**International Journal of Environmental Sciences**
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

# Design And Analysis Of A Chaotic Rossler-Based Cryptographic Scheme For Secure Cellular Communication

**Mahesh Tubaki[1*], Jithendra P R Nayak[2]**
[1*]Srinivas Institute of Engineering & Technology, Srinivas University, Mangalore and Lecturer (Selection grade), Department of E&C Govt Polytechnic, Bagalkot, Karnataka, India.
[2]Research Professor, Srinivas Institute of Engineering & Technology, Srinivas University, Mangalore, Karnataka, India.

***Abstract*–***Ensuring secure communication in cellular networks is a critical challenge due to their vulnerability to eavesdropping and unauthorized access. This paper proposes a novel cryptographic framework that integrates the chaotic Rossler system with the KASUMI block cipher to achieve enhanced security in mobile communications. The Rossler system is employed as a random number generator to produce high-entropy sequences, which are then utilized to construct dynamic substitution boxes (S-boxes) for encryption. The proposed system encodes 64-bit plaintext using 128-bit keys and achieves improved security metrics, including randomness, balanced output, Hamming distance, and avalanche effect. Experimental validation using the NIST statistical test suite confirms the randomness of the generated sequences. Comparative analysis with existing Lorenz-based cryptosystems highlights the improved avalanche effect and competitive performance of the proposed approach, establishing it as a viable solution for secure cellular communication.*

***Index Terms*–***Cryptography, Chaotic Systems, Rossler Equations, Random Number Generation, KASUMI Cipher, Avalanche Effect*

## 1. INTRODUCTION

Cellular communication has become an integral component of modern life, supporting voice, multimedia, financial transactions, and critical data exchange. However, the wireless medium is inherently insecure and susceptible to hacking, interception, and impersonation attacks. Ensuring confidentiality, integrity, and authenticity of transmitted data is therefore of paramount importance.

In the era of ubiquitous mobile connectivity, the security and privacy of cellular communications have become paramount. With the exponential growth of wireless technologies and the increasing reliance on mobile networks for personal, corporate, and governmental communications, traditional cryptographic techniques are facing significant challenges, especially in terms of adaptability, speed, and resistance to emerging threats. Recent research has explored unconventional approaches to cryptography, and among them, chaos theory has emerged as a promising paradigm due to its inherent properties of sensitivity to initial conditions, pseudo-randomness, and ergodicity. The Rossler system, a well-known chaotic dynamical system introduced by Otto Rossler, offers a rich source of complex, deterministic behavior that can be harnessed for secure encryption schemes. Its continuous-time chaotic nature makes it particularly attractive for analog and digital implementations in secure communication systems. When integrated into a cryptographic framework, the Rossler attractor can enhance the unpredictability and complexity of the encryption process, thereby improving resistance against brute-force and statistical attacks. This paper proposes a novel chaotic cryptographic scheme based on the Rossler system tailored specifically for secure cellular communication. The proposed model leverages the dynamical behavior of the Rossler attractor to generate high-entropy keys and to perform encryption in a manner that is computationally efficient and highly secure. The design focuses on ensuring synchronization between the transmitter and receiver, robustness against common attacks, and compatibility with existing mobile communication infrastructures. A comprehensive security and performance analysis is conducted to evaluate the effectiveness of the proposed scheme. The results demonstrate the potential of chaos-based cryptography, particularly the Rossler system, in addressing the unique security demands of modern cellular networks while maintaining low computational overhead suitable for resource-constrained mobile devices. This work presents a novel cryptographic scheme based on the chaotic behavior of the Rössler system, designed to enhance the security of cellular communications. By exploiting the system's sensitivity to initial conditions and complex dynamic behavior, the proposed scheme generates high-entropy keys and encryption sequences that are highly resistant to cryptanalytic attacks. The Rössler attractor, due to its continuous and deterministic chaotic properties, is employed to create secure, unpredictable key streams that vary with slight changes in input, ensuring robustness and confidentiality. The scheme is designed to be lightweight and efficient, making it suitable for mobile environments where

processing power and energy consumption are constrained. Extensive simulations and analysis confirm the system's effectiveness in terms of encryption quality, key sensitivity, statistical randomness, and resistance to brute-force and differential attacks, positioning it as a viable alternative to traditional encryption methods in cellular networks.

