Journal of Network Communications and Emerging Technologies (JNCET)
Volume 13, Issue 1, January (2025)

Ruzicka Indexed Schmidt-Samoa Certificateless Signcryptive Connectionist Artificial Deep Neural Learning for Secure Transmission Using Satellite Images

S. Padmalal
Department of Computer Science and Engineering, Mangalam College of Engineering, Kottayam, KERALA, India.
splaal71@gmail.com

I. Edwin Dayanand
Moderator Gnanadason Polytechnic College, NAGERCOIL, Tamil Nadu, India.
edwindaya3@gmail.com

F.R.Shiny Malar
Department of Computer Science and Engineering, Stella Mary's College of Engineering, Nagercoil, Tamil Nadu, India.
headcse@stellamaryscoe.edu.in

ABSTRACT

Content protection for digital images has become a critical concern due to their widespread use on the Internet. As digital images become increasingly integral to daily communication, ensuring their confidentiality and security during transmission is paramount. To address these challenges, this paper introduces a novel technique called Ruzicka Indexed Schmidt-Samoa Certificateless Signcryptive Connectionist Artificial Deep Neural Learning (RISCSCADL) for enhanced secure image transmission. The RISCSCADL method employs a multi-layer architecture comprising input, hidden, and output layers for processing satellite images. The method integrates Schmidt-Samoa certificateless signcryption within the initial hidden layer to enhance security through three distinct processes: Ephemeral Agreement session key generation, Schmidt-Samoa certificateless signcryption, and Ruzicka indexive Schmidt-Samoa certificateless unsigncryption. The framework generates session-specific private and public keys in the first hidden layer, performs signature generation and encryption in the second layer, and conducts signature verification through Ruzicka Indexed Schmidt-Samoa certificateless unsigncryption in the third layer. Experimental results demonstrate that the RISCSCADL method achieves superior image transmission security with enhanced confidentiality, integrity, and reduced computational complexity compared to existing approaches.

Index Terms – Secure Image Transmission, Connectionist Artificial Deep Neural Learning, Schmidt-Samoa Certificateless Signcryption, Ruzicka Indexed Certificateless Unsigncryption, Satellite Image Security.

1. INTRODUCTION

The proliferation of digital communications has brought data confidentiality to the forefront of organizational challenges, particularly regarding the protection, storage, and transmission of sensitive information. Contemporary digital content spans multiple formats, encompassing textual data, imagery, audio recordings, and video content. Within this spectrum, image data has emerged as a critical component in social applications, necessitating robust protection mechanisms during both utilization and transmission. Security measures typically employ cryptographic methodologies, transforming intelligible images into encrypted formats to enhance transmission security.

Recent advances in image encryption have produced various innovative approaches. Researchers have explored DNA-based cryptography, with notable work introducing key scrambling techniques for enhanced confidentiality [1]. While these DNA-based methods showed initial promise, they encountered challenges in maintaining consistent security across diverse image types. Subsequent research investigated Dynamic AES implementation with logistic chaotic mapping [2], achieving improved security parameters but revealing inherent tensions between confidentiality requirements and computational resources.

Further developments in the field included a compression-encryption framework utilizing dynamic symmetric key generation [3], though opportunities remain for improving data compression efficiency. Quantum cryptographic systems emerged as another avenue for securing medical imagery and sensitive content [4], presenting novel approaches to multi-level security, albeit with room for improving confidentiality metrics.

Investigation into inter-block difference techniques combined with AES implementations [5] contributed to the field, though image integrity optimization remains an ongoing challenge. Quantum technology-based encryption methods [6] demonstrated potential through expanded key-spaces and reduced time complexity, while deep neural network approaches [7] introduced new perspectives on image security, warranting further investigation into computational complexity implications.

Significant contributions to image encryption methodology include:

- Implementation of 2D Hénon-Sine mapping integrated with DNA coding [8]
- Development of asymmetric multiple image elliptic curve cryptography [9]
- Innovation in 2D Logistic Sine Chaotic Mapping (2D-LSMM) [10]
- Advancement in chaotic mapping techniques for image cryptography [11-12]
- Evolution of multimedia encryption through 2D alteration methodologies [12] Recent developments have focused on specialized applications, including:
- Integration of sine square logistic mapping with chaotic systems [13]
- Lightweight encryption protocols for healthcare applications [14]
- Compound Sine-Piecewise Linear Chaotic Mapping [15]
- Variable-length key implementations with modified Henon mapping [16]
- One-dimensional chaotic map amplification [17]
- Bisection method integration with piecewise chaotic mapping [18]
- Color/grayscale encryption utilizing sine-cosine cross-chaotic mapping [19]
- Novel asymmetric encryption methodologies [20]
- Research Objectives

This paper introduces the RISCSCADL (RuzickaIndexive Schmidt-Samoa Certificateless Artificial Deep Learning) technique, with the following primary objectives:

1. Enhancement of satellite image transmission security through:
    - Implementation of Ephemeral Agreement session key generation
    - Integration of Schmidt-Samoa certificateless signcryption
    - Application of Ruzicka indexive Schmidt-Samoa certificateless unsigncryption
2. Improvement of transmission confidentiality through:
    - Integration of Schmidt-Samoa certificateless signcryption with Connectionist Artificial Deep Neural Learning
    - Implementation of session-specific key generation
    - Application of deep learning-based cipher image generation with digital signatures
3. Optimization of integrity through:
    - Ruzicka similarity index-based signature verification
    - Sequential decryption methodology

- Enhanced protection against unauthorized image manipulation

The subsequent sections of this paper are organized as follows: Section 2 presents a comprehensive description of the RISCSCADL technique and associated system frameworks. Section 3 details the experimental setup and result analysis, while Section 4 provides comparative analysis against existing methodologies. Concluding remarks are presented in Section 5.

