Hindusthan Institute of Technology
(AN AUTONOMOUS INSTITUTION)

ICECMSN

# 4th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN 2024)

**28-29, November 2024**

# Proceedings

ELSEVIER


Organised by

Hindusthan Institute of Technology,
Coimbatore, India

| | |
|---|---|
| 73 | Analysis of Solar Panel Power Investigation using Fixed Axis, Single Axis and Dual Axis Solar Tracker<br>*Md. Humayun Kabir, Md. Himel Abu Jihad, Suman Chowdhury* |
| 74 | Advancing Bionic Solution through Artificial Intelligence in Healthcare IoT Environment<br>*Girish Wali, Dr. Chetan Bulla* |
| 75 | Lamport Blum Shub Signcryptive Extreme Learning Machine for Secure Transmission of Digital Images<br>*V Prabavathi, Dr. M Sakthi* |
| 76 | A Novel Stable Feature Selection Algorithm for Machine Learning based Intrusion Detection System<br>*Sowmya T, Dr. Mary Anita E A* |
| 77 | Fake News Detection: Exploring the Efficiency of Soft and Hard Voting Ensemble<br>*Arifur Rahman, Sakib Zaman, Shahriar Parvej, Pintu Chandra Shill, Md. Shahidul Salim, Dola Das* |
| 78 | Predicting Institute Graduation Rate using Evolutionary Computing and Machine Learning<br>*Mala H Mehta, N C Chauhan, Anu Gokhale* |
| 79 | Cloud based LoRaWAN Enabled Water Tank Automation Framework<br>*Abubeker K M, Aravind Nuthalapati* |
| 80 | Reduction of Mismatch Power Loss in a Partially Shaded Photovoltaic System using the OTR<br>*Shivangi Mittal, Amit Mittal, Dhiraj Nitnawre* |
| 81 | Enhancing Educational Video Discovery using Advanced Latent Semantic Analysis<br>*Dr. B Sindhu, A Bhaskar, G Yugesh, S Reshma, B Rohit* |
| 82 | EM-ACO-ARM: An Enhanced Multiple Ant Colony Optimization Algorithm for Adaptive Resource Management in Cloud Environment<br>*Prathamesh Lahande, Parag Kaveri, Harvinder Singh, Sukhjit Singh Sehra, Jatinderkumar R Saini* |
| 83 | Stray Dog Detection System using YOLOv5<br>*Ashwini Bhosale, Pranav Shinde, Yash Firke, Shivprasad Patil, Pranav Mitake, Samruddhi Shinde* |
| 84 | Application of Hyperledger Blockchain Technology to Logistics Supply Chain with IoT<br>*Ahmet Sayar, Muhammet Cuneyd Kurtbas, Caglayan Sancaktar, Rana Dudu Kabak, Sukru Cakmak* |
| 85 | Floral-Inspired Artificial Magnetic Conductor for Versatile Dual-Band Wireless Communication<br>*Vishakha Yadav, Abhijyoti Ghosh, Achinta Baidya, Zonunmawii, L Lolit Kumar Singh, Sudipta Chattopadhyay* |
| 86 | Leveraging Deep Learning for Comprehensive Multilingual Hate Speech Detection<br>*Atul Kumar Srivastava, Mitali Srivastava, Sanchali Das, Vikas Jain, Tej Bahadur Chandra* |
| 87 | Integrating Human Motion Dynamics in CNN Architecture to Recognize Human Activity from Different Camera Angles<br>*Kishan Kesari Gupta, Joo-Ho Lee, Parag Ravikant Kaveri, Prashant Awasthi* |

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2025) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Evolutionary Computing and Mobile Sustainable Networks

# Lamport Blum Shub Signcryptive Extreme Learning Machine for Secure Transmission of Digital Images

[1]Ms. V.Prabavathi[1], Dr. M. Sakthi[2]

[1]*Research Scholar, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Affiliated to Bharathiar University Pollachi, Tamil Nadu,India.*
[1]*prabadhanya11@gmail.com*
*ORCID:0000-0003-4325-1152*
*Ph.No: 9095544124*

[2]*Associate Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Affiliated to Bharathiar University Pollachi, TamilNadu,India*
[2]*sakthi.cs.phd1@gmail.com*
*Ph.No.:9842025261*

**Abstract**

Image transmission refers to sending or transferring digital images from one location to another, typically over a network or communication channel across various domains, including telecommunications, multimedia messaging, surveillance systems, medical imaging, remote sensing, etc. However, with growing popularity of digital skills, ensuring safety and integrity of transmitted images has become a significant concern. For increasing security, Machine learning and cryptographic techniques have been discussed. Nevertheless, confidentiality during image transmission faces major challenges. Proposed Lamport Blum ShubSigncryptive Extreme Learning (LBSSEL) Method is introduced for secured image transmission with minimal time consumption. The Extreme Learning machine comprises different layers. Several natural images gathered as of dataset. The input layer receives these images for secure transmission. The proposed cryptographic method performs key generation, signcryption, as well as unsigncryption. Lamport One-Time Digital signature method applied in first hidden layer to generate key pairs. Signcryption carried out in second hidden layer which includes encryption and digital signature. For secured transmission, an encrypted image (i.e., cipher image) as well as signature broadcast to receiver to preserve input image. In third hidden layer, unsigncryption process carried out for receiving original image by authorized users through signature verification and decryption. Finally, confidentiality is improved during image transmission at the output layer. Simulation estimated with dissimilar factors. Outcomes of LBSSSEL model in terms of achieving maximum PSNR, confidentiality during transmission, with minimal time consumption when compared with existing approaches.