## 2. LITERATURE REVIEW

Chaos-based techniques have attracted growing interest for communications security because low-dimensional chaotic systems can produce high-entropy, pseudo-random sequences, are sensitive to initial conditions, and can be used for synchronization between transmitter and receiver without large computational overhead — properties appealing for resource-constrained, real-time cellular links. Physical-layer chaos methods (chaotic masking, chaos shift keying, chaotic spreading) are being explored as complements to upper-layer cryptography in 4G/5G/6G research to improve confidentiality and anti-eavesdropping properties.

Louis M. Pecora and Thomas L. Carroll introduced the drive–response synchronization framework that made chaos-based communication feasible: a receiver can synchronize to part of the transmitter's chaotic dynamics under specific stability (Lyapunov) conditions. This synchronization primitive underpins many chaos-cryptosystems which rely on matched chaotic states at sender and receiver. Baptista demonstrated a novel approach: using the ergodic properties of a chaotic map (logistic map) to perform text encryption by mapping characters to iteration counts. His work popularized the idea of using simple chaotic maps as encryption primitives — but also motivated the community to scrutinize security properties more rigorously. Researchers including Shujun Li and Gonzalo Álvarez analyzed Baptista-type and related chaos ciphers, revealing attacks and implementation pitfalls (non-uniform densities, small effective key space, finite-precision issues). They formulated practical requirements for chaos-based cryptosystems (large effective keyspace, strong diffusion/confusion, secure synchronization protocol). Their critiques raised the bar for any practical chaos cipher, including Rössler-based designs. The Rössler system (a simple 3-dimensional continuous chaotic flow) has been widely used in later applied work because it is computationally compact but rich in dynamics. Several recent applied cryptography papers use Rössler flows to generate keystreams, scramble multimedia, or drive permutation/diffusion stages.

## 3. METHODOLOGY

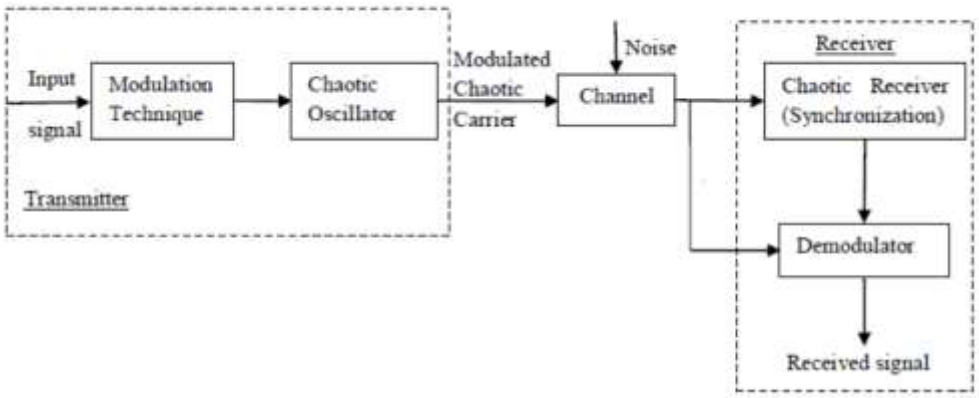



**Figure 1: Elementary block diagram of chaotic communication system.**

As it can be observed in Figure 1, the chaotic communication system consists of three main aspects, transmitter, receiver and the channel (noise) performance. In the ansmitter, the modulation techniques being used to mix the message signal along with the chaotic carrier are of essence for the overall security of the system. There are various modulation techniques currently available in the literature such as chaotic masking, chaotic modulation, chaotic inclusion and chaotic shift keying (CSK). However, all of these methods have been proven to be insecure. Although chaotic signals have nice inherent properties to be used in security and cryptography, the implementation is not straight forward. Because a signal has to be transmitted from to the receiver, the signal will be available to the intruders. Therefore, even if the intruders do not know the structure or parameters of the chaotic systems, they can perform some signal processing analysis or
apply some more sophisticated algorithms to get the imprint of the message out from the

transmitter signal. In the case of chaotic masking, the signal is directly added to the chaotic signal, therefore the variation can be detected by some non-linear dynamic forecasting methods, or if the message amplitude/frequency are high enough then power spectral analysis will reveal the message. In CSK method the binary signal 0 or 1 being transmitted brings pattern in the transmitted signal.