2. PROPOSED METHODOLOGY

2.1. System Overview

The evolution of multimedia processing has led to an increasing need for secure transmission and storage of diverse multimedia data across public networks. Digital images, in particular, present unique challenges in network communication due to their information-rich nature. This growing concern for privacy and security motivates the development of our proposed RISCSCADL technique.

2.2. Architecture Design

The RISCSCADL architecture implements secure image transmission through connectionist artificial deep neural learning. Figure 1 illustrates the system architecture, which processes satellite images through multiple security layers utilizing Schmidt-Samoa certificateless signcryption.

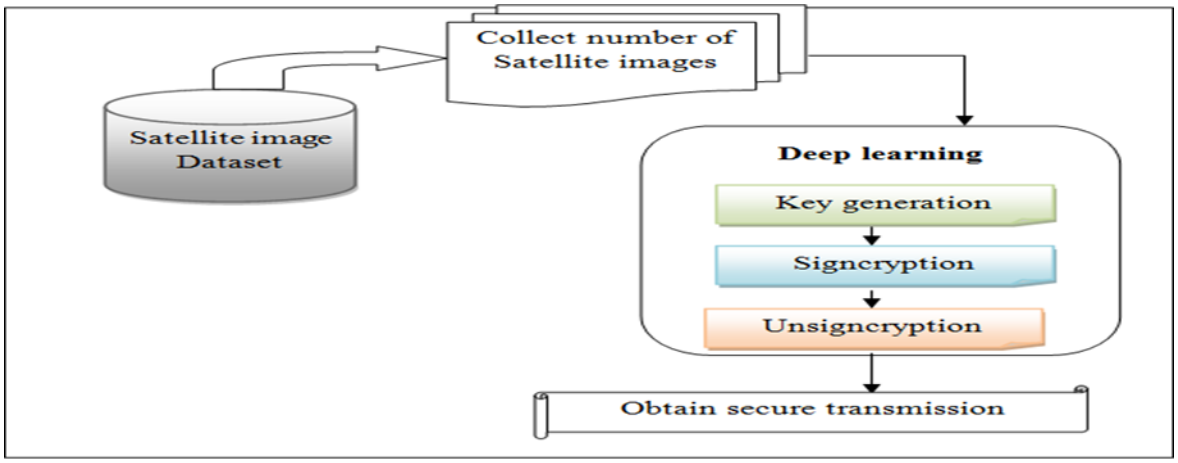

Fig.1 architecture for the proposed RISCSCADL

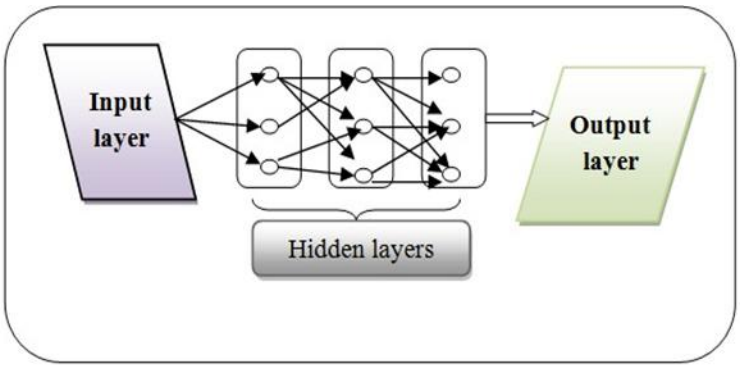

Fig. 2 schematic representations of connectionist artificial deep neural learning

The neural network architecture, depicted in Figure 2, employs a feed-forward methodology with multiple interconnected layers. This structure facilitates:

1. Input processing of satellite images
2. Progressive security implementation through hidden layers

3. Secure transmission of processed images

2.3. Neural Network Implementation

The network processes satellite images through three primary stages: Initial hidden layer:
Key generation

Second hidden layer: Signcryption processing Third hidden layer:
Unsigncryption implementation

The neural activity at the input layer follows the formulation: $yi = \sum(xi \times wij + bi)$ (1)

Where:

xi represents the satellite image count

wij denotes the input-hidden layer weight coefficient bi represents the bias term (value: +1)

The input is send into initial hidden layer where key generation process is performed by using Schmidt-Samoa certificateless signcryption technique. The signcryption method is further computationally efficient and also provides greater security as well as confidentiality.

