Received: May 13, 2024. Revised: June 22, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Improving Prediction Error Expansion with Regression Using Mirror Embedding for Reversible ECG Steganography

Pramudya Tiandana Wisnu Gautama[1] **Tohari Ahmad**[1]*

[1]*Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, 60111, Indonesia*
* Corresponding author's Email: tohari@its.ac.id

Abstract: Health developments have made it easier to transfer patient information although raising concerns about data vulnerability. In such scenarios, ensuring patient data security when transmitted and stored is essential. Steganography with the Prediction Error Expansion (PEE) can be a solution for storing critical patient data in ECG signals. However, PEE has shortcomings in balancing the quality and capacity of the embedding with the threshold used. Therefore, the method's improvisation utilizes a mirror embedding scheme in PEE with a regression predictor to decrease the disparity of prediction results. To evaluate the method, the experiment used datasets from ECG MIT-BIH. The results show that the resulting ECG signal can be maintained in a manner that is as similar as possible to the original signal. The quality of the embedding results can also be maintained above 52.8 dB for SNR and below 0.252 for PRD at high bps, which is higher than that of other PEE-based or newest ECG steganographic methods. The resulting algorithm shows an increasing speed of up to 22.7 times from the existing method.

Keywords: Data hiding, Electrocardiogram, Information security, Network infrastructure, Reversible steganography.

1. Introduction

The health sector has experienced substantial growth because of the integration of technology for treating chronic diseases. In addition, healthcare professionals increasingly rely on health devices equipped with sensors that can transmit medical data, including scans, signals, and patient-specific details, to the internet. One application that relies heavily on this process is telemedicine, health services with the help of electronic communication and information technology to facilitate patients with medical personnel, such as online consultations, telehealth care, health information exchange, reporting management, and remote rehabilitation [1]. Telemedicine requires health workers to have observation and diagnostic capabilities to administer appropriate treatment. In addition, the transfer of patient information data is crucial as it could enable doctors to respond promptly. However, the availability of patient information raises deep concerns regarding data vulnerability.

One potential problem is the risk of a man-in-the-middle attack, whereby someone could acquire access to the patient's personal data and tamper with it, thus disrupting the entire remote monitoring system [2]. Patient information stored on the server/cloud requires additional security mechanisms to prevent essential data leaks, including disease history, electrocardiogram signals (ECG), Magnetic Resonance Imaging (MRI), and Computed Tomography Scan (CT scan), which can compromise patient confidentiality [3]. To safeguard patient data, incorporating mechanism like steganography, which involves entering patient data as a watermark to maintain signals, could be beneficial as an addition to the security layer.

A method that could be utilized to assess a patient's condition is ECG, whose signals can indicate the presence of various cardiovascular diseases, including stroke, heart attack, arrhythmia, and coronary artery disease. Due to its critical position in disease management and diagnosis, there have been several advancements in the healthcare sector related to ECG.

Received: May 13, 2024. Revised: June 22, 2024.

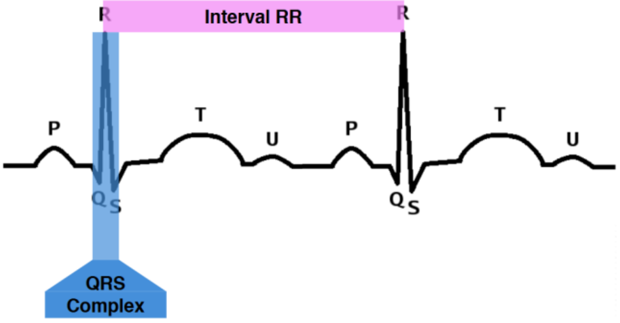

Figure. 1 ECG wave structure

The introduction of a monitoring system has made it feasible to use ECGs in hospitals, remote settings, and homes. Advances in ECG technology have given rise to mobile sensors, heart rate detection, disease diagnosis, emotion recognition, and compression methods through the implementation of the Internet of Things (IoT), mobile computing, and edge computation [4]. Steganography can be used as a method to enter important patient data into the ECG. However, ensuring the reversibility of the added watermark in the ECG is challenging.

Previous research on steganography for ECG has proposed a method that first determines the wave structure. The ECG sample interval consists of P, Q, R, S, and T waves (sometimes U also), with the R wave being the peak, as shown in Fig. 1. With certain segments playing an important role in clinical features, some research has utilized this wave, such as embedding secret data only in the TP segment [5]. Banerjee and Singh predicted modified samples in the TP segment using a long short-term memory recurrent neural network (LSTM RNN), thereby reducing the original and prediction signal errors. Another study has divided the region into QRS and non-QRS [6]. In this work, Sony et al. used the hybrid approach of combining integer wavelet transform and modified the least significant bit (IWT-mLSB) in the QRS complex area. In contrast, the technique used in non-QRS areas is pixel inverted pixel value differencing (PI-PVD).

