Reed Solomon Coding-Based Medical Image Data Hiding Method against Salt and Pepper Noise

Mehmet Zeki Konyar 1,* and Sitki Öztürk 2,*

1 Information System Engineering Department, Kocaeli University, 41001 Kocaeli, Turkey
2 Electronics and Communication Engineering Department, Kocaeli University, 41001 Kocaeli, Turkey
* Correspondence: mzeki.konyar@kocaeli.edu.tr (M.Z.K.); sozturk@kocaeli.edu.tr (S.O.)

Received: 13 April 2020; Accepted: 19 May 2020; Published: 1 June 2020

Abstract: Medical data hiding is used to hide patient information inside medical images to protect patient privacy. Patient information in the image should be protected when sending medical images to other specialists or hospitals over the communication network. However, the images are exposed to various unwanted disruptive signals in the communication channel. One of these signals is salt and pepper noise. A pixel exposed to salt and pepper noise becomes completely black or completely white. In pixel-based data hiding methods, it is not possible to extract the secret message in the pixel exposed to this kind of noise. While current data hiding methods are good for many disruptive effects, they are weak against salt and pepper noise. For this reason, the proposed study especially focuses on the accurate extraction of patient information in the salt and pepper noisy medical images. This study was proposed for the most accurate extraction of secret message despite salt and pepper noise, by use of a Reed Solomon error control coding-based data hiding method. The most important feature of Reed Solomon codes is that they can correct errors in non-binary (decimal) numbers directly. Therefore, the Reed Solomon coding-based data hiding method that proposed in this study increases the resistance against salt and pepper noise. Experimental studies show that secret data is accurately extracted from stego images with various densities of salt and pepper noise. Stego medical images created by the proposed method have superior quality values compared to similar literature studies. Additionally, compared to similar methods, the secret message is extracted from the noisy stego image with higher accuracy.

Keywords: medical images; Reed Solomon codes; robust data hiding; secret message; salt and pepper noise

1. Introduction

With the developing technology, the availability and sharing of medical images on computer systems has increased. The availability of images on online systems provides serious convenience for both doctors and patients. However, the presence of medical images on the internet brings an important security problem. It is important to protect images containing private disease information. It is important to protect medical images containing disease information for patient privacy. In addition, many health institutions want to add information such as copyright and digital signature to medical images. Medical data hiding is one of the suggested solutions for this purpose.

Various information such as patient information, doctor comments and hospital logo can be added to the image using data hiding methods. The purpose of data hiding is to add secret information into various cover objects, such as images, videos, or sounds. It is critical that the carrier (stego) object containing secret information does not differ significantly from the original (cover) object.

The same is true for medical images. Medical images such as ultrasound (US), X-ray, magnetic resonance imaging (MRI), and computed tomography (CT) created by the imaging device are used
The general structure of data hiding in medical images is given in Figure 1. Some pre-processes are applied to the patient information that will be hidden inside the medical image. Although these pre-processes vary according to the data hiding method, there may also be security operations such as encryption, coding or scrambling. The message information formed after the pre-processing is hidden in the medical image with the data hiding algorithm. The stego image containing the secret information is sent to the receiver through the communication channel. The secret message is retrieved with the data extraction algorithm on the receiver side. If there is any pre-processes like encryption or coding, it is resolved with the post-processing, and patient information is retrieved.

**Figure 1.** General structure of data hiding in medical images.

### 1.1. Literature Review

The methods proposed for hiding data in medical images vary. From histogram-based methods [1] and [2], hide data on peaks and zeros in the histogram of images separated into non-overlapping blocks. In [3], a data hiding is proposed according to the improvement of medical images by histogram stretching and histogram equalization methods. In addition, there are studies which propose data hiding with the difference expansion of adjacent pixels [4–7]. In the medical image, some methods separate the region of interest (ROI) and region of non-interest (RONI). These methods hide data into encrypted RONI and the least significant bit (LSB) [8–10], wavelet coefficient [11,12], discrete cosine transform (DCT) coefficients [13] and dividing blocks [14].