A signcryption scheme includes three major processes namely Ephemeral Agreement session Key generation, Schmidt-Samoa certificateless signcryption, and Ruzicka indexive Schmidt- Samoa certificateless unsigncryption.

2.4. Security Implementation

- Ephemeral Agreement Session Key Generation

The security protocol initiates with dynamic session key generation, creating unique key pairs for each transmission session. This approach enhances security by:

- Generating session-specific private and public keys
- Disabling keys post-session
- Creating new keys for subsequent sessions The key generation process follows:

$m = p \times q$ (2)

Where p and q represent distinct large prime numbers, generating the public key m. The private key generation follows:

$d = e^{(-1)} \bmod \lambda(m)$ (3)

Where: $\lambda(m) = lcm(p-1, q-1)$ (4)

- Schmidt-Samoa Certificateless Signcryption

The signcryption process implements both encryption and digital signature generation. For satellite image I, pixel encryption proceeds as:

$P = pixel(I)$ (5)

The encryption algorithm generates the cipher image: $C = P^e \bmod m$ (6)

Where:

- C represents the cipher image
- e denotes the receiver's public key
- P represents the pixel values Digital signature generation follows: $S = H(M)^d \bmod m$ (7)

Where:

- S represents the digital signature
- H(M) denotes the hash function

- d represents the sender's private key

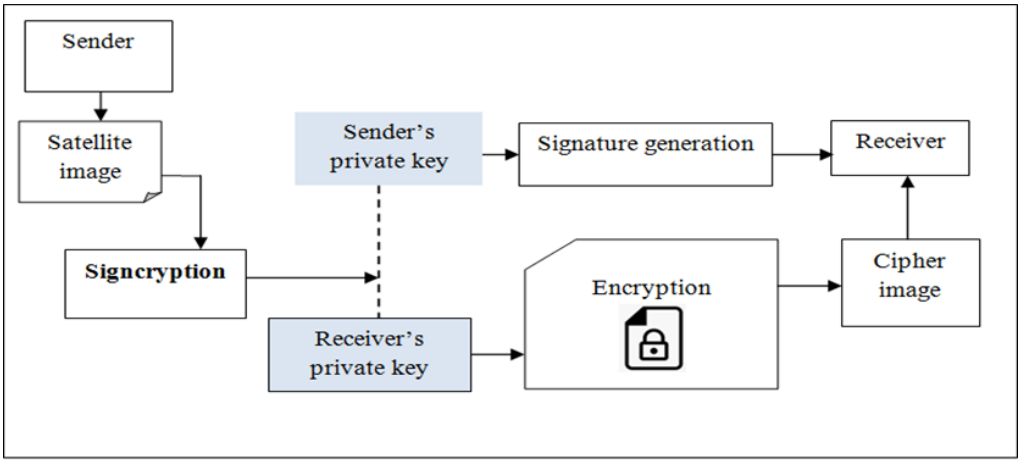

Fig. 3 Schmidt-Samoa certificate less signcryption

Fig. 3 demonstrates the block diagram of the Schmidt-Samoa certificate less signcryption consisting of encryption and digital signature generation. The sender first encrypts the images with aid of receiver's public key. Hence it is called public-key cryptography. Let us consider the number of satellite image $SI = \{si_1, si_2, \ldots, si_m\}$. The cipher image is obtained with aid of receiver's public key. Initially, the proposed technique study on the pixel value from input image.

$$\boldsymbol{P}(SI) = \begin{bmatrix} p_0 & p_1 & p_2 \\ p_3 & p_4 & p_5 \\ p_6 & p_7 & p_8 \end{bmatrix} \qquad \textbf{(5)}$$

Where, $P(SI)$ denotes pixels of input satellite image $p_0, p_1, p_2, \ldots \ldots p_n$. Then the encryption of image pixels is carried out as follows,

$$C(SI) = P(SI)^{E_{Bk}(R)} \ mod \ E_{Bk\,(R)} \qquad (6)$$

Where, $C(SI)$ denotes cipher image which is obtained based on receiver public key 'E_{Bk}' and the image pixels $P(SI)$. Subsequently, the digital signature of the input image is produced by using sender's private key.

Allow us consider input image pixels is transferred into a message bit $m_i \in [0,1]$. Then the signature is generated as follows:

$$\varphi_s = H\left(E_{pk\,(S)} | m_i\right) \qquad (7)$$

From (7), signature 'φ_s 'is generated by the sender's private key '$E_{pk\,(S)}$', H denotes a hash, m_i and denotes a message bit. Then the cipher image along with the signature is sent to the receiver.

- Ruzicka indexive Schmidt-Samoa certificateless unsigncryption

The unsigncryption process implements two-phase verification: Sr = H(M)^e mod m (8)

Where Sr represents the receiver-side signature verification.

