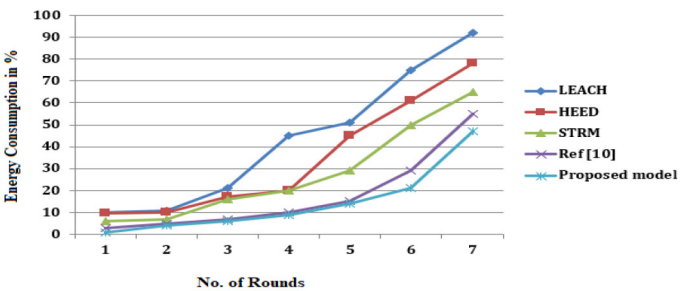

Figure 6

Analysis of Energy Consumption

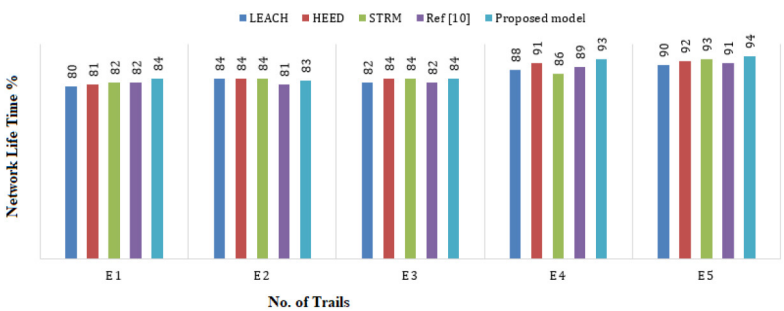

Figure 7

Analysis of Network Lifetime

These findings suggest that the integration of lightweight cryptographic techniques with image-based steganography can significantly enhance the security of WSNs without imposing additional resource burdens. This approach addresses a critical gap in WSN security, aligning with the observations by [12] on the need for resource-efficient security solutions. However, it is important to acknowledge certain limitations of this study. The scalability of the proposed strategy in extremely large and diverse network topologies remains to be thoroughly evaluated. Additionally, the potential biases in the simulation settings, such as network configurations and threat models, may influence the generalizability of the results. The suggested model is compared to three current algorithms—LEACH, HEED, and STRM in Figure 7, which shows a network lifespan analysis. We ran five separate trials to measure the network's efficiency; they are labeled E1, E2, E3, E4, and E5. The significance of this research is also vast, making a practical and cost-effective answer to ensuring the security of employing WSN applications. It is a difficult balance to strike since most previous studies have not had the optimal dual-layer security. However, this approach works because it provides multi-layered protection and assists in meeting the WSN's operational requirements, which reduces threats originating from cyber.

5. Conclusion

In conclusion, the current study is able to provide an innovative cryptographic image-based security architecture for WSNs that combines the virtues of high level of protection and resource-related efficiencies. The findings to highlight show that the proposed lightweight encryption algorithm addresses a major concern of dramatic computation and energy overheads commonly associated with WSN security, complemented by steganography for secure data delivery. This bidirectional method does not only resolve the peculiarity of WSNs but also provides a new security standard in network area. This research has diverse practical aspects. Especially in fields such as environmental monitoring, healthcare, and smart cities because of increasing applications of the WSNs can become a basic strategy to ensure data security from cyber threats. The ability to adapt the cryptographic and steganographic techniques to fit individual application criteria may be another interesting research direction, promising the development of tailored security solutions for different types of WSN applications.

References

[1] Shabana Urooj, Shabana Mehfuz, S Kalathil, Cryptographic Data Security for Reliable Wireless Sensor Network, *Alexandria Engineering Journal*, Volume 72, Pages 37-50 (2023).

[2] P. Ramadevi, S. Vijayakumar, R. Sudha, Security for wireless sensor networks using cryptography, *Measurement: Sensors,*Volume 29, 100874 (2023).

[3] Sadashiva V. Chakrasali, A. Azhagu Jaisudhan Pazhani, Computer vision based healthcare system for identification of diabetes & its types using AI, *Measurement: Sensors,* Volume 27, 10075 (2023).

[4] Naidu, P. Ramesh, Gupta, Anand Kumar. Development of object identification model with deep reinforcement learning algorithm, Journal of Information aHarnessing intelligent systems for water managementnd Optimization Sciences, 44:3, 355–367 (2023).

[5] Sharma, Parismita, Anand Kumar. A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm, *Journal of Interdisciplinary Mathematics*, 26:3, 519-530 (2023).

[6] Prasad, K.D.V., Chinamuttevi, Veera Sivakumar. A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 861-873 (2023).

[7] Kumar, Pullela SVVSR, Chaturvedi, Abhay. Securing networked image transmission using public-key cryptography and identity authentication, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 779-791 (2023).

[8] M. Nagabushanam, K. Raghavendra. Vector space modelling-based intelligent binary image encryption for secure communication, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1157-117 (2022).

[9] Ghazaala Yasmin, Jaisudhan Pazhani, A novel method of data compression using ROI for biomedical 2D images, *Measurement: Sensors*, Volume 24, 100439 (2022), ISSN 2665-9174.

[10] Ravi Shankar, Naziya Hussain, Industrial quality healthcare services using Internet of Things and fog computing approach, *Measurement: Sensors,* Volume 24, 100517 (2022), ISSN 2665-9174.

[11] Pullela SVVSR Kumar, B. Ashreetha, Performance Analysis of Energy Efficiency and Security Solutions of Internet of Things Protocols. IJEER 11(2), 442-450 (2023).

[12] N. Hussain, A. K. . N, "A Novel Method of Enhancing Security Solutions and Energy Efficiency of IoT Protocols ", *IJRITCC*, vol. 11, no. 4s, pp. 325–335 (May 2023).

[13] N. S. Reddy and B. Ashreetha, "Technologies for Comprehensive Information Security in the IoT," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, pp. 1-5 (2023).

[14] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[15] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.

[16] S P Ravi and L Dhanalakshmi, "DWT and Modified AES based Secure Image Steganography on ARM A8 Processor", *International Journal of Engineering Research & Technology* (IJERT) (2015).

[17] N.B. Anuar, S. Misra, "Artificial immune system for detecting intrusion instego-crptonetworks", *Journal of Computer and Net work Applications*, vol. 42, no. 4, pp. 102-117 (2019).

[18] P. Karthika and P. Vidhya Saraswathi, "Image Security Performance Analysis for SVM and ANN Classification Techniques" in In: *International Journal of Recent Technology and Engineering* (IJRTE), vol. 8, no. 4, pp. 436-442 (2019).

[19] E. Y. Baagyere and M. I. Daabo, "A New Image Encryption and Decryption Technique using Genetic Algorithm and Residual Numbers", *2019 IEEE AFRICON*, pp. 1-9 (2019).

[20] Chen and C. Chieh Lee, "Improvement of an Encryption Scheme for Binary Images", *Pakistan Journal of Information and Technology*, vol. 2, no. 2, pp. 191-200 (2018).