Steganography in ECG mostly uses wavelet transformation to hide secret data. Kumar et al. researched a semi-blind scheme called ROSEmark [7]. Initially, ROSEmark decomposes the signal into segments of the same size and selects several segments for steganography. The tensed segments are then transformed using a three-level stationary wavelet transform (SWT) and discrete cosine transform (DCT). Yang and Wang employ a different transformation, like discrete wavelet transformation (DWT) [8]. Integer wavelet transform (IWT) is used with a combination of least significant bit replacement (LSB-r), coefficient alignment technique, and standard deviation blocks. When the standard deviation block is calculated before the embedding process, the data bits can be effectively included in the coefficients of IWT, increasing resistance to attack. Another similar transformation utilized by Mathivanan et al. [9] begins by converting patient data into a QR, followed by decomposition of the Daubechies four (db4) wavelet to the ECG signal. Subsequently, the coefficient of discrete wavelet transform (DWT) embeds the quick response (QR) codes from patient data in ECG signals. In addition, Mathivanan and Ganesh also proposed DWT with a pixel swapping technique to choose coefficient locations that could minimize signal degradation [10].

Khaldi et al. attempted to transform the signal into a 2D form and then implemented the fast DCT method [11]. Schur decomposition is utilized to process the coefficient results. Another approach that also performs transformations to 2D shapes using the pan-tomskin technique was proposed by Rani et al. Using a hybrid method of Multi-resolution Singular Value Decomposition (MSVD) and Contourlet Transform (ConT), the resulting steganography signal becomes more invisible and robust [12]. The main problem with the wavelet transformation approach is that the ECG used would not be fully reversible.

To guarantee reversible steganography results, Wang et al. presented a steganography technique by adding a histogram shifting approach that utilizes a local linear predictor (LLP) and prediction error expansion (PEE) [13]. In this method, the ECG signal is separated into three types of samples, each of which uses a different predictor model. LLP is used as a sample predictor with sufficient neighboring samples, and a simple average is used if the predictor does not have enough neighboring samples. Bhalerao et al. modified the capabilities of the PEE method using Artificial Neural Networks (ANN), random forest regression, and Support Vector Regression (SVR) predictors [14, 15]. In contrast to the LLP scheme, the predictors obtain predicted values from four neighboring samples, thereby dividing the ECG into two segments: the embedding sample and the tip sample (the two earliest and last samples that are not embedded). Assuming that the overall signal has a prediction error value below the threshold, the data-hiding capacity can reach 0.99 bps (bits per sample). However, the samples that can store the secrets bit can be reduced according to the existing prediction error threshold. To maximize the capacity augmentation, Gautama and Ahmad improved the schemas using looping PEE and regression predictors, making it harder for attackers to predict the value, although decreasing the overall quality [16]. Another similar method by Samudra and Ahmad on audio could minimize the contrast of the original and watermarked samples by mirroring the value [17].

In this study, the proposed method considers ECG as a cover for reversible steganography. To improve PEE performance, the regression model is used as a predictor of new sample values. Regression also presents a solution that makes it more challenging to detect predicted values compared to the simple LLP method, although it still provides speed in calculations. Existing problems in PEE where the prediction has a vast distance from the original value, can be fixed with a mirror embedding approach; hence, it can further improve the quality and capacity of data hiding. The contributions include the following: 1) the improvement of reversible ECG steganography with a PEE-mirror embedding approach and 2) the quality enhancement of the reversible steganography while preserving large capacity.

The remainder of this paper is organized into three parts. Section 2 discusses the details of the proposed technique. Section 3 demonstrates the results of the experimental analysis. Finally, section 4 provides a conclusion on the contents of the paper.

2. Proposed method

The proposed method is intended to embed larger secrets inside the ECG. Existing research [6-12] primarily utilizes various transform domain approaches. However, the transform domain makes it challenging to produce the initial ECG signal from the entire extraction results. PEE provides the option of full reversibility of the extraction signal, as shown in [13-15]. However, problems arise when the predicted values differ significantly from the original values, causing more embedding slots to be wasted, resulting in reduced capacity and quality. The last study based on looping steganography with regression has a critical downside [16]. It creates a significant difference in errors from prediction error expansion, which removes the sample plot to embed the bit data. However, this worsens the overall quality of the watermark signal. Furthermore, improvement will combine modified prediction error expansion along with mirror embedding to add further embedding slots and enhance the capacity of ECG steganography while maintaining the quality as close as the original signal. The schemes are discussed in this section.

2.1 Prediction scheme

Before processing the ECG signal, the signal is divided into two usages: machine learning training and steganography implementation. Each signal will be cut into 10-second signals and converted into integers from floating-point by multiplying by 1000. For machine learning training, the 10-second signal is separated into a group of samples consisting of five consecutive records. Records will be divided into features and targets, as in model training. For each sample, the middle sample is defined as the target, while others are included in the feature. The process is explained in Fig. 2, where A, B, C, D, and E are the consecutive samples. For data preparation, A, B, D, and E are used as features to predict the value of C. It follows the same rule as the next consecutive groups: B, C, D, E, and F.

In the steganography implementation, the 10-second signal is used for cover. This whole cover is then divided into two parts: embedded and unchanged, as illustrated in Fig. 3. The unchanged part is located in the first and last two samples in the specified cover and is responsible for four sample points. In addition, the embedded part is responsible for hiding the secrets using the PEE method with the size of $N_c - 4$ samples with N_c representing cover size. Each sample could manage at least one bit of secret data for the ideal prediction. The terms of ideal prediction are discussed in Section 2.3.

The embedding and extraction consist of three phases. Assuming that one sample saves one bit of secret data, each phase could manage for around 0.33 bps. As proposed by Bhalerao [14], the first phase will modify the values of C, F, and I.