The Ruzicka similarity coefficient (R) validates signature authenticity: R = ∑min(Si, Sj) / ∑max(Si, Sj) (9)

Where:

- Si represents the sender's signature
- Sj represents the receiver's signature Verification follows the condition:

R = {1 if valid, 0 if invalid} (10)

Upon successful verification, decryption proceeds:

I' = C^d mod m (11)

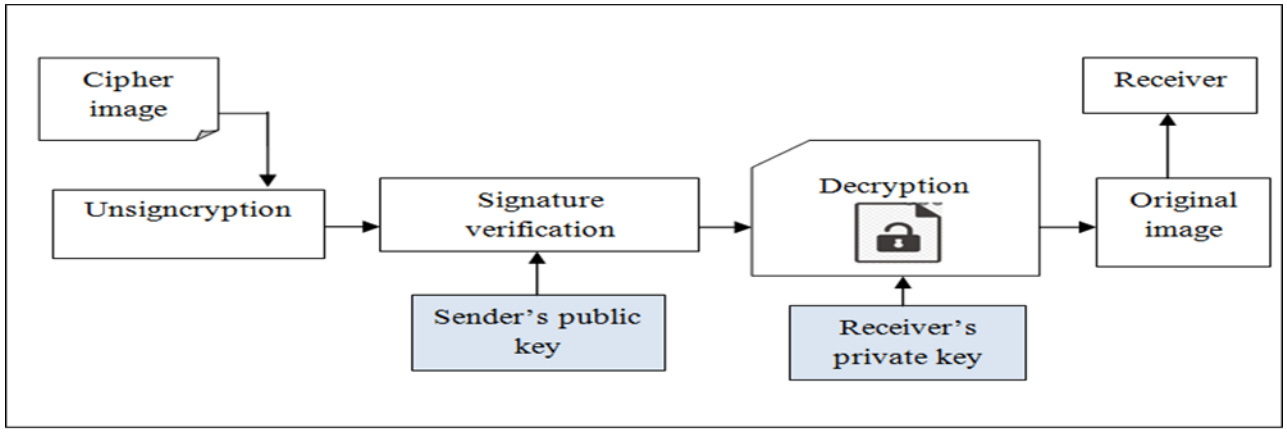

Fig. 4 block diagram of Ruzicka indexive Schmidt-Samoa Certificateless Unsigncryption

In above fig.4, represent the block diagram of Schmidt-Samoa certificate less signcryption. Lastly, proposed technique performs the unsigncryption based on the digital signature verification. At the receiver end, the signature of the received message is generated with the same hash function at the time of signcryption.

$$\varphi_s'' = H\left(E_{Bk\ (S)} | m_i\right) \quad (8)$$

Where, φ_s'' indicates a signature at the receiver with senders public key '$E_{Bk\ (S)}$'. Finally, verifies the generated signature φ_s'' is matched with the signature generated by the sender (φ_s) using Ruzicka similarity. Ruzicka similarity function is used for verifying the signature for ensuring the user is legitimate or not. The similarity between the two signatures is verified as a given blow:

$$\delta = \frac{\varphi_s \cap \varphi_s''}{\sum \varphi_s + \sum \varphi_s'' - \varphi_s \cap \varphi_s''} \quad (9)$$

In above (9),δ is a Ruzicka similarity coefficient, φ_s is a signature at sender, φ_s'' denotes a represents signature at receiver, $\varphi_s \cap \varphi_s''$ is a mutual dependence with signature. The Ruzicka similarity coefficient (δ) give the similarity value between 0 and 1.

$$\delta = \begin{cases} 1, & Signature\ is\ valid \\ 0, & Signature\ is\ not\ valid \end{cases} \quad (10)$$

In (10), Ruzicka similarity coefficient (δ) returns '$1'$, indicates that the signature is valid. Whereas $\delta = 0$ denotes indicates that signature is not suitable. If signature is suitable, then receiver decrypts the cipher image. Otherwise, the signature is said to be invalid and the receiver did not decrypt the cipher image. This helps to enhance the security of satellite image transmission between the sender and receiver. Therefore, the decryption is performed with the receiver's private key $\left(E_{pk\ (R)}\right)$ as given below,

$$SI = C(SI)^{E_{pk\ (R)}}\ mod\ xy \quad (11)$$

At last, the original image 'SI' is obtained. The hidden layer output is obtained as follows:

$$K\ (t) = [\sum_{i=1}^{n} si_i * v_1] + [v_2 * K_{(t-1)}] \quad (12)$$

Where, $K\ (t)$ indicates an output of a hidden layer, $K_{(t-1)}$ refers to an output from the previous hidden layer and 'v_2 'indicates a weight of the hidden layers, v_1 indicates a weight between input and hidden layers, si_i represents the input satellite image. Finally, the secured image transmission is obtained at the output layer.

$$Y = [v_3 * K\ (t)] \quad (13)$$

In (13), 'Y' is an output of deep learning, v_3 is a weight between hidden and output layer, $K\ (t)$ specified as output of a hidden layer. In this way, secure image transmission is performed with higher confidentiality by avoiding unauthorized access. The

algorithmic process of the secure image transmission is described as follows:

Input : Number of satellite images S1 = {si_1,si_2,si_3,…….,si_m}

Output : Increase the security of image transmission

Begin

Number of satellite images SI = {si_1,si_2,si_3,…….,si_m} taken as input at the input layer

Key generation //hidden layer 1

For each satellite images si transmission

Generate the pair of keys E_{pk} , E_{Bk}

End for

// Signcryption //hidden layer 2

Encrypt input image using receivers public key ' C(SI)'.