*Keywords:* Image transmission, security, Signcryption, Extreme Learning, Lamport One-Time Digital signature method, Blum Shub pseudorandom number generator.


Peer-review under responsibility of the scientific committee of the 4th International Conference on Evolutionary Computing and Mobile Sustainable Networks

## 1. Introduction

Digital images are electronic representations of visual information, such as photographs, graphics, or illustrations, during different fields namely photography, art, medicine, science, and communication. Digital image transmission refers to the process of sending images from one location to another over wireless networks. Due to the nature of wireless communication transmission, ensuring security is a challenging task, aiming to guarantee confidentiality, integrity, and authenticity while mitigating the risk of unauthorized access.

For secret sharing between users, modified Robust Reversible Watermarking in Encrypted Images by Secure Multi-party (RRWEI-SM) scheme was developed [1]. However, the lightweight encryption did not enhance safety. Defense performance was developed in [2] by discrete memristor-basis of logistic map with a deep neural network. However, issue of time-efficient security enhancement remained unaddressed.

With higher protection, AES method was designed [3]. However, it did not perform secure communication. To enhance secure transmission, double image encryption method was introduced [4]. However, it was difficult to perform encryption with multiple images to achieve a more detailed security level.

Transport images are protected in [5] with significant Visual Cryptography. An image broadcast was preserved in [6] by symmetric image encryption structure. However, confidentiality level was not improved.

The secure medical image transmission method was introduced in [7]. However, it failed to support the transmission of multiple medical images. Safety was increased [8] by image cryptosystem adopting quantum chaotic map technique.

New grayscale image cryptosystem was introduced in [9], based on hybrid chaotic maps for improving security. However, neuro-fuzzy were not employed. A new image encryption approach was developed in [10] and [11] utilizes chaotic map and RSA algorithm respectively. However, computational complexity was high.

In [12], visually secure image encryption model was developed. However, secure transmission was not improved. A secure image encryption method was introduced in [13] using chaos-based block permutation. Nevertheless, big data environments were not applicable. A hash-based digital image encryption algorithm was designed in [14] to enhance security. However, the image quality was not improved after decryption. A new secure video occupancy monitoring model was developed in [15], integrated with encryption highly secure against several attacks. But, it failed to lessen time.

Contributions to this article.

LBSSEL method contributions given by,

LBSSEL method has been developed, incorporating the Signcryption, Extreme Learning, Lamport One-Time Digital signature for enhance protection of image transmission.

For enhancing image quality, Lamport One-Time Digital Signature-based cryptographic technique is implemented within an Extreme Learning Machine (ELM). This helps to improve PSNR.

To enhance confidentiality rate, Blum Shub pseudorandom number generator is utilized in the key generation process. Subsequently, encryption and decryption are carried out using these keys, preventing unauthorized receivers from accessing the image.

To enhance integrity rates, the LBSSEL method performs signature verification before image decryption. The signature validation ensures that the image received by an authorized user remains unaltered by intruders, thereby enhancing data integrity rates.

To minimize computational time, key generation, signcryption, and unsigncryption processes are executed within the hidden layers of the extreme learning machine during image transmission.

Finally, a comprehensive and comparative analysis performed by LBSSEL using various metrics.

**Road map:**

Remaining portions of article are arranged: related works described in Section 2. Proposed LBSSEL

Method along with a clear architecture diagram explained in Section 3. Section 4 elaborates on the experimental settings. Performance assessment of LBSSEL Method technique in comparison with existing techniques is illustrated in Section 5. Summary presented in Section 6.

## 2. **Method**

LBSSEL Method described with enhancing security during image transmission via a wireless network. With the extensive growth of information technology, confidentiality, as well as integrity frequently risked via prohibited behavior during digital image transmission from one place to another. This problem is overcome by introducing cryptographic methods called LBSSEL to protect the privacy of digital images during the transmission.

