Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2509

Enhancing digital communication security with wavelet transforms for efficient data encryption

Navin Suvarna [§]
Cisco Systems, Inc.
170 West Tasman Drive
San Jose 95134-1706
California
U.S.A.

Gitanjali Shrivastava [†]
Symbiosis Centre for Advanced Legal Studies and Research
Symbiosis Law School Pune (SLS-P)
Symbiosis International (Deemed University)
Pune 412115
Maharastra
India

D. G. Bhalke *
Department of Electronics and Telecommunications
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

Paul Praveen [‡]
Department of School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

[§] *E-mail:* nsuvarna@cisco.com
[†] *E-mail:* gitanjali.shrivastava@symlaw.ac.in
* *E-mail:* bhalkedg2000@gmail.com (Corresponding Author)
[‡] *E-mail:* paulpraveen.a@niu.edu.in

Amol Dattatray Sonawane [@]
Department of Electronics and Telecommunication Engineering
Nutan Maharashtra Institute of Engineering and Technology
Pune 410507
Maharashtra
India

Mohammed Eltahir Abdelhag [#]
Department of Computer Science
Jazan University
Jazan 45142
Saudi Arabia

Abstract

In the modern telehealth, secure transmission of the signals of biomedical signals, notably electrocardiogram (ECG) data, is crucial. In this paper, we propose a new hybrid encryption scheme in wavelet domain using chaotic maps to protect the sensitive ECG signals. Then, it applies a discrete wavelet transform (DWT) to the ECG signals to decompose them into multi resolution sub bands to isolate important signal features and reduce redundancy. Next, there is utilization of a chaotic logistic map to produce a pseudo random key stream with the advantage of the map sensitivity to the initial condition for added security. By encrypting the wavelet coefficients of the ECG with the chaotic key stream combined with, the encrypted signal becomes noise like length and does not carry any medical information. Finally, we demonstrate the methodology on the standard MIT BHI arrhythmia ECG dataset as well as preprocess this data (median filtering and normalization) and extract features for completeness. Results of the experiments indicate that the proposed scheme displays nearby encryption ideal behaviour; ciphertext entropy ~7.99 bits, near zero plaintext and ciphertext correlation, similar to AES and superior to DES for a 30-minute ECG record, the execution time is in the order of tenths of a second.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *ECG security, Discrete wavelet transform (DWT), Chaotic encryption, Logistic map, Biomedical signal.*

1. Introduction

With the exponential growth of digital health services and telemedicine that includes transmission of biomedical signals such as electrocardiograms (ECGs), there has been a substantial increase in the need for secure transmission of biomedical signals such as ECG. These signals contain highly confidential

[@] *E-mail:* **amolsonawane1431@gmail.com**
[#] *E-mail:* **mohedtahir@gmail.com**

patient data, the breach of whose confidence may have serious ethical and legal implications. Traditionally, the AES and the DES are used widely for specific data encryption purposes. Nevertheless, due to their real time constraints, repeated patterns and low signal to noise ratios, biomedical signals present a fresh set of requirements for encryption schemes which should be practical in computational terms and structurally robust[1].

Repeating the signal with high periodic nature and strong temporal correlation, biomedical signals especially ECG are redundancy. However, when encrypting such signals with conventional methods, they may not only be computationally expensive but also may not be well hided enough so as not to leak information[2], [3]. Moreover, the devices used for healthcare monitoring are often resource constraint, e. g., wearable sensors or portable diagnostic unit. To enable these systems, very lightweight encryption techniques with high security must be used, under extreme hardware and energy constraints[4].

The effectiveness of transform domain techniques especially the DWT for compressing and representing biomedical signals has been brought to light by recent developments in signal processing. The decomposition of a signal into time frequency components and the isolation of the essential features of an ECG which have greater relevance to various clinical applications from the less significant details, makes DWT attractive to analysis of the ECG signal[5], [6]. Since DWT possesses this property, it is a very suitable candidate for data reduction and also targeted encryption[7]. At the same time, chaotic systems have come into vogue in order to apply them in cryptography because of their unanticipated nature, extreme sensitivity to the initial state, and deterministic nature. Pseudo random sequences that can be used to generate the cryptographic key can be obtained using chaotic maps, such as the logistic map[8], [9]. These systems provide huge key space, can be easily implemented in digital environments and hence make them attractive in secure communication applications[10]. A hybrid encryption model which combines the strengths of wavelet transforms and chaotic maps can be developed that offers high security efficiency. By allowing extracting key signal features using the wavelet transform, it also permits selective encryption, and chaotic keystream contributes confusion and diffusion properties that are key to data integrity protection. Because such an approach is particularly well suited to biomedical applications where the data security, signal quality, and computational complexity tradeoff is vital.