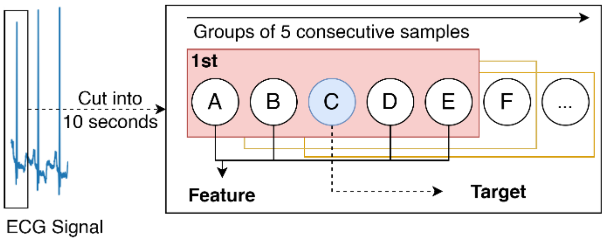

Figure. 2 Preprocessing of ECG samples to their respective groups

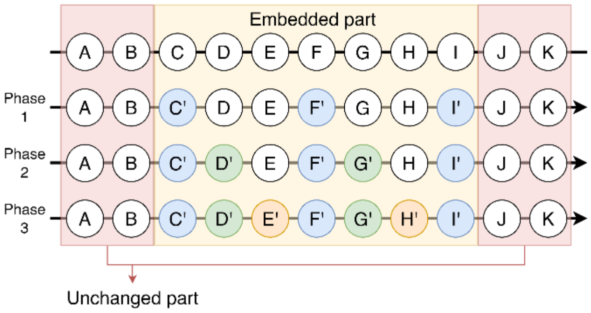

Figure. 3 Partition in the embedding phase with an example containing 11 samples

Sample C will be determined by the values of A, B, D, and E as its two nearest sample neighbors; hence, this returns watermarked sample C’. If the entire secret data is not embedded, the second phase will be initiated. In the illustration, D and G are considered the next sample that will be added to the secret bit. Watermarked sample D’ will be obtained using B, C’, E, and F’. This phase achieved a maximum of 0.66 bps. The same procedure was implemented in the last phase, obtaining an overall value of 0.99 bps.

2.2 Predictor with a regression model

The regression algorithm is a supervised learning method in machine learning that forecasts data from independent variables (feature) to analyze the relationship with the dependent variable (target). This research implements multiple types of regression models, such as ElasticNet, Bayesian Ridge, LASSO, and SGD Regressor, which are pipelined with Standard Scaler. Then, the model is trained using the prepared dataset. After training, the model will be used as a predictor for obtaining the closest value to the target sample.

2.3 Embedding stage

The proposed work starts the embedding stage after the ECG has been processed and the model has been trained. Parameters like threshold T and bit rate of payload R_p should be determined first. The other parameters used are contained in Table 1 to ease the readers’ understanding. In the usual PEE technique, the prediction error is calculated from the deviation of the prediction value obtained from the closest samples and the original. The improvement from the previous approach is the combination of the mirror embedding technique explained in [18] that is applicable to ECG signals. The process is detailed below.

Table 1. Notation list

Symbol	Description
T	Threshold
R_p	Payload rate
x_i	Original signal index i
Px_i	Prediction value of the index i
Px'_i	Prediction value of index i from extraction
e_i	Embedding error
e'_i	Extraction error
S_i	Size of the total embedding error bits
S'_i	Size of the total extraction error bits
B_i	Total bit data that can be embedded
B'_i	Total bit data that could be extracted
Pd_i	Decimal representation of the bit data
$C(M_i)$	Total available mirror for embedding
$C'(M_i)$	Total available mirror for extraction
d_i	New embedding difference
x'_i	New stego ECG index i
I_i	Hidden information of the index i

1) Begin from the index of the initial sample in the first phase of the embedding part.
2) Predict new estimation of the ECG sample and call it the predicted value Px_i . The calculation contrast between the original x_i and the predicted value Px_i is defined as error e_i, computed on Eq. (1).

$$e_i = |x_i - Px_i| \tag{1}$$

3) Next, calculate the size of the total bits, represented as S_i, that could be inserted as watermarked with Eq. (2). Here, if the size is more than 1, this is defined as the ideal prediction. If the ideal prediction cannot be achieved (or simplified by $e_i < 2$), the calculation will move to step 7 because there is no secret bit that can be embedded.

$$S_i = \lfloor log_2 \, e_i \rfloor \tag{2}$$

4) Determine the total bit data B_i that could be inserted using Eq. (3). Then, B_i bit taken from the secret data represented by $Pb(B_i)$ is converted to its decimal value with Eq. (4).

$$B_i = \begin{cases} \lceil R_p + T \rceil \; if\left(S_i \geq R_p + T\right) \\ \\ S_i \;\; if\left(S_i < R_p + T\right) \end{cases} \tag{3}$$

$$Pd_i = bin2dec\left(Pb(B_i)\right) \tag{4}$$

5) Compute the new difference $\mathrm{d_i}$ from prediction value and the mirrored value. To bring this value closer to the original value, the added secret value Pd_i is mirrored with a certain number of existing mirror points from predicted Px_i and original value x_i, notated by $C(M_i)$ with Eq. (5). The new difference $\mathrm{d_i}$ is calculated using Eq. (6).

$$C(M_i) = \left\lfloor \frac{e_i}{2^{B_i}} \right\rfloor \tag{5}$$

$$d_i = \begin{cases} 2^{B_i} \times C(M_i) + \left(2^{B_i} - Pd_i\right) mod 2^{B_i}; \\ \quad if \; C(M_i) \; is \; odd \\ \\ 2^{B_i} \times C(M_i) + Pd_i; \\ \quad if \; C(M_i) \; is \; even \end{cases} \tag{6}$$

6) Add the difference with the predicted value to obtain a new watermarked value. As in step 3, value of Px_i should not be the same as x_i; hence, $Px_i \neq x_i$. Furthermore, the new stego-ECG sample x'_i is determined by Eq. (7).

$$x'_i = \begin{cases} Px_i + d_i;\ if\ Px_i < x_i \\ Px_i - d_i;\ \ if\ Px_i > x_i \end{cases} \quad (7)$$

7) Continue the next index and apply the same step from 2 to 6 until the entire secret has been embedded.