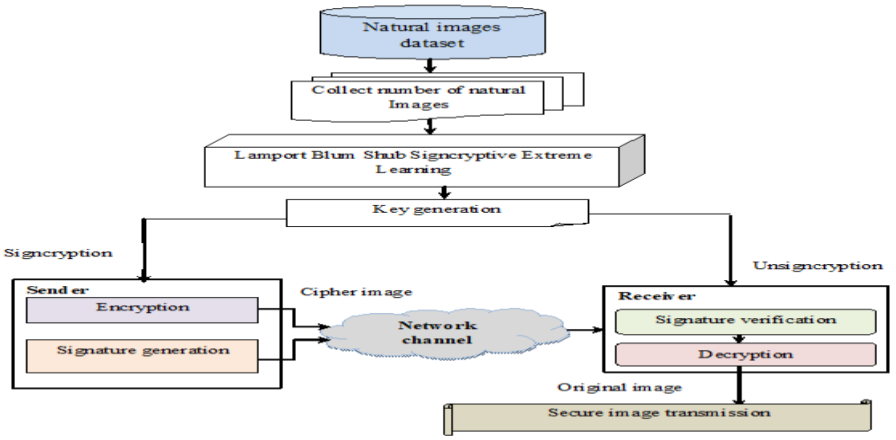


**Figure 1 Structural design of LBSSEL**

By improving secure image transmission, LBSSEL design depicted in Figure 1. In dataset, several natural images gathered. Cipher image generated by Signcryption technique. The proposed technique comprises three major steps. Signcryption process simultaneously performs both encryption and signature generation at sender's side. During wireless communication channel, cipher image is transmitted toward receiver. Signature verification and decryption process are executed in receiver end. Based on the above process, secure image transmission between the sender and receiver is achieved. The explanation of LBSSEL Method illustrated as given below.

### 2.1 Lamport Blum ShubSigncryptive Extreme Learning-based secure image transmission

Extreme Learning Machine has feed-forward neural networks. The ELM is an efficient technique for fast and efficient learning from large-scale data, resulting in increased training speed as well as simplicity than traditional DL methods. The signcryption is implemented into the ELM to further enhance the performance of a security with minimal time. Signcryption combines digital signature as well as encryption offering efficiency and security compared to conventional encryption algorithms.

In traditional cryptographic techniques, signature and encryption are typically performed as separate steps. However, Signcryption reduces computational overhead by simultaneously performing the signature generation as well as encryption operations. It provides integrated security guarantees, including authenticity, integrity, and confidentiality, ensuring more robust protection for transmitted images.

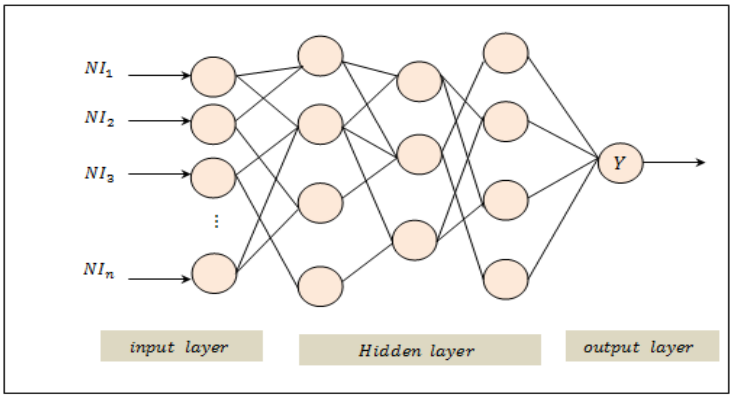


**Figure 2 Structure of extreme learning machines**

Extreme learning machines structure portrayed in Figure 2 which includes one input layer, three hidden layers, as well as one output layer. Every layer consists of a tiny individual unit named neuron. This helps to transfer the input from one layer to another. Assume training set {NI, Y}, 'NI $NI$' indicates training natural images {NI_1,NI_2,NI_3,….,NI_n } $\{NI_1, NI_2, NI_3, \ldots., NI_n\}$ and 'Y $Y$' representing its output of extreme learning machines.

The input layer receives the number of natural images, but it does not perform any calculations. The neurons in layer assign the weights and the biasfor each input image as follows,

$$A = \sum_{i=1}^{n} \sum_{j=1}^{m} (NI_i * Q_j) + B_{ih} \quad (1)$$

Where, $A$ indicates a neuron output, $Q_j$ denotes weights among input as well as hidden layer $NI_i$is palm image. Here, bias indicates ' $B_{ih}$. Input sample transmit to first hidden layer. Employing Lamport key generation algorithm, key generation executed.

Let us consider the random numbers generated by applying a Blum-Blum-Shub pseudorandom number generator.

$$R = P_n^2 \ mod \ M(2)$$

$$M = x * y(3)$$

Where,$P_n$ denotes a pseudorandom number in the sequence, $M$denotes a product of two large prime numbers x and y. The generated number 'R' is secret signature key.(i.e. private key)

$$S_k = R \quad (4)$$

Public verification key $P_k$ generated by,

$$P_k = F(R) \quad (5)$$

In (5), one-way function is $F(R)$ as well as given by,

$$F(R) = R + 1 \ mod \ 16 \quad (6)$$

The one-way function generates the public verification key with the secret key. In this way, secure image transmission enhanced by creating private as well as public key.

- **Signcryption**

Second hidden layer performs Signcryption process. Signcryption simultaneously performs digital signature as well as encryption, thereby reducing the computational time and enhancing security.