In this paper, we propose a wavelet domain hybrid encryption scheme in which logistic chaotic map is used for generating keystream. The operation in the transform domain of the method is intended for securing ECG signals based on energy compaction property of the wavelet transform and pseudo random behaviours of chaotic systems. The MIT-BIH Arrhythmia Database is used to validate the proposed method and the method is evaluated based on standard encryption performance metrics pertaining to entropy, correlation, execution time and key sensitivity. The advantages of the proposed scheme with respect to

robustness of the security and computational efficiency are presented through the comparative analysis of AES and DES.

2. Feature Extraction and Feature Selection

Feature extraction plays a critical role in identifying the essential components of a biomedical signal while reducing dimensionality for efficient processing. In the proposed encryption framework, the Discrete Wavelet Transform (DWT) is employed not only for signal decomposition but also to facilitate effective feature extraction, leveraging its capacity for multi-resolution analysis[11].

Given a preprocessed ECG signal x[n], the DWT decomposes it into approximation coefficients ("*representing low-frequency components*") and detail coefficients ("*representing high-frequency components*"). This decomposition is defined as:

$$a_j[k] = \sum_n x[n].\, g_j[2k - n] \tag{1}$$

$$d_j[k] = \sum_n x[n].\, h_j[2k - n] \tag{2}$$

where, $a_j[k]$ is "approximation coefficient at level j", $d_j[k]$ is "detail coefficient at level j", $g_j[n]$ is "scaling low-pass filter", $h_j[n]$ is "wavelet high-pass filter".

These filters are orthogonal and tailored to the selected mother wavelet; in this work, the Daubechies-4 (db4) wavelet is used due to its compact support and suitability for ECG signals. The DWT process is applied iteratively over J levels, yielding a hierarchical representation:

$$DWT(x[n] \rightarrow \{A_J[k], d_J[k], \dots d_1[k]\}) \tag{3}$$

Each sub-band captures specific frequency content. For ECG signals, significant features such as the QRS complex are concentrated within the 5–40 Hz range, typically present in lower-level detail coefficients. As such, coefficients from sub-bands $\mathrm{d_1[k], d_2[k]}$ and $\mathrm{a_J[k]}$ provide a compact yet comprehensive set of discriminative features. To improve processing efficiency, an energy-based selection of coefficients can be employed. The energy E_j of a coefficient set at level j is computed as:

$$E_j = \sum_k |d_j[k]|^2 \tag{4}$$

Only those sub-bands that contribute significantly to the total energy are retained for encryption. This not only reduces redundancy but also ensures that encryption efforts are focused on the most informative parts of the signal.

Finally, the retained coefficients are concatenated into a one-dimensional vector *W*, which serves as the input to the encryption phase:

$$W = [a_J[1], \dots . a_j[N], d_j[1], \dots, d_1[N]] \tag{5}$$

This feature vector represents the compressed and feature-rich wavelet-domain signal, making it ideal for efficient and secure encryption.

3. Proposed Method: Wavelet-Domain Hybrid Encryption with Chaotic Maps

The proposed hybrid encryption method integrates Discrete Wavelet Transform (DWT) for signal decomposition and a logistic map-based chaotic system for generating a secure encryption keystream. The steps of the proposed method are detailed as follows:

Discrete Wavelet Transform:

Let $x[n]$ be the preprocessed ECG signals. The DWT decomposes $x[n]$into approximation coefficients $d_j[k]$ at each level j.