Generate digital signature with senders private key 'ϕ_s'

Send cipher image and digital signature to receiver

//Unsigncryption //hidden layer 3

Generate the digital signature 'ϕ_s'' '

If($\delta = 1$) then

Signature is valid

The receiver decrypts the cipher image using receiver private key 'SI'

Obtain original satellite image

Else

The signature is not valid

End if

End

Algorithm1 Ruzicka Indexed Schmidt-Samoa Certificate less Signcryptive Connectionist Artificial Deep Neural Learning for Secure Transmission using Satellite Images

Algorithm 1 given above describes the step-by-step process of secure image transmission. The numbers of images are collected from the database in the input layer. For each image transmission, key pair such as Ephemeral Agreement session Key generation process is performed in initial hidden layer. Followed by, signcryption process being carried out using Schmidt-Samoa certificateless signcryption in the second hidden layer. After the signcryption, Ruzicka indexive Schmidt-Samoa certificateless unsigncryption is performed in the third hidden layer.This helps to increase confidentiality and integrity.

2.5. Neural Network Output Processing

The hidden layer output computation follows:

$h = \sum(yi \times wij + wi)$ (12)

Where:

- h represents hidden layer output
- yi denotes previous layer output
- wij represents inter-layer weights

- wi represents input-hidden layer weights

The final output formulation:

$O = \sum(h \times wo)$ (13)

Where:

- O represents the network output
- wo denotes hidden-output layer weights

3. EXPERIMENTAL SETUP AND IMPLEMENTATION

3.1. Dataset Description

The experimental validation of the RISCSCADL technique was conducted using satellite imagery from the Hurricane Damage Assessment Dataset[1]. This comprehensive dataset was specifically chosen for its extensive collection of pre- and post-hurricane satellite imagery, enabling robust testing of the proposed security framework while maintaining practical applicability to disaster assessment scenarios.

- Implementation Environment

The implementation framework consisted of:

- Programming Platform: Java Development Environment
- Comparative Methods:

1. Proposed RISCSCADL technique
2. DNA-based key scrambling technique [1]
3. Dynamic AES implementation [2]

- Dataset Organization

The dataset architecture comprises four primary segments:

1. Training Dataset (train_another)
2. Testing Dataset (test)
3. Secondary Testing Set (test_another)
4. Validation Dataset (validation_another)

For this experimental analysis, we focused on the training dataset (train_another) which contains a balanced distribution of:

- 5,000 satellite images showing hurricane damage
- 5,000 satellite images showing undamaged regions

This balanced dataset distribution ensures unbiased evaluation of the security implementation while maintaining practical relevance to damage assessment applications.

- Experimental Objectives

The primary experimental objectives include:

1. Evaluation of secure transmission protocols for satellite imagery
2. Assessment of encryption efficiency for damage assessment applications
3. Comparative analysis of security measures against existing methodologies
4. Validation of system performance in practical disaster assessment scenarios

4. RESULTS AND PERFORMANCE ANALYSIS

This section presents a comprehensive evaluation of the proposed RISCSCADL methodology, analyzing its performance against established encryption approaches, specifically the DNA-based key scrambling technique [1] and Dynamic AES implementation [2]. The comparative analysis encompasses three critical performance metrics:

1. Confidentiality Rate Analysis: Assessment of information security preservation
2. Integrity Rate Evaluation: Measurement of data consistency maintenance
3. Computational Complexity Assessment: Evaluation of resource utilization efficiency

The following subsections present detailed quantitative analyses through statistical measurements and graphical representations, demonstrating the comparative advantages and limitations of each approach.

Our evaluation methodology emphasizes reproducibility and statistical significance in performance measurements.

4.1. Analysis of Confidentiality Rate

Confidentiality rate is a different significant parameter of secure image transmission from sender to receiver. The Confidentiality rate is calculated transmitted images accessed or viewed by authorized entity. The confidentiality rate is measured as:

$$Con_{Data} = \left(\frac{naa}{n}\right) * 100 \quad (14)$$

In (14), '(C_{Data})' is a data confidentiality rate refers to amount of images accessed or viewed by authorized entity 'n_{aa}' to number of images taken as input 'n'. The data confidentiality rate is measured in percentage (%).

Table 1 Confidentiality Rate

Number of satellite images	Confidentiality rate (%)		
	RISCSCADL	DNA-based key scrambling technique	Dynamic AES
1000	95	89	86
2000	93	88	83
3000	95	89	86
4000	94	88	85
5000	96	90	86
6000	95	88	85
7000	94	89	86
8000	95	91	88
9000	97	92	90
10000	96	91	89