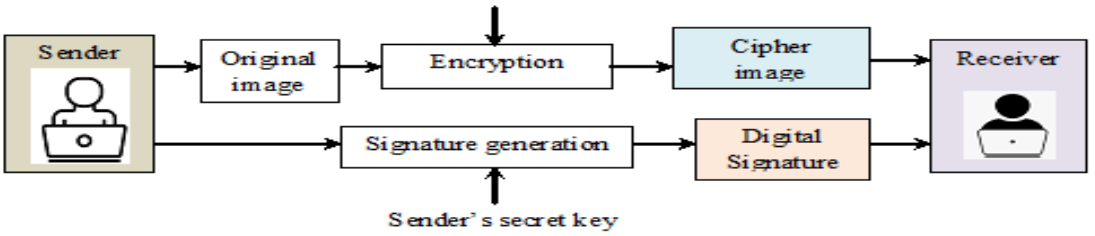


**Figure 3 block diagram of signcrypion**

Signcryption process illustrated in above Figure 3 which includes both encryption as well as signature generation.

Let us consider the input image $NI_1, NI_2, .., NI_n$ and the ⟦$NI_1$, $NI_2$, $NI_n$) number of pixels in images denoted by $\beta_1, \beta_2, .., \beta_m$ β1, β2, βm that encrypted by receiver public key as follows,

$$CI \leftarrow Enc\left[P_{kr}, \beta_j\ (NI)\right] \quad (7)$$

Where, $CI$indicates a cipher image, $Enc$Encis encryption by public key of receiver $(P_{kr})$,$\beta_j\ (NI)$indicates a pixel of natural images. Sender's private key creates digital signature. In the signature generation phase, first digests the input pixel by applying the hash function.

$$D = H\ (\beta_j(NI)) \quad (8)$$

Where $D$ denotes a message digest, $D \in \{0,1\}$D ∈ {0,1} denotes a hash$H$' of the pixel of input image '$\beta_j(NI)$'$\beta_j$(NI)'. Then map the hash value by location of sender private key to generate the signature. For each bit in the hash value, the signer selects one number from the corresponding pair in the private key.

$$\varphi_S = \{S_{ks\ (i,j)}: S_{ks\ (i,0)}\ if\ D = 0\ and\ S_{ks\ (i,1)}\ if\ D = 1\} \quad (9)$$

Where, $\varphi_S$φ$_S$ represents the signature, $D$ denotes a message digest that map to location of private key $S_{ks}$of sender. If the bit is D=0, the sender selects the first number from the pair. If the bit is 1 (i.e. D=1), the sender selects the second number from the pair. This process produces a sequence of numbers to form the signature. Finally, the sender transmits the cipher image"$CI$' and signature '$\varphi_S$' to the receiver through the wireless communication channel.

- **Unsigncryption**

Unsigncryption process executes third hidden layer to securely receive the original image. Unsigncryption refers to the process of reversing the signcryptionoperation, that is, decrypting the ciphertext and verifying the signature to recover the original image. This process involves two main steps signature verification and decryption.

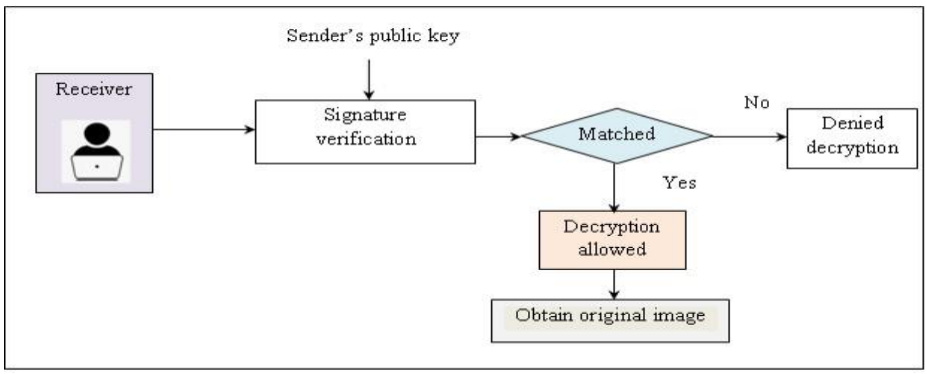


**Figure 4 block diagram of the unsigncryption process**

An unsigncryption explained in figure 4. Via sender's public key, receiver conducts signature verification utilizing sender's public key.Lamport signature verification scheme employed to reconstruct hash value using the following function.

$$\varphi_S{}' = F\ (\varphi_S) \quad (10)$$

$$F\ (\varphi_S) = \varphi_S + 1\ mod\ 16 \quad (11)$$

Where '$\varphi_S{}'$' indicates a reconstructed signature in receiver area, $F$ is one-way function, $\varphi_S$ signature at sender side is During sender's public key, reconstructed signature is verified.