Studies using error control coding methods for data hiding in medical images are limited. In [14], both noise reduction block and a simple error control coding named repetition codes are used. Repetition codes repeat the secret message several times. The author of [14] repeated the secret message eight times and create a new thread. The new thread was embedded in MRI images. These stego MRI images were exposed to salt and pepper noise. For the extraction of the secret message, in the first stage they removed noise with the noise reduction block. In the second stage, they extracted the thread, which included the secret message eight times. In the study [15], after the pixels in the cover object were duplicated by over-sampling, a secret message was added to the bits of the appropriate pixels. BCH coding was used as an error control method in wavelet-based hiding of [11] and [16] studies.

Reed Solomon (RS) coding, which is a common error control coding method, has been used limitedly in data hiding methods. Moreover, [17] evaluated the use of error coding methods and RS codes in data hiding. Additionally, [18] hides the message by selecting the polynomial coefficients in RS codes, with the matrix coding method which is used in various [19] data hiding applications. In study [20], which hides the codeword, it selects the place where the message will be hidden according to the base of the polynomial coefficient. The authors of [21] use the RS code to fix errors in the video file from which the hidden message was extracted. The authors of [22] hide the RS encoded
message into the image, which is divided into blocks. In [23], the cover file is made suitable for RS by sampling. The data part of the message coded with RS is added to the image and the control part is added to the region where the upper sampling is performed. The methods proposed in [22,23] have a complicated data hiding process due to the preferred data hiding algorithms and they take a lot of the processing load.

1.2. Contributions of the Proposed Work

For the vast majority of medical data hiding methods in the literature, no method against salt and pepper noise is recommended. Moreover, methods that apply salt and pepper noise to the Stego image generally yield results for 1% density noise. This does not show full resistance to salt and pepper noise. The study [14], which offers results of salt and pepper noise in different densities, is only recommended for the MRI images. Moreover, in addition to noise filtering, this study can also get good results by hiding the same secret message eight times with repetition code. Although there are studies using different error control coding for non-medical images, these encodings are binary compatible and not used in decimal numbers.

Considering the existing works, the advantages of the proposed study and its contributions to the literature are:

- Results tested for CT, MRI, US, and X-ray images, against salt and pepper noise at several densities.
- It is proposed to use more effective RS coding instead of complex data hiding algorithms to remove salt and pepper noise.
- To the best of our knowledge, this is one of the first data hiding studies of medical images-based on Reed Solomon coding.
- Since the proposed data hiding method directly hides decimal numbers, the hiding capacity per pixel is high.
- Noise-resistant spatial plane data hiding becomes more resistant to noise with the proposed method.

The rest of this paper is as follows; in Section 2, Reed Solomon encoding and decoding processes are described. The proposed method is presented in Section 3. Experimental test results are evaluated in Section 4. Section 5 contains the conclusion.

2. Reed Solomon Coding

The Reed Solomon (RS) coding [24] used in this study is the decimal class of BCH codes used for non-binary coefficients. In RS coding, the amplitude of the error varies according to the Galois field used and may be a decimal value.

RS codes are defined in the Galois field \( GF(2^m) \), where \( m \) denotes the number of bits in a symbol. The symbols for \( GF(2^m) \) are \( \{0, 1, 2, \ldots, (2^m - 1)\} \). When an information message with the symbol number \( k \) is encoded with the RS code, together with the parity symbols added, a codeword with the symbol number \( n = (2^m - 1) = k + 2t \) is obtained, and denoted by RS\((n, k)\) [25,26]. When the parity symbol length is accepted as \( 2t \), up to \( t \) incorrect symbols can be corrected in the RS\((n, k)\) code. For information with symbol length \( k \), the information polynomial is as follows:

\[
b(x) = b_{k-1}x^{k-1} + \cdots + b_1x + b_0
\]

(1)

\( b(x) \) is the element of Galois field and all \( b_i \) coefficients are created with the help of minimal polynomial systematic RS\((n, k)\) code, that can be given as in Equation (2).

\[
c(x) = b(x)x^{n-k} + p(x)
\]

(2)