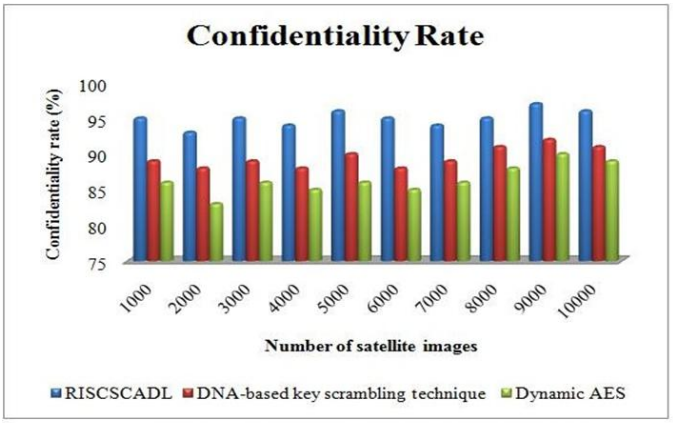

Figure 5 Performance of confidentiality rate

The performance analysis of confidentiality rate using three techniques RISCSCADL technique and DNA-based key scrambling technique [1], Dynamic AES [2] is depicted in Table I. The described outcome prove that RISCSCADL technique outperforms

well in terms of achieving a better confidentiality rate. The observed confidentiality rates of the three methods are illustrated in fig.5.

In Fig. 5 describe the performance of confidentiality rate Vs different number of satellite images using three methods RISCSCADL technique and DNA-based key scrambling technique [1], Dynamic AES [2]. The above figure demonstrates that the RISCSCADL method improve the confidentiality rate when compared to existing methods. To optimize performance, the RISCSCADL technique employs Schmidt-Samoa certificateless signcryption within a connectionist artificial deep neural learning framework, enabling secure communication through a sophisticated process of key generation, signcryption, and unsigncryption mechanisms. In the key generation, key pair is generated for each image transmission. In signcryption, the encryption and signature generation is performed. If signature is suitable, the authorized user receives the original image in unsigncryption and improves the secure image transaction. This helps to improve the confidentiality.

4.2. Analysis of Integrity Rate

Integrity rate is ratio of number of images which are not distorted or modified by any intruders to number of images transmitted. The integrity rate is measured as,

$$I_{rate} = \left[\frac{nn_a}{n}\right] * 100 \qquad (15)$$

From (15), I_{rate} denotes an image integrity rate, nn_a denotes the number of images that are not altered or modified by others, 'n' is a total number of images. The integrity rate is measured in percentage (%).

Table 2 Integrity rate

Number of satellite images	Integrity rate (%)		
	RISCSCADL	DNA-based key scrambling technique	Dynamic AES
1000	94	87	85
2000	92	86	84
3000	94	88	85
4000	93	86	84
5000	95	88	85
6000	94	86	84
7000	93	87	85
8000	94	89	86
9000	96	90	88
10000	95	89	86

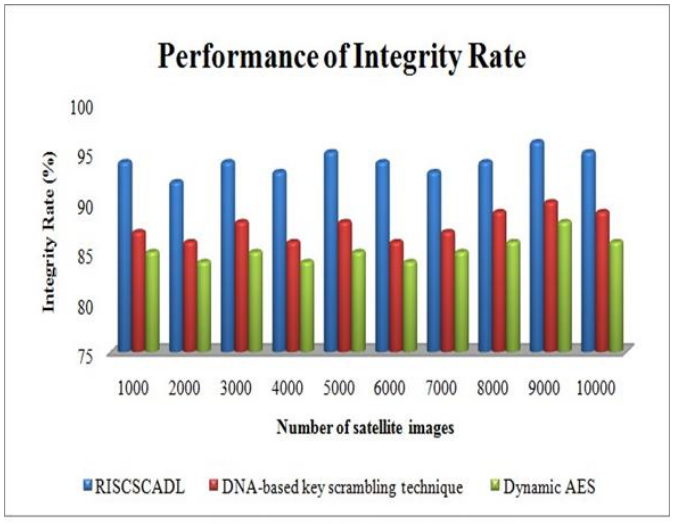

Fig. 6 Performance of Integrity Rate

Table 2 and fig. 6 noticed that the integrity rate of three different techniques RISCSCADL technique and DNA-based key scrambling technique [1], Dynamic AES [2] according to number of images gathered from dataset. In experimental consideration, the numbers of images are taken in the ranges from 1000 to 10000. Compared to existing methods, the RISCSCADL technique increases the integrity rate. Let us consider 1000 images for conducting the experiments. By applying RISCSCADL, the observed image integrity rate using RISCSCADL is 94%. The integrity rates of DNA-based key scrambling technique [1] and Dynamic AES [2] were evaluated across multiple experimental outcomes. The RISCSCADL technique demonstrated superior performance, enhancing integrity rates by approximately 7% compared to [1] and 10% relative to [2], signifying a notable improvement in cryptographic efficacy. This is due to the application of signature generation in hash value. In hash function generation, the original pixel values are not altered by any intruders. This helps to improve the integrity rate.

4.3. Analysis of Computational Complexity

It is defined as amount of time taken to carry out secure communication of satellite images. The computational complexity is measured as:

$$CC = n * t\ (SCSI) \quad (16)$$

From (16),CC denotes a computational complexity, 'n' is a number of images, and '$t\ (SCSI)$' is a time taken for secure image transmission. Computational complexity is measured in milliseconds (ms).