After the overall embedding phase, multiple pieces of information should be saved because they are parameters needed for the extraction stage:

- Last sample index and phase from the embedding stage.
- Total bit data inserted from the last embedding process.
- Regression model used for embedding.
- Bit rate of payload R_p and threshold T used in the overall process.
- Hidden information representing the distance between $x_i$and the closest mirroring point is calculated by Eq. (8).

$$I_i = e_i - 2^{B_i} \times C(M_i) \quad (8)$$

2.3 Extraction stage

Data extraction is accomplished by reversing the order of the embedding process. The saved information can be retrieved as additional arguments to gather the hidden bit information. To ensure that the predictor could determine the same error, the same regression model as embedding will predict the sample. The detailed process is presented below.

1) Begin from the last phase and index of embedding part.
2) Find the error e'_i by subtracting prediction Px'_i and the watermarked value x'_i in ECG sample computed below Eq. (9).

$$e'_i = |x'_i - Px'_i| \quad (9)$$

3) Check if the extraction error has a value less than 2 (represented by $e'_i < 2$), the sample is not determined as an ideal prediction; hence, move to Step 6. If the sample is defined as an ideal prediction, similar to Eq. (2), obtain the total size of error bit S'_i that could be extracted from the sample by following Eq. (10).

$$S'_i = \lfloor log_2\, e'_i \rfloor \quad (10)$$

4) Compute the availability of the total bit data that could be taken from the sample using Eq. (11).

$$B'_i = \begin{cases} \lceil R_p + T \rceil;\ if(S'_i \geq R_p + T) \\ S'_i;\ if(S'_i < R_p + T) \end{cases} \quad (11)$$

5) Figure the total mirror points $C'(M_i)$ varied from the prediction value to the watermarked value following Eq. (12). Subsequently, reflect the extracted error based on the mirror points as closer to the predicted value. To obtain the hidden value in decimal Pd_i, use the equation represented by Eq. (13) and change it to binary.

$$C'(M_i) = \left\lfloor \frac{e'_i}{2^{B'_i}} \right\rfloor \quad (12)$$

$$Pd_i = \begin{cases} \left|e'_i - 2^{B'_i} \times \left(C'(M_i)+1\right)\right| mod\ 2^{B'_i}; \\ if\ C'(M_i)\ is\ odd \\ \left|e'_i - 2^{B'_i} \times C'(M_i)\right|; \\ if\ C'(M_i)\ is\ even \end{cases} \quad (13)$$

6) Finally, the original value x_i could be calculated by Eq. (14). The determination of the initial value can be divided into three conditions, with the initial condition being the development of the value $e'_i < 2$, which is equivalent to $Px'_i = x'_i\ or\ |x'_i - Px'_i| = 1$. The remaining conditions are determined from the comparison of greater or less than with respect to prediction Px'_i and the watermarked x'_i.

$$x_i = \begin{cases} x'_i \\ if\ Px'_i = x'_i\ or\ |x'_i - Px'_i| = 1 \\ Px'_i + \left(2^{B'_i} \times C'(M_i) + I_i\right) \\ if\ Px'_i < x'_i \\ Px'_i - \left(2^{B'_i} \times C'(M_i) + I_i\right) \\ if\ Px'_i > x'_i \end{cases} \quad (14)$$

7) Repeat the same steps from 2 to 6 with the next index until the first index of the first phase is processed.

Received: May 13, 2024. Revised: June 22, 2024.

The extraction process can be performed by constructing the whole original value to form the ECG signal. The secret data are represented by the binary value of the hidden decimal.

3. Experimental analysis

3.1 Dataset

The Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) dataset [19, 20] was used as the source for the preparation process in section 2.1. Of the 48 records, 46 ECG signals with MLII availability were processed into segments of 10 seconds each. With a frequency of 360 Hz, the total number of samples obtained was 3600. These samples were then divided for use in machine learning regression and steganography. Meanwhile, the secret data used the same key dataset as that used in the study conducted by Gautama and Ahmad [16], where the secret was randomly arranged with the total number of bits adjusted to the BPS (bits per sample) ranging from 0.08 to 0.99 bps.