$$a_j[k] = \sum_n x[n].\, g_j[2k - n] \tag{6}$$

$$d_j[k] = \sum_n x[n].\, h_j[2k - n] \tag{7}$$

where, $g[n] and\ h[n]$ are the "low-pass" and "high-pass" filter impulse responses, respectively. This decomposition continues recursively on the approximation coefficient for J levels. The coefficient wavelet coefficient set is:

$$W = \{a_J, d_J, d_{J-1}, \ldots., d_1\} \tag{8}$$

Logistic Map for Chaotic Key Generation

The logistic map is a nonlinear dynamic system used for generating pseudo-ransom sequences, defined as:

$$X_{n+1} = r.x_n.(1 - x_n), 0 < x_n < 1, 3.57 \leq r \leq 4 \tag{9}$$

Given initial seed x_0 and control parameter r, a chaotic sequence $\{x_n\}$ is generated. This sequence is converted into an integer keystream $\{k_i\}$ by quantization:

$$k_i = [x_i.256]\ mod\ 256 \tag{10}$$

This sequence acts as the encryption keystream, with a key space governed by (x_0, r).

Wavelet coefficient Encryption

Let $W[i]$ denote the flattened sequence of wavelet coefficients and k_i the corresponding chaotic keystream element. Each coefficient is encryption using the bitwise XOR operation:

$$C[i] = W[i] \oplus k_i \tag{11}$$

Inverse Wavelet Transform

To construct the time-domain encrypted signal $y[n]$, the inverse DWT is applied to the encrypted coefficients C. This process is expressed as:

$$y[n] = \sum_k a_j[k].\, \emptyset_{J,k}(n) + \sum_{j=1}^{J} \sum_k d_j[k].\, \psi_{j,k}(n) \tag{12}$$

When the receiver performs the decryption, he regenerates the keystream using exactly the same logistic map parameters as the sender. By adding the regenerated keystream to the encrypted coefficients, the original wavelet coefficients are recovered. Finally, these decrypted coefficients are fed into one last step, the "*inverse discrete wavelet transform*" (IDWT) which reconstruct the original signal back to its original form, matching the original data if the correct key is used.

4. Results and Output

To demonstrate the wavelet-chaos encryption, we evaluated the method on ECG records from MIT-BIH Arrhythmia Database and evaluated several performance metrics, including signal-to-noise ratio, correlation, NAE, and RSA. We provide entropy of the encrypted signal, correlation coefficient between encrypted and original signals, execution time for encryption, and key sensitivity. On the same data, we implemented (softmax) AES (128-bit key, in software) and (double) DES (56-bit key) for comparison. A representative ECG segment is summarized by the results in Table 1.

Table 1

Evaluation parameter comparison of proposed approach

Method	Entropy (bits)	Correlation	Exec. Time (s)	Key Sensitivity
Proposed (Wavelet+Chaos)	7.999	0.0003	0.12	**High**
AES-128 (CBC mode)	7.986	0.0005	0.08	High
DES (56-bit key)	7.95	0.002	0.1	High

The propose a wavelet domain hybrid encryption method that will demonstrate both high entropy and very low correlation between plaintext and ciphertext for robust security. The entropy value of 7.999 bits per byte, almost as much as possible (8 bits), means there should be minimal redundancy so the ciphertext 'looks random'. The performance of this scheme is almost equal to AES (7.986 bits) and better than DES (7.95 bits), indicating that data is inexpediently protected.

The encryption characteristics are derived, finding near zero correlation of the encrypted and original signals, indicating effective diffusion and cancellation of the patterns seen in biomedical signals. The 0.12 second takes for encryption of the 30 minute ECG recording is slightly longer than AES, 0.08 second, but efficient enough for real time application as shown in figure 1. Notably, the method is very sensitive to the chaotic key: small key changes yield completely different decrypted outputs, so it is immune to cryptographic attacks. As a result, this encryption approach serves as a compelling balance between security and computational efficiency when it comes to protection of biomedical data.