Table 3 Computational Complexity

Number of satellite images	Computational complexity (ms)		
	RISCSCADL	DNA-based key scramblin g technique	Dynamic AES
1000	30	35	40
2000	34	38	44
3000	39	45	48
4000	46	52	56
5000	55	60	65
6000	59	66	72
7000	64	70	75
8000	76	79	84
9000	80	83	86
10000	86	90	92

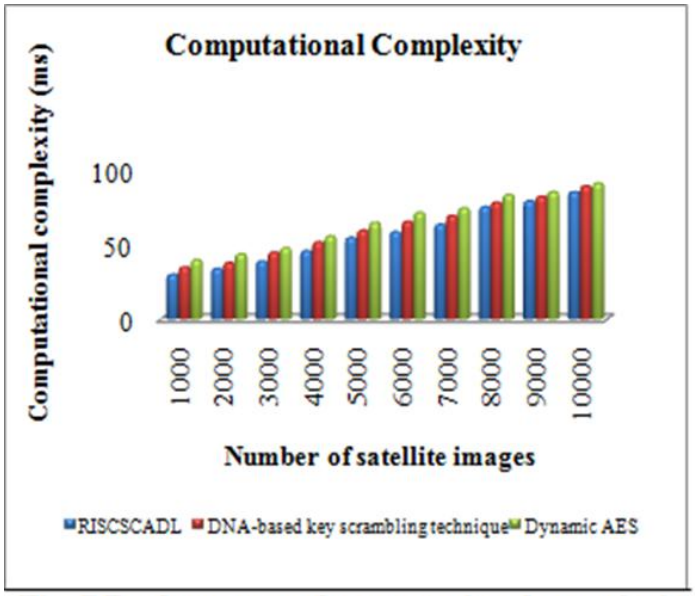

Fig. 7 Performance of computational complexity

In Table 3 and fig. 7, shows the performance results of computational complexity of three different methods RISCSCADL technique and DNA-based key scrambling technique [1], Dynamic AES [2]. The experimental results specified to computational complexity of RISCSCADL is relatively lesser computational complexity than conventional methods. With the consideration of 1000 images, the time consumption taken to perform secure image transmission was found to be '$30ms$' using RISCSCADL. However, the time consumption of existing [1] [2] was found to be $35ms$' and $40ms$ respectively. The experiential results specify that RISCSCADL lesser the computational complexity. Comparative analysis of ten experimental results reveals that the RISCSCADL method significantly reduces time consumption, demonstrating a 9% improvement over existing method [1] and a 16% reduction compared to method [2], highlighting its computational efficiency. This is owing to application of the Connectionist Artificial Deep Neural Learning technique for improving the security of image communication by lesser time consumption.

5. CONCLUSION

In secured transmission, image encryption is essential in field of digital world. To overcome this work, a RISCSCADL technique-based image signcryption system is developed for enhancing the security level through encryption as well as digital signature generation. First, the Schmidt-Samoa certificate less signcryption is employed to CADL for increasing the security level by three different processes namely Ephemeral Agreement session Key generation, Schmidt-Samoa certificate less signcryption, and Ruzicka indexive Schmidt-Samoa certificate less unsigncryption. The experimental evaluations are performed with total number of satellite images and compared to two existing algorithms. The observed results have confirmed to proposed RISCSCADL method has improved performance in confidentiality rate, integrity rate, and computational complexity than other state-of-the-art methods.