3.2 Performance evaluation

As utilized in previous research, the quality of the resulting signal will be assessed with two essential metrics, namely the signal-to-noise ratio (SNR) represented by Eq. (15) and the percentage residual difference (PRD) represented by Eq. (16). The length of the existing signal is expressed by Y. Parameter x_i and y_i indicate sample points for input signal X and output signal Y, respectively, where i is the signal index.

$$SNR(X,Y) = 10 \cdot log_{10}\left(\frac{\sum_{i=1}^{N}(x_i)^2}{\sum_{i=1}^{N}(x_i - y_i)^2}\right) \quad (15)$$

$$PRD(X,Y) = \frac{\sqrt{\sum_{i=1}^{N}(x_i - y_i)^2}}{\sqrt{\sum_{i=1}^{N}(x_i)^2}} \times 100 \quad (16)$$

In executing the PEE method with mirror embedding, various parameters are manipulated to demonstrate the contrast between the original signal and the one that contains the secret payload. In the case example shown in Fig. 4, four examples of implementation using the LASSO machine learning model exist. As shown, between columns is a comparison of the payload rate and threshold, such as using payload rate 1 and threshold 0, when compared with payload rate 3 and threshold 1. The sum of the payload rate and threshold values is called the maximum available bits that could be accommodated in one sample, following Eq. (3). In the maximum available bit comparison, the biggest influence is the contrast in the amplitude of the sample points. With bps of 0.99, payload rate 1 and threshold 0 appear to have subtler differences compared with payload rate 3 and threshold 1, resulting in an SNR difference of only 9.55 dB.

Meanwhile, between rows, different BPS secret data values are shown. When compared in terms of BPS, the most obvious influence is the distribution of points, which becomes more distinguished even when the BPS value increases. This is visible when comparing graphics with payload rate 3 and threshold 1, where the original signal difference appears at almost every sample point at higher BPS. Another thing that should be mentioned is the difference in SNR and PRD values in the case of bps 0.99, payload rate 1, and threshold 0 compared with bps 0.08, payload rate 3, and threshold 1 of Fig. 4 reaches 1.2 dB and 0.023, indicating that the lower maximum available bits have a more significant influence on reducing the contrast of metric's values when facing a larger BPS.

Based on the regression models, as illustrated in Fig. 5, there is a model with the worst performance, namely ElasticNet, but its value is close to that of the other models. This worse value is caused by calculations during mirror embedding, where the ElasticNet predicted value turns out to push the mirrored value further from the original value. However, the driving mirror value is still within reasonable limits of around 2^{B_i}.

In addition, the different results from each model indicate that this method can make it difficult for attackers to determine which predictor to use. When faced with a low BPS, such as 0.08 bps, the SNR and PRD values approach 64 dB and 0.070, respectively. Even at high BPS, the SNR and PRD values can be maintained above 52.8 dB and below 0.252 for the average maximum bit samples. In addition, as the need for secret data increases, the distance between the metric values becomes smaller, which can be seen at a distance between 0.66 and 0.99 bps. Therefore, this method has the advantage of accommodating more secret data while maintaining quality.

Compared with the maximum available bit value, the SNR value can reach 67.5 dB for the lowest total number of bits, as illustrated in Fig. 6. The greater the BPS, the more this value slopes closer to 57 dB. The same graphic form as in Fig. 6 also applies to the PRD value. Increasing the value of maximum available bits decreases differences in metric quality. Therefore, at high maximum available bits, the increase in total bit value becomes insignificant.

Received: May 13, 2024. Revised: June 22, 2024.