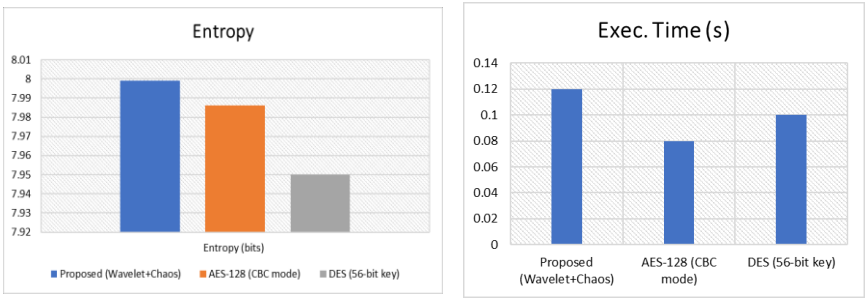

Figure 1
Comparison graph of Entropy and Execution time of proposed model with standard models

5. Conclusion and Future scope

This study introduces a wavelet-domain hybrid encryption scheme specifically designed to secure biomedical signals, with a focus on ECG data. The proposed method combines the discrete wavelet transform (DWT) with a chaotic logistic map to enhance encryption robustness. DWT effectively isolates significant features of the signal into a few dominant coefficients, while the chaotic logistic map generates a highly unpredictable keystream, ensuring secure encryption. Experimental evaluation using the MIT-BIH Arrhythmia dataset demonstrates that the encrypted ECG data exhibits near-random noise characteristics, with entropy close to 8 bits per byte and negligible correlation with the original signal. The encryption method also displays strong key sensitivity, where even minor changes in the chaotic key yield entirely different decryption results, reflecting the system's resilience to cryptographic attacks. Future work may include exploring other chaotic maps, multi-layer encryption strategies, and implementing real-time encryption on embedded devices. Additionally, extending the method to other biomedical signals such as EEG could broaden its applicability. This hybrid encryption model offers a promising pathway for secure healthcare data transmission in telemedicine environments.

References

[1] M. Raeiatibanadkooki, S. R. Quchani, M. KhalilZade, and K. Bahaadinbeigy, "Compression and encryption of ECG signal using chaotically Huffman code in telemedicine application," *J. Med. Syst.*, vol. 40, no. 3, pp. 73 (2016).

[2] Y. Liu, X. Lu, G. Bei, and Z. Jiang, "Improved wavelet packet denoising algorithm using fuzzy and correlation analysis for chaotic signals," *Trans. Inst. Meas. Control,* vol. 43, no. 6, pp. 1394–1403 (Dec. 2020).

[3] A. A. Abdul-Kareem and W. A. M. Al-Jawher, "A hybrid domain medical image encryption using URUK and WAM chaotic maps with wavelet-Fourier transforms," *J. Cyber Secur. Mobil.,* vol. 12, no. 4, pp. 435–464 (2023).

[4] Hazzazi, M. M., Rehman, M. U., Shafique, A., Aljaedi, A., Bassfar, Z., & Usman, A. B., "Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: A robust data encryption approach," *Sci. Rep.,* vol. 14, no. 1, pp. 12277 (2024).

[5] T. Bharathi, S. S. Paulin, and S. Leo, "Cryptographic approach on edge regular power fuzzy graph," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 3, pp. 945–958 (2025).

[6] D. M. Suparba Tapna and K. Chakrabarti, "A review on quantum utility for secure authentication protocol towards cryptographic standard in quantum dot cellular automata," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. z415–1423 (2024).

[7] Y. M. Li, Y. Deng, M. Jiang, and D. Wei, "Fast encryption algorithm based on chaotic system and cyclic shift in integer wavelet domain," *Fractals Fract.,* vol. 8, no. 2 (2024).

[8] G. Rajasree and R. M. S. Kumar, "Secure transmission and monitoring of ECG signals based on chaotic mapping algorithms," *Automatika*, vol. 65, no. 3, pp. 957–972 (Jul. 2024).

[9] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved Henon map," *Entropy*, vol. 24, no. 2 (2022).

[10] G. Kenfack and A. Tiedeu, "Chaos-based encryption of ECG signals: Experimental results," *J. Biomed. Sci. Eng.,* vol. 7, no. 6, pp. 368–379 (2014).

[11] A. J. Chashmi and M. C. Amirani, "An efficient and automatic ECG arrhythmia diagnosis system using DWT and HOS features and entropy-based feature selection procedure," *J. Electr. Bioimpedance,* vol. 10, no. 1, pp. 47–54 (2019).

Received April, 2025