\( p(x) \) denotes the parity polynomial, and refers to the \((n - k - 1)\) degrees remainder after division of \((n - k)\) times shifted information polynomial to the generator polynomial \( g(x) \).
\[ p(x) = \left[ b(x)x^{n-1} \right] \mod g(x) \]  
(3)

\[ g(x) = (x + a^1) + (x + a^2) + \ldots + (x + a^{2t}) \]  
(4)

The \((n-k)\) degree \(g(x)\) polynomial has coefficients within \(GF(2^m)\) and is fully divided by \(x^{n-1}\). The RS(n, k) codeword, which is formed as in Equation (5); the symbols are elements of \(GF(2^m)\)

\[ c = (c_{n-1}, c_{n-2}, \ldots, c_2, c_1, c_0) \]  
(5)

The \(c\) codeword is sent to the receiver from the communication channel. Subject to noise or distortion in the channel such as \(e(x)\), the new codeword is taken by the receiver as \(r(x)\) in Equation (6).

\[ r(x) = c(x) + e(x) \]  
(6)

RS decoding consists of the error detection and correction process from the data transmitted through the noisy channel. The decoding process, which is more complex than the encoding process, will be briefly summarized here. See [25] and [26] for more information. With RS decoding, the corrected codeword of \(\hat{c}(x)\) is recovered, by trying to correct the incorrect symbols in the \(r(x)\) message. To find the error in the message, the syndrome (error indicator) of the received signal is calculated first.

\[ S(a^1) = r(a^1) = e_{p1}(a^1)^{p1} + e_{p2}(a^1)^{p2} + \ldots + e_{pt}(a^1)^{pt} \]

\[ S(a^2) = r(a^2) = e_{p1}(a^2)^{p1} + e_{p2}(a^2)^{p2} + \ldots + e_{pt}(a^2)^{pt} \]

\[ S(a^{2t}) = r(a^{2t}) = e_{p1}(a^{2t})^{p1} + e_{p2}(a^{2t})^{p2} + \ldots + e_{pt}(a^{2t})^{pt} \]  
(7)

The syndrome has \(2t\) terms, such as \(S(a^1), S(a^2), \ldots, S(a^{2t})\). The \(e_{pi}\) variable in the syndrome represents the amplitude of the error at the \(pi\) position, and \((a^i)^{pi}\) indicates the location of the error. The number of error, \(u\) and variable \(i\) are defined as \(1 \leq u \leq t\) and \(1 \leq i \leq 2t\), respectively. If the \(2t\) pieces of \(S(a^i)\) terms in the syndrome are all equal to zero, then there is no error. So, there is no need for a correction. However, if one or more \(S(a^i)\) terms are nonzero, error location polynomials must be found. Error location polynomial for \(x = a^j\) is shown as,

\[ \Delta(x) = \Delta_0 + \Delta_1 x + \ldots + \Delta_{u-1} x^{u-1} \]  
(8)

The Berlekamp–Massey algorithm is the best known method to create error location polynomial in RS coding. After creating the polynomial with this algorithm, the easiest way to find the roots \((a^i)\) of the polynomial defined in \(GF(2^m)\) is to use the Chien search method. After the roots of the polynomial are found, the opposite roots \((x^{-1} = (a^i)^{-1})\) of these roots in \(GF(2^m)\) give the location of the error.

In the first stage, the error location polynomial, the roots of the polynomial and the error locations were found, but this information is not enough to correct the error, since RS encoding is recommended for non-binary numbers. Therefore, the amplitude of the error should also be determined. To determine the amplitude of the error, the error amplitude polynomial \(\Omega(x)\) is created as in Equation (9).

\[ \Omega(x) = [S(x)\Delta(x)] \mod(x^{2t}) \]  
(9)

Forney equations are used to construct the error amplitude polynomial, and calculate the amplitude of the error. The amplitude of the error for the value of \(a^i\) in \(GF(2^m)\) is

\[ e_{pi} = \frac{\Omega(a^{-i})}{\Delta'(a^{-i})} \]  
(10)
where \( \Delta'(x) \) denotes derivate of \( \Delta(x) \). Thus, the location and amplitude of the errors in the \( u \) positions are found in the noisy \( r(x) \) codeword in the receiver. After all error values \( (e(x)) \) are found, the error of the information message in the RS(n, k) codeword is corrected as in Equation (11), where \( \oplus \) denotes bit-wise ex-or operation.