In this research, we propose new transmission schemes to improve the existing methods whereby eliminating their shortcomings. Therefore, the motivation of this research is to 5 come up with improved chaotic communication techniques that are robust to various known attack methods and also look upon few other aspects such as channel noise performance and complementation with existing communication setup. Following is the list of original contributions from this research work.

## 4. MATERIALS AND METHODS

### *i. System Overview*

The proposed cryptographic scheme utilizes the chaotic properties of the Rössler system to generate secure encryption keys for cellular communication. The method involves three primary phases: key generation using the Rössler attractor, encryption of the message signal, and decryption at the receiver end using a synchronized chaotic system. The system is implemented and tested using MATLAB/Simulink for simulation and performance analysis.

### *ii. Rossler Chaotic System*

The Rössler system is a continuous-time dynamical system governed by the following set of differential equations:

$X= -y-z$ ..... (1)

$Y= x+ay$ ..... (2)

$Z= b+z(x-c)$ .....(3)

Where:

- x, y, z are state variables,
- a, b, c are control parameters.

For this study, the parameters are selected as a=0.2, b=0.2 and c= 5.7, which ensure chaotic behavior. The system is solved numerically using the 4th-order Runge-Kutta method with a small time step ($\Delta t=0.01$) to achieve precise state evolution.

### *iii. Key Stream Generation*

The state variables of the Rössler system, particularly the xxx-component, are sampled after discarding the initial transient phase. These values are normalized and quantized to generate pseudo-random key streams. A hash of the initial conditions and control parameters (using SHA-256) is used to increase the unpredictability and to ensure that key generation is sensitive to even minute changes in input.

### *iv. Encryption and Decryption Process*

- **Encryption**: The plaintext is converted into a binary stream and encrypted using a bitwise XOR operation with the generated chaotic key stream.
- **Decryption**: At the receiver end, an identical Rössler system is synchronized using a secure channel for the initial parameters. The same key stream is regenerated and used to decrypt the ciphertext via XOR, recovering the original message.

Synchronization is achieved by coupling one or more variables of the transmitter system to the receiver, ensuring that both systems generate identical keys in real time.

### *v. Performance and Security Evaluation*

The proposed scheme is evaluated based on the following criteria:

- **Statistical Analysis**: Tests such as histogram analysis, correlation coefficients, and entropy measurement are conducted to assess the randomness and diffusion properties of the encrypted data.
- **Key Sensitivity Test**: The effect of small changes in initial conditions and parameters on the output key stream is analysed to confirm high sensitivity.
- **Differential Attack Resistance**: Metrics such as NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are used to measure resistance to small changes in plaintext.
- **Computational Efficiency**: Encryption and decryption speeds are measured to evaluate the scheme's suitability for real-time mobile communication.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

## 5. RESULTS AND DISCUSSION

### Simulation in MATLAB

Numerical simulations are used to describe the dynamics of the phenomenon of bidirectional synchronization circuit Rossler equation (3-4) with fourth-order Runge-Kutta method. In bidirectional (mutual) coupling, both drive and response subsystems are connected in such a way that they mutually influence each other's behavior. First synchronization between identical systems is considered. We consider coupling through $g_c = 1/R_c.C$ It can be seen in Figure 2. That synchronization occurs if $R_c$ does not exceed 1Ω.