REFERENCES

[1] Machbah Uddin, Farah Jahan1 , Mohammad Khairul Islaz, Md. Rakib Hassan, "A novel DNA-based key scrambling technique for image encryption", Complex & Intelligent Systems, Springer, Volume 7, 2021, Pages 3241–3258.
[2] Mahdi Shariatzadeh, Mohammad Javad Rostami, Mahdi Eftekhari, "Proposing a novel Dynamic AES for image encryption using a chaotic map key management approach", Optik, Elsevier, Volume 246, 2021, Pages 1-13.
[3] Emy Setyaningsih, Retantyo Wardoyo, Anny Kartika Sari, "Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution", Digital Communications and Networks, Elsevier, Volume 6, Issue 4, 2020, Pages 486-503.
[4] T. Janani, M. Brindha, "A secure medical image transmission scheme aided by quantum representation", Journal of Information Security and Applications, Elsevier, Volume 59, 2021, Pages 1-19.
[5] Srinivasa Rao Thamanam, Potti Nagaraja, B. Balaji Naik & K. Manjunathachari, "A Novel Image Encryption Technique Based on Inter Block Difference", Journal of Shanghai Jiaotong University (Science), Springer, Volume 26, 2021, Pages 488-493.
[6] Manju Kumari & Shailender Gupta , "Performance comparison between Chaos and quantum- chaos based image encryption techniques", Multimedia Tools and Applications, Springer, Volume 80, 2021, Pages 33213-33255.
[7] Shima Ramesh Maniyath , Thanikaiselvan V, "An Efficient Image encryption using Deep Neural Network and Chaotic Map", Microprocessors and Microsystems, Elsevier, Volume 77, 2020.
[8] Junxin Chena, Lei Chen, Yicong Zhou, "Cryptanalysis of a DNA-based image encryption scheme", Information Sciences, Elsevier, Volume 520, May 2020, Pages 130-141.
[9] Wei Li, Xiangyu Chang, Aimin Yan, Hongbo Zhang, "Asymmetric multiple image elliptic curve cryptography", Optics and Lasers in Engineering, Elsevier, Volume 136, 2021, Pages 1- 10.
[10] Jieyu Zheng and LingFeng Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map", IET Image Processing, Volume14, Issue11, 2020, Pages 2310-2320.
[11] Abdellatif JarJar, "Image Encryption Using Hybrid Cryptographic System Incorporating Three Improved Standards" Image Encryption Using Hybrid Cryptographic System Incorporating Three Improved Standards", Complex & Intelligent Systems, Springer, Volume 7, 2021, Pages 3241–3258.
[12] Ibrahim Yasser, Mohamed A. Mohamed, Ahmed S. Samra, and Fahmi Khalifa, "A Chaotic-, Based Encryption/Decryption Framework for Secure Multimedia Communications", Entropy 2020, Pages 1-23.
[13] Bedir Yousif, Fahmi Khalifa, Ahmed Makram and Ali Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps", AIP Advances, Volume 10, Pages 1-10.
[14] Mohammad Kamrul Hasan, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha- Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam, Saleh Alyahya, Musse Mohamed Ahmed, Samar Kamil and Md Arif Hassan, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications", IEEE Access, Volume 9, 2021, Pages 47731 – 47742
[15] Shijie Zhang and Lingfeng Liu, "A novel image encryption algorithm based on SPWLCM and DNA coding", Mathematics and Computers in Simulation, Elsevier, Volume 190, 2021, Pages 723-744.
[16] Hongxiang Zhao, Shucui Xie, Jianzhong Zhang, Tong Wu, "A dynamic block image encryption using the variable-length secret key and modified Henon map", Optik, Elsevier, Volume 230, 2021, Pages 1-22.
[17] Ali Mansouri and Xingyuan Wang, "A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme", Information Sciences, Volume 563, 2021, Pages 91-110.
[18] Aesha N. Elghandour, Ahmed M. Salah, Yasser A. Elmasry, Abdelrahman A. Karawia, "An Image Encryption Algorithm Based on Bisection Method and One-Dimensional Piecewise Chaotic Map", IEEE Access, Volume 9, 2021, Pages 43411 – 43421.
[19] Noura Khalil, Amany Sarhan, Mahmoud A.M. Alshewimy, "An efficient color/grayscale image encryption scheme based on hybrid chaotic maps", Optics & Laser Technology, Elsevier, Volume 143, 2021, Pages 1-21.
[20] Yabin Zhang, Li Zhang, Zhi Zhong, Lei Yu, Mingguang Shan, Yigui Zhao, "Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation", Optics and Lasers in Engineering, Elsevier, Volume 143, 2021, Pages 1-12.

Authors

Dr. S. Padmalal, is currently working as Professor in the Department of Computer Science and Engineering at Mangalam College of Engineering, Kottayam District, Kerala, India. He Studied B.Sc computer science and M.C.A from Madurai Kamaraj Univetrsity, Madurai. He received the Master Degree M.Tech and Master of Philosophy (M.Phil) from Manonmaniam Sundaranar University, Tirunelveli, and Tamilnadu. He received his PhD degree (November – 2015) in computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu. He has 24 years of experience in teaching and administrative field in the technical level institutions. He has published a number of papers in national and international journals. His research interests include Image Processing, Networking, Network security and Cloud computing.

Dr. I. Edwin Dayanand, retired as Principal in Moderator Gnanadason Polytechnic College, Nagercoil, Kanyakumari District, Tamilnadu, India. He got his M.Sc Physics degree from Madurai Kamraj University, Tamilnadu in the year 1987, MCA degree in the year 1993, M.Tech in Computer and Information Technology in the year 2011 from Manonmaniam Sundaranar University. He received his PhD degree in computer and Information Technology in 2021 from Manonmaniam Sundaranar University, Tirunelveli, and Tamilnadu. He has 33 years of experience in teaching and administrative field in the technical level institutions. He has published a number of papers in national and international journals. His research interests include Image Processing, Networking, and Network security and Cloud computing.

Dr. F.R. Shiny Malar was born in Nagercoil, Tamil Nadu State, India in 1986. She studied Information Technology in St.Xavier's Catholic college of Engineering, Chunkankadai, Kanyakumari District, Tamil Nadu State, India from 2003 to 2007. She received Bachelor degree from Anna University, Chennai in 2007. She received the Master degree from Manonmaniyam Sundaranar University Tirunelveli. And also received Doctorate degree in the Department of Computer Science and Engineering, in Noorul Islam Center for Higher Education, Noorul Islam University, Kumarakoil, Tamilnadu, India; Currently she is working as a Professor in Stella Mary's College of Engineering, Nagercoil, Tamil Nadu State, India. She has published more than 10 international journals and presented more than 10 papers in international and national conferences and their research interest include image security, networking and image processing. She has published a patent on "Water Management and leakage Detection problems solutions using IOT" and also published a book chapter on "Advances in Computer Technology and Applications".