$Z = \begin{cases} \varphi_S{}' = P_{ks}; \text{signaturevalid} \\ \text{otherwise}; \text{signaturenotvalid} \end{cases}$ When signature suitable, receiver decrypts cipher image. Otherwise, receiver failed to decrypt cipher image. With this, safety was ensured among sender as well as receiver. Authorized receiver decrypts cipher image as follows,

$$NI \leftarrow Dec[S_{kr}, CI] \quad (13)$$

Where $NI$ is original image, '$Dec$' is decryption, $S_{kr}$ is sender private key, $CI$ is cipher image. In authorized receiver, original image achieved. Output layer obtains secured transmission with maximum integrity.

| **// Algorithm 1: Lamport Blum Shub Signcryptive Extreme Learning based secure image transmission** |
|---|
| **Input:** Dataset, Number of natural images$NI_1, NI_2, NI_3, \ldots, NI_n$,<br>**Output:** Enhance security of image transmission |
| **Begin**<br>**1. Collect** the number of natural images$NI_1, NI_2, NI_3, \ldots, NI_n$, **-input layer**<br>2. **for each** input images<br>**3.** Allocate weight and bias using **(1)**<br>4. **End for**<br>**5. For each user -------hidden layer 1**<br>**6.** Create private and public key using(4) (5)<br>**7. End for**<br>**Signcryption**<br>**8.** Encrypt the image using receivers public key CI←Enc $[P_{kr}, \beta_j\ (NI)]$CI ← Enc $\left[P_{kr}, \beta_j(NI)\right]$**--hidden layer 2**<br>9. Generate digital signature '$\varphi_S$' using (9)<br>10. Send CI and $\varphi_S$ to receiver |

**Unigncryption**
11. **for each** signature $\varphi_S$ --**hidden layer 3**
12. Reconstruct the signature using (10) (11)
13. **End for**
14. **If** ($\varphi_S'$'=$P_{ks}\varphi_S' = P_{ks}$) **then**
15. Signature valid
16. **else**
17. Signature not valid
18. **End if**
19. **If** signature valid **then**
20. Receiver decrypt the image using **(13)**
21. **End if**
22. Achive security of image transmission -- **output layer**
23. **End**

Secure image transmission among sender and receiver illustrated in Algorithm 1. Initially, input layer receives the natural images provided by the sender. Subsequently, the input images are transferred to the first hidden layer. Private and public keys produced in Lamport key generation by all user, utilizing the Blum-Blum-Shub pseudorandom number generator. Once the keys are generated, the signcryption process is executed. This process involves encryption and signature generation. Signature cipher image and signature are then transmitted to the receiver. Unsigncryption implements third hidden layer. Signature verification employed in sender's public key. Signature verified, user is considered an authorized user. Decryption executed for obtaining original image. Secure transmission from sender to receiver is successfully completed.

## 3. Simulation Result

Proposed LBSSEL, conventional methods [1] and [2] is implemented in Python. To conduct the simulation, a dataset of Nature Images is collected from the Kaggle repository (https://www.kaggle.com/code/nageshsingh/nature-image-classification/input). This image dataset comprises Natural Scenes from various locations around the world. The dataset consists of images extracted from the training folder specifically 14034 images sized 150x150 pixels located in the 'seg_train' folder. These images are distributed evenly across six classifications. Each category contains a varying number of images, with some categories having more images than others.

## 4. Performance comparison analysis

This section analysis various factors namely PSNR, confidentiality level, and integrity rate and execution time of LBSSEL and traditional techniques [1] and [2].

**PSNR:**: It estimates superiority of decrypted image via MSE. MSE calculated as dissimilarity among original image size as well as accurately decrypted image.

$$PSNR = 10 * \left[log_{10}\left(\frac{255^2}{MSE}\right)\right] \qquad (14)$$

$$MSE = \sum(NI_o(size) - NI_R(size))^2 \quad (15)$$

Where $PSNR$ denotes a Peak signal-to-noise ratio, $MSE$ denotes a mean square error, $NI_o(size)$ indicates original natural image size, $NI_R(size)$ denotes the reconstructed image or decrypted image size natural images. The peak signal-to-noise ratio is measured in decibels (dB). The higher the peak signal to noise ratio, the quality of

decrypted image gets improved.

**Confidentiality rate:** It defined as proportion of number of images received through authorized users. It determined in percentage (%).

$$CR = \sum_{i=1}^{n} \left[\frac{IRAU}{NI_i}\right] * 100(16)$$

Where, CR$CR$ denotes a Confidentiality rate,$NI$ indicates number of images, $IRAU$ denotes the number of natural images received via official user.

**Integrity rate:** This metric is determined by percentage of number of images that remain unmodified or unaltered. By unauthorized users to the total number of images transmitted over the communication channel

$$= \sum_{i=1}^{n} \left[\frac{IUA}{NI_i}\right] * 100(17)$$

Where, $IR$ denotes an integrity rate, $NI$ indicates number of images, number of natural images unaffected indicated as IUA. It estimated in percentage (%).

**Computational time:** it referred to as time consumed for secure image transmission from sender to receiver distressed data samples is defined as the prediction time. The overall time is calculated as follows:

$$CT = \sum_{i=1}^{n} NI_i * [time(SIT)] \quad (18)$$

$\mathrm{CT} = \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{NI_i}$ *[time(SIT)]

Where$\mathrm{CT}$, $CT$ indicates a computational time, n$n$represents as number of images $'NI'time(SIT)$, time(SIT) denotes a time for secure image transmission. Time computed in milliseconds (ms).