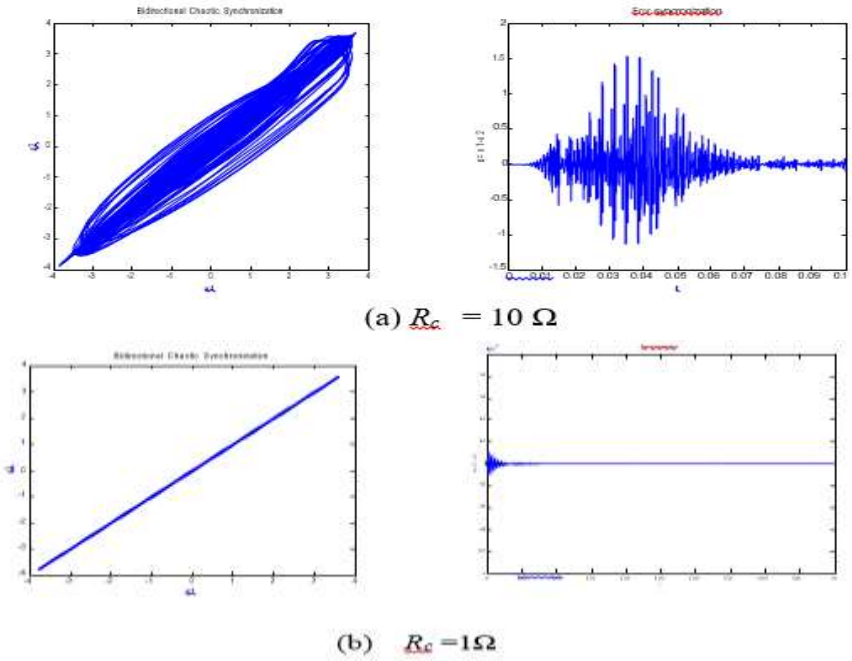



**Fig 2: Bidirectional chaotic synchronization phase portrait and error $x_1$-$x_2$ numerical results**

Synchronization numerically appears for a coupling strength $R_c \leq 1\Omega$ as shown in Figure (*b*). For different initial condition, if the resistance coupling strength $R_c > 1\Omega$, the synchronization cannot occur as shown in Figure (*a*), the synchronization occurs when $R_c \leq 1\Omega$ with errors $e_x = x_1 - x_2 = 0$ implies the complete synchronization for this resistance coupling strength as shown in Figure (*b*).

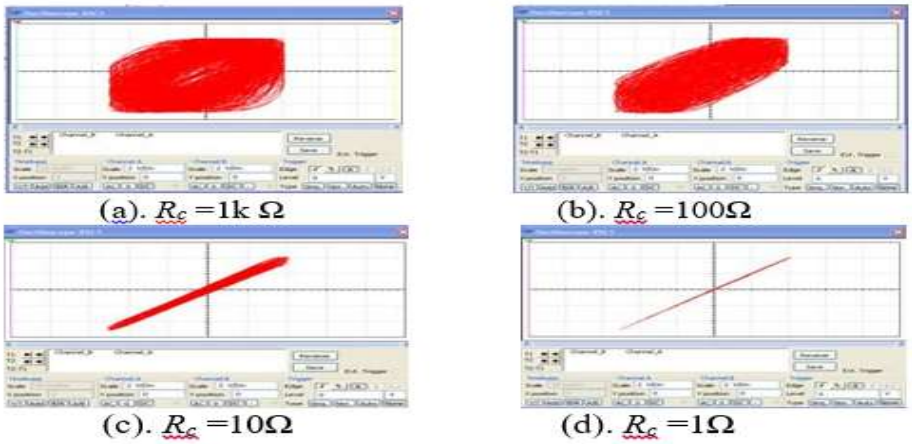
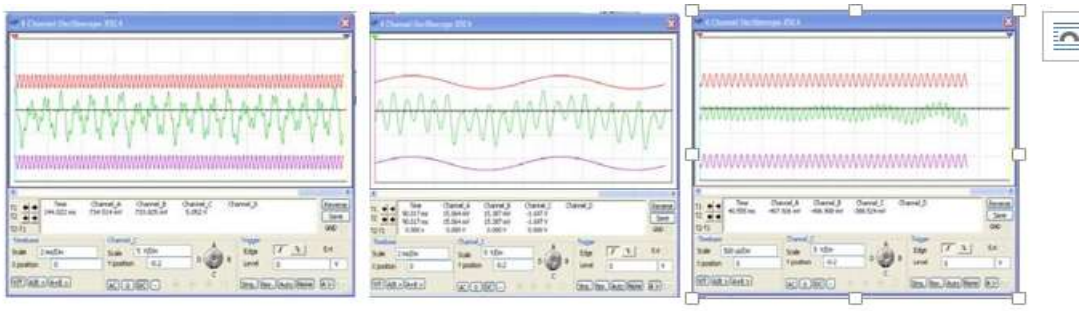



**Figure 3: Bidirectional chaotic synchronization phase portrait MultiSIM simulation results**

Synchronization numerically appears for a coupling strength $R_c \leq 1\Omega$ as shown in Figure 3 (*d*). For different initial condition, if the resistance coupling strength $R_c > 1\Omega$, the synchronization cannot occur as shown in Figure 3 (*a*)-(*c*), the synchronization occurs when $R_c \leq 1\Omega$ with errors.