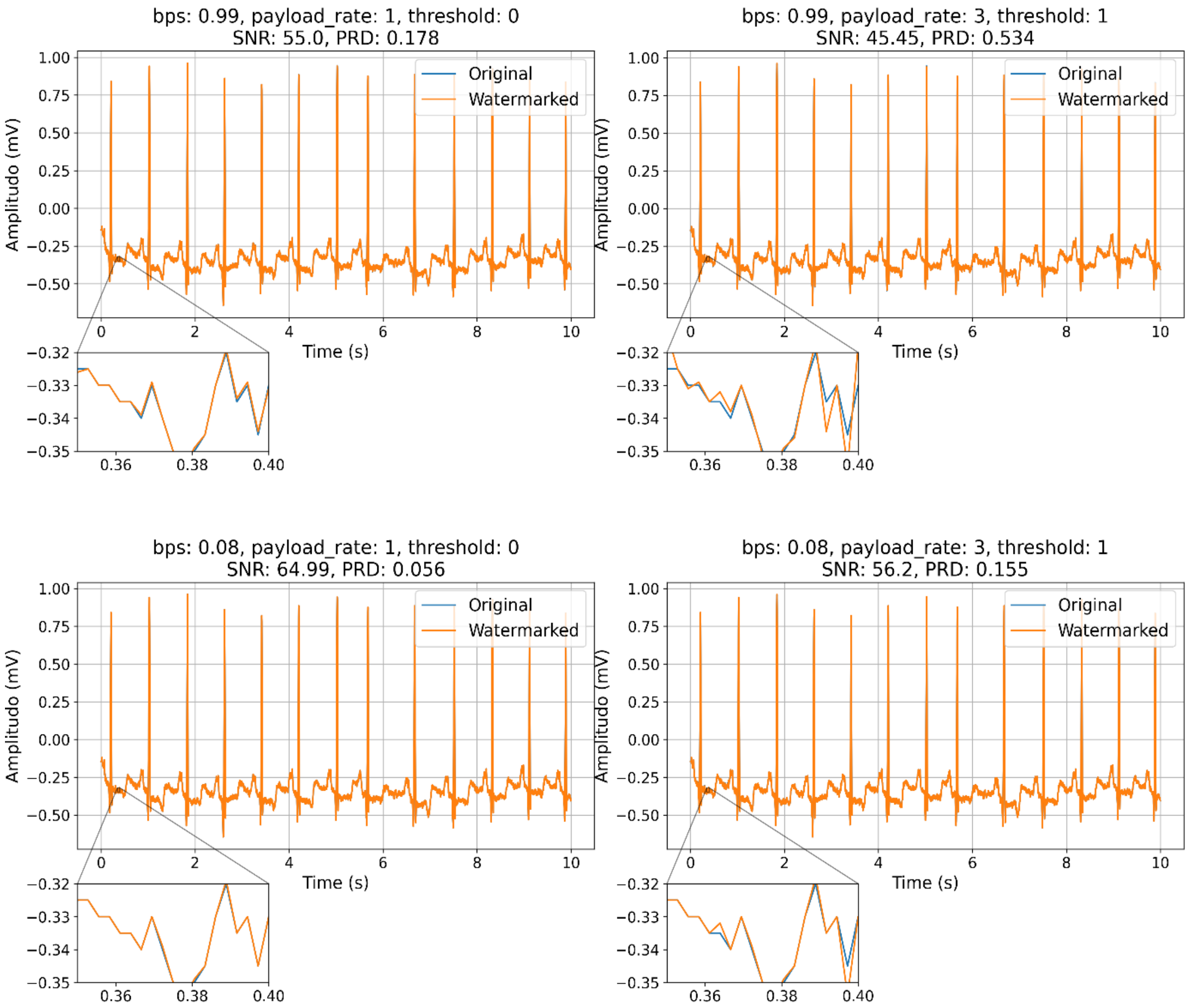

Figure. 4 Comparison of the original and watermark in multiple parameters for patient code 100 with LASSO

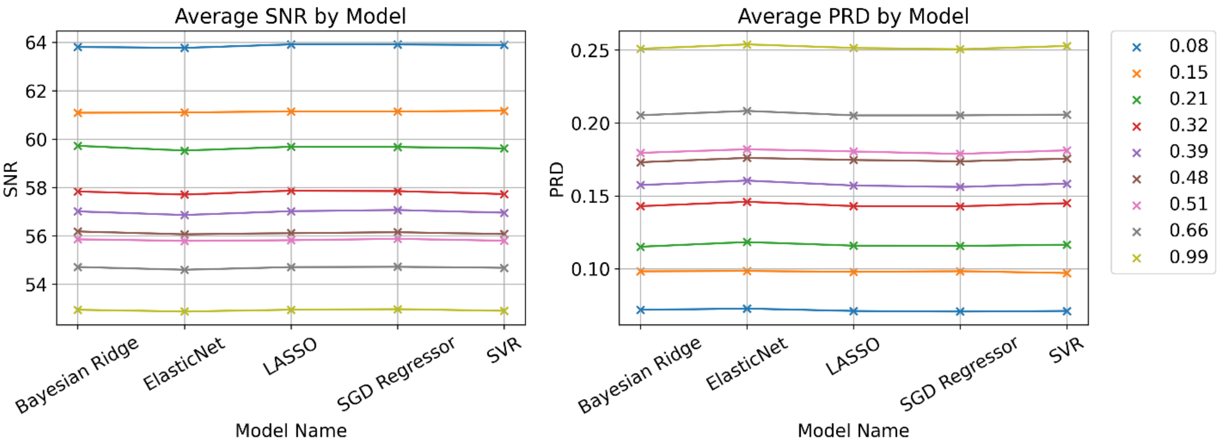

Figure. 5 Average SNR and PRD performances based on regression models

When a comparison is made with the latest transform domain method, the proposed method has the advantage of full reversibility. However, the quality can still outperform the other methods, as shown in Table 2. Even when the BPS reaches 0.99 bps, the PEE-mirror embedding method can still compete with the best PRD values. The SNR value is somewhat lower than [12] because the BPS values are very distant (contrast of 0.74 bps), but when corresponding under the same BPS conditions, the proposed technique can reach values above 60 dB.