**Table 1 PSNR**

| Number of images | Original Image Sizes (KB) | Peak signal to noise ratio (dB) | | |
|---|---|---|---|---|
| | | LBSSEL | Modified RRWEI-SM scheme | Discrete memristor-based logistic map with deep neural network |
| Image 1 | 15.92 | 66.54 | 52.28 | 58.02 |
| Image 2 | 16.42 | 62.11 | 55.66 | 58.58 |
| Image 3 | 24.75 | 62.55 | 50.62 | 55.66 |
| Image 4 | 22.61 | 69.04 | 58.88 | 64.04 |
| Image 5 | 10.91 | 68.13 | 57 | 65.85 |
| Image 6 | 18.15 | 65.33 | 56.08 | 60.17 |
| Image 7 | 15.50 | 56.53 | 50.98 | 53.81 |
| Image 8 | 20.55 | 58.58 | 53.32 | 55.26 |
| Image 9 | 13.81 | 64.04 | 52.71 | 57 |
| Image 10 | 12.96 | 63.02 | 53.97 | 58.30 |

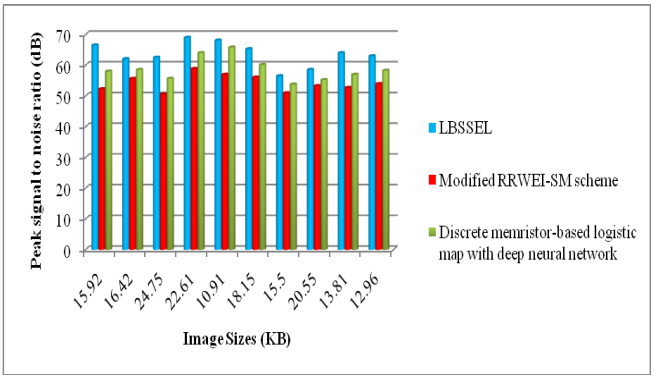


**Figure 5 graphical illustration of PSNR**

PSNR against image sizes using three different methods namely LBSSEL and existing methods [1], [2] portrayed in above Figure 5. Size of images indicated in horizontal axis and result of PSNR denoted in vertical axis. Among the three methods, the LBSSEL provides improved PSNR. For each method, various results were observed. Outcome of PSNR using LBSSEL method was higher by 17% as well as 8% than [1], [2]. An improvement achieved with Lamport One-Time Digital Signature-based cryptographic technique within an Extreme Learning Machine (ELM). MSE reduced and image excellence improved.

**Table 2 Confidentiality rate**

| Number of images | Confidentiality rate (%) | | |
|---|---|---|---|
| | LBSSEL | Modified RRWEI-SM scheme | Discrete memristor-based logistic map with deep neural network |
| 1000 | 95.1 | 89.6 | 92.3 |
| 2000 | 94.75 | 87.5 | 89.25 |
| 3000 | 95.06 | 88.5 | 90 |
| 4000 | 94.62 | 86.45 | 89.12 |
| 5000 | 95.3 | 87.3 | 91.3 |
| 6000 | 94.25 | 87.75 | 90.2 |
| 7000 | 96.5 | 89.21 | 91.78 |
| 8000 | 96.95 | 89.06 | 91.56 |
| 9000 | 95.81 | 90.27 | 92.94 |
| 10000 | 94.23 | 87.56 | 90.36 |

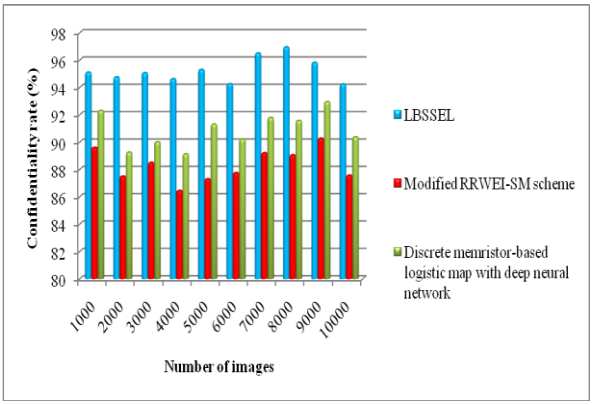


**Figure 6 graphical illustration of confidentiality rate versus number of images**

Figure 6 above depicts confidentiality rates. Contrary to conventional, results of CR higher using LBSSEL. Experiments conducted by1000 images, CR observed as 95.1% by LBSSEL, and 89.6% and 92.3% using the existing methods [1] and [2]. CR increased for LBSSEL with 8% as well as 5% than [1] [2].Improvement is achieved by the LBSSEL method utilizing the Lamport Blum ShubSigncryptive Extreme Learning. Only authorized user receives image when signature valid. Otherwise, the image is not received by the user due to an invalid signature. This helps achieve higher levels of confidentiality during image transmission.