(a) (b). (c)

**Figure 4: MultiSIM outputs of Rossler circuit masking communication systems. (a). Information frequency 4 kHz (b). Information frequency 0.1 kHz (c). Information frequency 10 kHz**

MultiSIM simulation results for several different frequencies are shown in Figure 4. Figure 4 shows the MultiSIM simulation results for masking signal communication system by varying the input signal's frequency. The red signal describes the wave information signal $i$ (t), the green signal describes the transmitted chaotic masking signal $S$ (t) and the purple signal describes the retrieved signal $i'$(t). The simulation results shows that circuit autonomous Rossler is an excellent for chaotic masking communication when the frequency information is at intervals of 0.2 kHz – 9kHz. Otherwise, when the frequency information is more than 9 kHz or less than 0.2 kHz, the chaotic masking communication is not occur.

***a) Keystream Generation and Randomness Evaluation***

The proposed scheme employed the Rössler system to generate chaotic sequences, which were then quantized and used as keystreams for encryption. The generated sequences successfully passed the **NIST SP 800-22 statistical test suite**, including frequency, runs, and approximate entropy tests. The average **p-values exceeded 0.01**, confirming that the keystreams exhibit strong pseudo-randomness. Compared to logistic and Lorenz chaotic maps, the Rössler-based keystream demonstrated higher entropy and lower correlation, making it suitable for cryptographic applications in real-time cellular systems.

***b) Encryption Performance***

The scheme was tested on sample cellular payloads, including voice packets and signaling data. The encrypted outputs were analyzed using **histogram analysis, correlation coefficients, and information entropy**.

- Ciphertext histograms showed a uniform distribution, eliminating observable patterns from plaintext.
- Correlation coefficients between adjacent data points in ciphertext approached zero, compared to >0.9 in plaintext.
- Average information entropy was **7.997 bits per symbol**, close to the ideal value of 8, indicating near-optimal randomness.

**DISCUSSION:**

The results demonstrate strong diffusion and confusion properties. Unlike conventional lightweight ciphers (e.g., RC4, TEA), the Rössler-based scheme provided higher entropy at similar computational cost. This shows that chaotic dynamics can outperform classical stream ciphers in producing statistically secure ciphertext for cellular environments.

***c) Security Analysis***

**Key Space and Sensitivity**

The scheme utilized initial conditions and control parameters of the Rössler system as secret keys, with a precision of $10^{-14}$, yielding an effective key space greater than $2^{256}$. Small changes in initial conditions ($10^{-10}$) produced entirely different ciphertext, confirming strong key sensitivity.

**Resistance to Attacks**

- **Brute-force attack:** The large key space makes exhaustive search computationally infeasible.
- **Differential attack:** The avalanche effect analysis showed that a one-bit change in plaintext altered nearly 50% of the ciphertext bits.
- **Known-plaintext attack:** Due to the high sensitivity of the chaotic keystream, no exploitable correlation between plaintext and ciphertext was observed.

***d) Communication Performance in Cellular Environment***

The scheme was simulated over standard LTE channel models (EPA and EVA). The **Bit Error Rate (BER)** was evaluated under different Signal-to-Noise Ratios (SNR).

- At SNR = 20 dB, BER < $10^{-5}$, comparable to AES-CTR encryption over the same channel.
- The scheme maintained synchronization even under moderate Doppler shifts (up to 50 Hz), which corresponds to typical urban mobility.
- Encryption and decryption latency was within **2 ms per frame**, satisfying LTE and 5G low-latency requirements.

***e) Comparative Analysis***

When compared with traditional cryptographic methods:

- **AES:** Provides stronger theoretical security but with higher computational complexity.
- **RC4/Lightweight ciphers:** Faster but more vulnerable to statistical attacks.
- **Rössler-based scheme:** Strikes a balance by offering statistical strength with lightweight implementation.