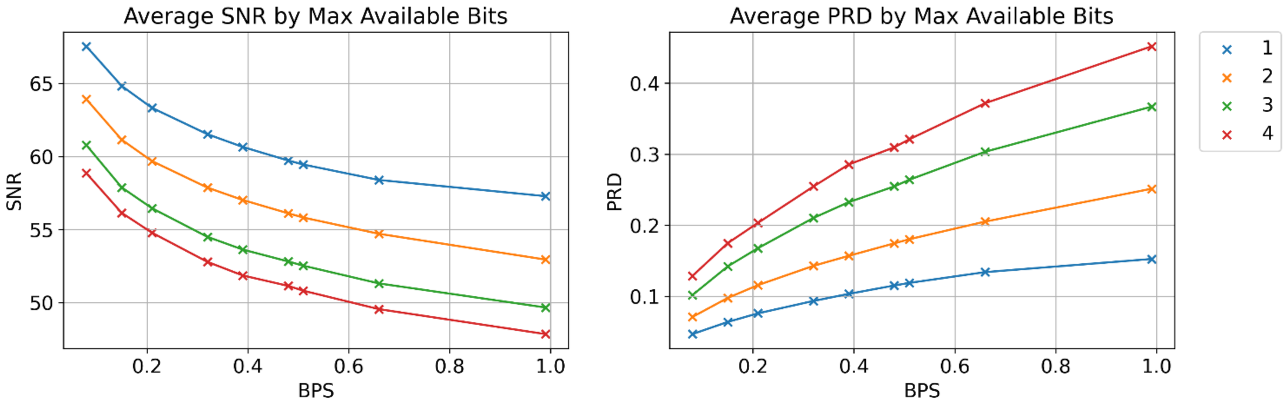

Figure. 6 Average SNR and PRD performances based on the maximum sample bits

Table 2. Comparison method with previous studies

Method	**Algorithm**	**Database**	**Payload**	**Maximum Payload (bps)**	**Metrics**	**Maximum SNR**	**Lowest PRD**	**Reversi-bility**
[13]	PEE+LLP	MIT-BIH	Binary data	0.45	PRD	-	0.528	Yes
[14]	PEE+ANN	MIT-BIH	Binary data	0.99	SNR, PRD, and NCC	30.04	3.539	Yes
[15]	PEE+SVM	MIT-BIH	Binary data	0.99	SNR, PRD, and NCC	29.98	3.5	Yes
[10]	DWT + Pixel Swapping	MIT-BIH	Image (2160 bytes)	-	SNR, PRD, and NCC	33.79	4.6	No
[11]	Fast DCT	MIT-BIH	QR Code (21904 bits)	0.082	SNR, PRD, and Bit Error Rate (BER)	48.37	0.5632	No
[12]	ConT and MSVD	MIT-BIH PTB-DB	Image (64x64)	0.25	SNR, PRD, and NCC	58.78	0.5121	No
[16]	PEE + regression with looping	MIT-BIH	Binary data	0.99	SNR, PRD, and NCC	23.83	7.184	Yes
Proposed Work	PEE+Regression +mirror embedding	MIT-BIH	Binary data	0.99	SNR, PRD	57.28	0.152	Yes

* Payload may not be the same

In addition, the experiment on this method is compared with existing PEE methods as in research [13-16]. The proposed method can display embedding quality performance values that surpass those of other methods with high bits per sample. At the highest capacity (around 0.99 bps), the SNR value can reach 57.28 dB, surpassing other methods in addition to the PRD value of approximately 0.152. In addition, the proposed method can maintain the reversibility proposed by PEE.

3.3 Time complexity

This research was carried out on the same operating system as that used in [16] with 32 GB RAM. Based on the experimental results, as shown in Table 3, ElasticNet performs slightly better than the other methods, with SVR being the worst. With an extensive training dataset, SVR requires $O(N^2)$ time from the number of samples; therefore, it impacts the

Table 3. Time comparison of different models and methods

Model	BPS										[13]	Ratio
	0.08	**0.15**	**0.21**	**0.32**	**0.39**	**0.48**	**0.51**	**0.66**	**0.99**	**Average**	**Average**	
Bayesian Ridge	0.012	0.023	0.032	0.049	0.059	0.074	0.077	0.101	0.151	0.064	1.494	23.3
ElasticNet	0.012	0.022	0.030	0.047	0.056	0.071	0.073	0.095	0.144	0.061	1.428	23.4
LASSO	0.013	0.024	0.033	0.051	0.061	0.076	0.079	0.103	0.155	0.066	1.456	22.1
SGD Regressor	0.012	0.023	0.033	0.049	0.059	0.075	0.076	0.100	0.150	0.064	1.468	22.9
SVR	0.193	0.359	0.498	0.755	0.919	1.130	1.202	1.555	2.328	0.993	21.750	21.9
Average Ratio												22.7

model size, affecting the research length. Other methods contain a way of handling large datasets so that they still produce good prediction quality. Compared with research [16], the proposed method maintains an average time performance 22.7 times better in the same environment.

4. Conclusion

This research proposes an improvisation of the Prediction Error Expansion method for ECG steganography to increase the quality value of the embedding results metrics. This method implements a regression predictor, which makes it difficult for attackers to predict the value of existing secret data. By using the mirroring technique, the difference between the original and watermarked ECG can be reduced to a minimum, thereby affecting the quality of the data hiding. In addition, the threshold is used to increase the amount of secret capacity that can be accommodated by the embedding process.

The performance results reveal a significant increase in quality. With metric calculations using SNR and PRD, the method can produce values above 52.8 dB and below 0.252 in average situations with high BPS. This value can increase to 64 dB and less than 0.070 with a low BPS compared with the existing methods. The resulting stego-ECG graph appears more dynamic and similar to the original signal. Apart from that, the mirroring method can maintain the quality as the capacity increases, as seen from the comparison of the total BPS of the secret data. In addition, the proposed method can deliver speed performance up to a ratio of 22.7 times that of the previous method.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, PTWG and TA; methodology, PTWG and TA; software, PTWG; validation, PTWG and TA; resources, TA; writing—original draft preparation, PTWG; writing—review and editing, TA; visualization, PTWG; supervision, TA; project administration, TA; funding acquisition, PTWG and TA.

Acknowledgments

The authors gratefully acknowledge support from the Institut Teknologi Sepuluh Nopember.