**Table 3 integrity rate**

| Number of images | Integrity rate (%) | | |
|---|---|---|---|
| | LBSSEL | Modified RRWEI-SM scheme | Discrete memristor-based logistic map with deep neural network |
| 1000 | 94.7 | 86.5 | 91.2 |
| 2000 | 94 | 86 | 88.75 |
| 3000 | 94.83 | 88 | 89.5 |
| 4000 | 93.125 | 85 | 88.75 |
| 5000 | 94.9 | 86.3 | 90.9 |
| 6000 | 94 | 85.93 | 89.26 |
| 7000 | 95.92 | 87.5 | 90.74 |
| 8000 | 95.31 | 88.75 | 90.65 |
| 9000 | 94.66 | 89.44 | 91.73 |
| 10000 | 93.25 | 86.53 | 89.36 |

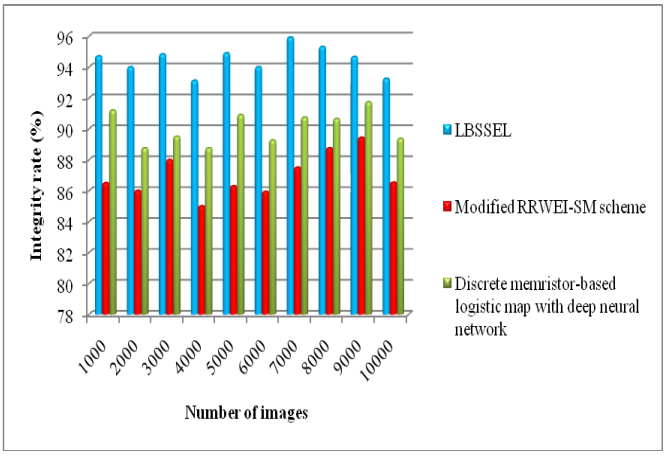


**Figure 7 Graphical illustration of integrity rate**

Figure 7 illustrates the performance outcomes of integrity rates ranging between 1000 and 10000 images taken from the dataset. To analyze data integrity, three methods are considered namely LBSSEL method and [1], [2]. Data integrity rate of LBSSEL method is notably higher when compared to [1] and [2], respectively. Let's consider the number of images to be 1000. The integrity rate of LBSSEL, [1] and [2] were observed to be 94.7%, 86.5% and 91.2%.Contrary to traditional [1], [2], integrity rate was increased by 9% and 5% using LBSSEL.This is due to the proposed LBSSEL method performing signature verification before decrypting image. Signature established, image confirmed towards received by an authorized user and is not altered by intruders, thus improving

the data integrity rate.

**Table 4 computational time**

| Number of images | Computational time (ms) | | |
|---|---|---|---|
| | LBSSEL | Modified RRWEI-SM scheme | Discrete memristor-based logistic map with deep neural network |
| 1000 | 25.3 | 30 | 28 |
| 2000 | 26.85 | 33.63 | 31.25 |
| 3000 | 30.1 | 36.45 | 33.2 |
| 4000 | 33.2 | 38.95 | 35.05 |
| 5000 | 35.78 | 43.2 | 40.12 |
| 6000 | 38.65 | 46.25 | 43.52 |
| 7000 | 40.1 | 50.02 | 45.65 |
| 8000 | 43.2 | 53.54 | 48.14 |
| 9000 | 45.8 | 55.02 | 50.12 |
| 10000 | 51.56 | 58.1 | 53.65 |

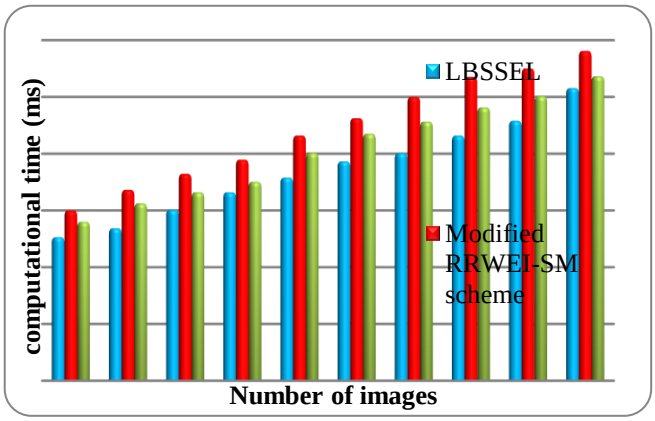


**Figure 8 graphical illustration of computational time**

Figure 8 portrays computational time. Observed performance results show that the computational time of secure image transmission for all three methods. Among three methods, the LBSSEL method reduces overall time consumption of image transmission compared to the other two methods [1], [2]. Let's consider the number of images to be 1000. The time consumption for secure image transmission using the LBSSEL method was found to be 25.3 ms, while for the other two conventional methods [1] and [2], it was found to be 30 ms and 28 ms, respectively. Computational time reduced for LBSSEL with 17% as well as 10% than conventional algorithms. It achieved by application of Extreme Learning Machine during image transmission. This helps minimize the time consumption of secured image transmission.