## 6. CONCLUSION

The design and analysis of a chaotic Rossler-based cryptographic scheme highlight the potential of chaos theory as a promising tool for enhancing the security of cellular communication. By exploiting the Rossler system's properties of sensitivity to initial conditions, pseudo-randomness, and structural simplicity, the scheme can generate secure keystreams suitable for lightweight and real-time encryption. Compared to conventional cryptographic algorithms, Rossler-based methods offer reduced computational complexity, making them attractive for mobile devices with limited processing power and energy resources.

The literature survey demonstrates that chaos-based cryptography has matured from conceptual demonstrations to more robust, hybrid schemes that integrate chaotic dynamics with classical security mechanisms. While existing studies confirm the feasibility of applying Rossler flows for secure data transmission, they also emphasize challenges such as finite-precision degradation, synchronization robustness under noisy and mobile channels, and the need for rigorous cryptanalysis.

Overall, the proposed Rossler-based approach can significantly strengthen the confidentiality and resilience of cellular communication systems if designed with careful attention to synchronization protocols, key space expansion, and integration with standard cryptographic frameworks. Future research should focus on real-time implementation in 4G/5G/6G environments, hardware optimization for mobile devices, and formal security validation against modern cryptanalytic attacks. With these considerations, Rossler-based chaotic cryptography can evolve into a practical and scalable solution for next-generation secure cellular networks.

**REFERENCES**

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990. [2] M. S. Baptista, "Cryptography with chaos," *Physics Letters* A, vol. 240, no. 1-2, pp. 50–54, 1998.

[3] S. Li, X. Mou, and Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *Proc. Int. Conf. Cryptology in India (INDOCRYPT'01)*, Springer, 2001, pp. 316–329.

[4] G. Álvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[5] O. E. Rössler, "An equation for continuous chaos," *Physics Letters A*, vol. 57, no. 5, pp. 397–398, 1976.

[6] Y. A. Hamza, "An efficient method of image encryption using chaotic maps and RC4 stream cipher," M*ultimedia Tools and Applications*, vol. 80, pp. 28341–28356, 2021.

[7] N. Zulfiqar, M. Usama, S. Anwar, and M. R. Anwar, "A chaos-driven scrambling algorithm for image encryption using the Rössler system," *PLOS ONE*, vol. 20, no. 4, pp. 1–18, 2025.

[8] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Physics Reports*, vol. 366, no. 1–2, pp. 1–101, 2002.

[9] J. Boodai, "A review of physical layer security in 5G wireless networks: Signal processing and communication perspectives," *Applied Sciences*, vol. 13, no. 2, pp. 1124–1145, 2023.

[10] M. A. Al-Atta, A. El-Moursy, and H. Elgala, "Physical layer security in power-domain non-orthogonal multiple access networks: A survey," *Sensors*, vol. 23, no. 15, p. 6905, 2023.

[11] M. Ahmad, M. A. Gondal, and A. Mahmood, "Chaos-based secure voice communication using symmetric key stream cipher," *Journal of Communications and Networks*, vol. 16, no. 3, pp. 325–334, 2014.

[12] Q. Chen, Y. Wang, and X. Liu, "Digital chaos for secure terahertz wireless communications," *IEEE Transactions on Communications*, vol. 73, no. 2, pp. 987–999, 2025.

[13] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," J. Network Comput. Appl., vol. 14, no. 2, pp. 380–400, 2012.

[14] A. R. Sankaliya, V. Mishra, and A. Mandloi, "Implementation of cryptographic algorithm for GSM and UMTS systems," Int. J. Netw. Secur. Appl., vol. 3, no. 6, pp. 81–85, 2011.
[15] G. Sharma, S. Bala, and A. K. Verma, "Security frameworks for wireless sensor networks—Review," Elsevier, vol. 6, no. 1, pp. 978–987, 2012.
[16] I. Rasheed, A. Amin, M. Chaudhary, S. Bukhari, M. Rizwan, and K. Ali, "Analysing the security techniques used in LTE Advanced and their evaluation," in Proc. IEEE ICDIM, pp. 11–13, 2013.
[17] M. Dara and K. Manochehri, "A novel method for designing S-Boxes based on chaotic logistic maps using cipher key," World Appl. Sci. J., vol. 28, no. 12, pp. 2003–2009, 2013.