References

[1] A. Haleem, M. Javaid, R. P. Singh, and R. Suman, "Telemedicine for healthcare: Capabilities, features, barriers, and applications", *Sensors International*, Vol. 2, No. 100117, 2021, doi: 10.1016/j.sintl.2021.100117.

[2] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-in-the-Middle Attack Mitigation in Internet of Medical Things", *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 3, pp. 2053-2062, 2022, doi: 10.1109/TII.2021.3089462.

[3] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan, "A Survey on Healthcare Data: A Security Perspective", *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 17, No. 2s, 2021, doi: 10.1145/3422816.

[4] M. A. Serhani, H. T. El Kassabi, H. Ismail, and A. Nujum Navaz, "ECG Monitoring Systems: Review, Architecture, Processes, and Key Challenges", *Sensors*, Vol. 20, No. 6, p. 1796, 2020, doi: 10.3390/s20061796.

[5] S. Banerjee and G. K. Singh, "A new approach of ECG steganography and prediction using

deep learning", *Biomedical Signal Processing and Control*, Vol. 64, p. 102151, 2021, doi: 10.1016/j.bspc.2020.102151.

[6] N. Soni, I. Saini, and B. Singh, "An integer wavelet transform and pixel value differencing based feature specific hybrid technique for 2D ECG steganography with high payload capacity", *Multimedia Tools Application*, Vol. 80, No. 6, pp. 8505-8540, 2021, doi: 10.1007/s11042-020-09856-9.

[7] S. Kumar, A. Rajpal, N. K. Sharma, S. Rajpal, A. Nayyar, and N. Kumar, "ROSEmark: Robust semi-blind ECG watermarking scheme using SWT-DCT framework", *Digit Signal Process*, Vol. 129, p. 103648, 2022, doi: 10.1016/j.dsp.2022.103648.

[8] C.-Y. Yang and W.-F. Wang, "An efficient data hiding for ECG signals based on the integer wavelet transform and block standard deviation", *Journal of King Saud University - Computer and Information Sciences*, Vol. 34, No. 8, pp. 5868-5882, 2022, doi: 10.1016/j.jksuci.2021.08.013.

[9] P. Mathivanan, S. E. Jero, and A. B. Ganesh, "QR Code-Based Highly Secure ECG Steganography", In: *Proc. of International Conference on Intelligent Computing and Applications*, Vol. 846, Singapore: Springer, pp. 171-178, 2019, doi: 10.1007/978-981-13-2182-5_18.

[10] P. Mathivanan and A. B. Ganesh, "ECG steganography using Base64 encoding and pixel swapping technique", *Multimedia Tools and Applications*, Vol. 82, No. 10, pp. 14945-14962, 2023, doi: 10.1007/s11042-022-14072-8.

[11] A. Khaldi, M. R. Kafi, and M. S. Moad, "Wrapping based curvelet transform approach for ECG watermarking in telemedicine application", *Biomedical Signal Processing and Control*, Vol. 75, p. 103540, 2022, doi: 10.1016/j.bspc.2022.103540.

[12] J. Rani, A. Anand, and S. Shivani, "SecECG: secure data hiding approach for ECG signals in smart healthcare applications", *Multimedia Tools and Application*, Vol. 83, No. 14, pp. 42885-42905, 2023, doi: 10.1007/s11042-023-17049-3.

[13] H. Wang, W. Zhang, and N. Yu, "Protecting patient confidential information based on ECG reversible data hiding", *Multimedia Tools Appl*, Vol. 75, No. 21, pp. 13733-13747, 2016, doi: 10.1007/s11042-015-2706-2.

[14] S. Bhalerao, I. A. Ansari, A. Kumar, and D. K. Jain, "A reversible and multipurpose ECG data hiding technique for telemedicine applications", *Pattern Recognit Letters*, Vol. 125, pp. 463-473, 2019. doi: 10.1016/j.patrec.2019.06.004.

[15] S. Bhalerao, I. A. Ansari, and A. Kumar, "Performance Comparison of SVM and ANN for Reversible ECG Data Hiding", *Soft Computing: Theories and Applications*, Vol. 1154, pp. 197-207, 2022, doi: 10.1007/978-981-15-4032-5_20.

[16] P. T. W. Gautama and T. Ahmad, "Analysis of Large Capacity Reversible Data Hiding for ECG Using PEE and Regression", In: *Proc. of 2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, pp. 392-397, 2024, doi: 10.1109/GECOST60902.2024.10474608.

[17] Y. Samudra and T. Ahmad, "Mirroring-Based Data Hiding in Audio", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 5, pp. 550-558, 2021, doi: 10.22266/ijies2021.1031.48.

[18] Y. Samudra and T. Ahmad, "Improved prediction error expansion and mirroring embedded samples for enhancing reversible audio data hiding", *Heliyon*, Vol. 7, No. 11, p. e08381, 2021, doi: 10.1016/j.heliyon.2021.e08381.

[19] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database", *IEEE Engineering in Medicine & Biology Society*, Vol. 20, No. 3, pp. 45-50, 2001, doi: 10.1109/51.932724.

[20] A. Goldberger, L. Amaral, L. Glass, J. Hausdorff, P. C. Ivanov, R. Mark, J. E. Mietus, G. B. Moody, C. K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals", *Circulation*, 2000, https://physionet.org/content/mitdb/1.0.0/ (accessed Mar. 07, 2024).