## 5. Summary

New LBSSEL designed with maximum safety. An Extreme Learning Machine is first designed to minimize computational time of secure image transmission. Then the proposed cryptographic method included in hidden layer of the Extreme Learning Machine. This process enhances security as authorized users receive original image. Comprehensive analysis estimated for LBSSEL as well as conventional approaches using different parameters. LBSSEL method achieves better performance in confidentiality rate, integrity rate, and minimizes computational time compared to conventional methods.

**References**

[1] LizhiXiong, Xiao Han, Ching-Nung Yang and Yun-Qing Shi, “Robust Reversible Watermarking in Encrypted Image with Secure Multi-party based on Lightweight Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology, Volume 32, Issue 1, January 2022, Pages 75-91.
**DOI:** 10.1109/TCSVT.2021.3055072

[2] B. Sakthi Kumar & R. Revathi, “An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network”, Journal of Engineering and Applied Science, Springer, volume 71, 2024, Pages 1-24.https://doi.org/10.1186/s44147-023-00349-8

[3] Mohamed Maazouz, AbdelmoughniToubal, BillelBengherbia, OussamaHouhou, Noureddine Bate, “FPGA implementation of a chaos-based image encryption algorithm”, Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 34, Issue 10, 2022, Pages 9926-9941.

https://doi.org/10.1016/j.jksuci.2021.12.022
[4] ZhenlongMana, Jinqing Li, Xiaoqiang Di, YaohuiShenga, ZefeiLiua, “Double image encryption algorithm based on neural network and chaos”, Chaos, Solitons& Fractals, Elsevier, Volume 152, 2021, Pages 1-16. https://doi.org/10.1016/j.chaos.2021.111318
[5] G. Selva Mary & S. Manoj Kumar, “Secure grayscale image communication using significant visual cryptography scheme in real time applications”, Multimedia Tools and Applications, Springer, Volume 79, 2020, Pages 10363–10382. https://doi.org/10.1007/s11042-019-7202-7
[6] Walid I. Khedr, “A new efficient and configurable image encryption structure for secure transmission”, Multimedia Tools and Applications, Springer, Volume 79, 2020, Pages 16797–16821. https://doi.org/10.1007/s11042-019-7235-y
[7] K. N. Madhusudhan, P. Sakthivel, “A secure medical image transmission algorithm based on binary bits and Arnold map”, Journal of Ambient Intelligence and Humanized Computing, Springer, Volume 12, 2021, Pages 5413–5420. https://doi.org/10.1007/s12652-020-02028-5
[8] Heping Wen, Chongfu Zhang, Ping Chen, Ruiting Chen, JiajunXu, Yunlong Liao, Zhonghao Liang, DanzeShen, Limengnan Zhou, And JuxinKe, “A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication”, IEEE Access, Volume 9, 2021, Pages 20481 – 20492. **DOI:** 10.1109/ACCESS.2021.3054952
[9] Ahmad Pourjabbar Kari, Ahmad HabibizadNavin, Amir MassoudBidgoli, MirkamalMirnia, “A new image encryption scheme based on hybrid chaotic maps”, Multimedia Tools and Applications, Springer, Volume 80, 2021, Pages 2753–2772. https://doi.org/10.1007/s11042-020-09648-1
[10] Dani Elias Mfungo, Xianping Fu, Yongjin Xian and Xingyuan Wang School of Information Science and Technology, Dalian Maritime U. “A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information”, Applied Sciences, Volume 13, Issue 12, 2023, Pages 1-25. https://doi.org/10.3390/app13127113
[11] Yaohui Sheng, Jinqing Li, Xiaoqiang Di, Xusheng Li and RuiXu, “An Image Encryption Algorithm Based on Complex Network Scrambling and Multi-Directional Diffusion”, Entropy Volume 24, Issue 9, 2022, Pages 1-23. https://doi.org/10.3390/e24091247
[12] Zhang Shuo, HouPijun, Cheng Yongguang, Bin Wang, “A visually secure image encryption method based on semi-tensor product compressed sensing and IWT-HD-SVD embedding”, Heliyon, Elsevier, Volume 9, Issue 12, 2023, pages 1-23. https://doi.org/10.1016/j.heliyon.2023.e22548
[13] Heping Wen, Yiting Lin, Shenghao Kang, Xiangyu Zhang, and Kun Zou, “Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion”, iScience, Elsevier, Volume 27, Issue 1, 2024, Pages 1-25. https://doi.org/10.1016/j.isci.2023.108610
[14] Ruifeng Han, “A Hash-Based Fast Image Encryption Algorithm”, Wireless Communications and Mobile Computing, Hindawi, Volume 2022, August 2022, Pages 1-8. https://doi.org/10.1155/2022/3173995
[15] YazeedYasinGhadi, Suliman A. Alsuhibany, Jawad Ahmad, Harish Kumar, WadiiBoulila, Mohammed Alsaedi, Khyber Khan, and Shahzad A. Bhatti, “Multi-Chaos-Based Lightweight Image Encryption-Compression for Secure Occupancy Monitoring”, Journal of Healthcare Engineering, Hindawi, Volume 2022, November 2022, Pages 1-14. https://doi.org/10.1155/2022/7745132