\[
\hat{c}(x) = r(x) \oplus e(x) \tag{11}
\]

3. Proposed RS-Based Data Hiding Method

In this study, we aim to increase the resistance of the message hidden in medical images against salt and pepper noise. In the proposed method, the secret message is encoded with Reed Solomon codes and hidden in medical images. It is assumed that the stego image created by the proposed method is exposed to salt and pepper noise in the communication channel. Although the main purpose of the study is to test the resistance to noise, the method used for data hiding is also compatible with high capacity hiding. With the proposed method, we aimed to determine how accurately the secret message was extracted from the noisy medical image.

In the proposed method, first of all, operations are made with the logo that will be hidden in the medical image as a secret message. The brightness values of the secret logo are transferred to a message array as a result of the row-column operations. Each element in the message array is converted to eight-bit numbers. A new array is created with all converted brightness value elements. In RS(n, k) coding, each symbol consists of decimal numbers encoded with \( m \) bits. Therefore, the bit sequence of the secret message is divided into \( m \)-bit symbols. Each \( m \)-bit symbol is converted to decimal values. Decimal message symbols are converted to \( GF(2^m) \) numbers in Galois field, with the help of \( x^m + x + 1 \) minimal polynomial. By taking \( k \) of these message symbols, \( b(x) \) polynomial is created. With the help of the information polynomial \( b(x) \), and the generator polynomial \( g(x) \), the parity polynomial, \( p(x) \) that will add to the RS(n, k) codeword, is calculated as in Equation (3). Finally, the RS(n, k) codeword that consists of \( k \) message symbols and \( 2t \) parity symbols, is obtained as a \( n \)-element Reed Solomon message array. The secret message is now ready to be hidden in the medical image.

In this study, we aimed to make corrections unless all \( k \) symbols in the codeword are distorted. RS(7, 3) coding has been used in terms of compliance with both these conditions and the proposed hiding method. Therefore, \( m = 3, n = 2^m - 1 = 7 \) and \( k = 3 \), and the maximum number of errors that can be corrected in a codeword, is \( t = 2 \) symbols.

\[
p_e(j) = \begin{cases} 
p(j) - p(j) [\mod 10] & p(j) < 250 \\
249 - 249 [\mod 10] & p(j) \geq 250
\end{cases} \tag{12}
\]

These symbols embed to the luminance value of medical images with the proposed embedding method. For the data hiding method, it is proposed to hide a symbol directly into the brightness value of the pixel instead of the classic bit substitution methods. Thus, each symbol will be added to a pixel luminance \( (p) \) according to Equations (12) and (13). In this process, the proposed method changes pixel values a little, but when compared with its other advantages, these changes can be neglected. Because, the proposed method change pixel values, but these changes are unnoticeable in the human visual system. By hiding an RS symbol to a pixel, we change and lose some information. However, we reduce the amount of RS symbols that are affected by noise. This is because if the bits of a symbol are divided into more than one pixel the amount of noise exposure will increase. Moreover, when a secret symbol is embedded with the proposed method, there is not much significant loss. A lot of data hiding algorithms, such as [19,27], aim to reduce the lost or changes after embedding secret messages, while providing high capacity and high fidelity.

In the proposed data hiding method, \( n \)-tuple of the pixel of the medical image is taken first. Then, the units digit of the each luminance value is emptied and the new pixel value \( (p_e) \) is obtained, as in Equation (12). Because of preventing pixel luminance from exceeding the range 0-255 in the stego
image, if a pixel value is 250 or greater, its value is set to 249. Each secret symbol of the Reed Solomon codeword is embedded to corresponding \( p_e \) as in Equation (13), and the modified pixel \((p_m)\) is obtained.

\[
p_m(j) = p_e(j) + s(j) \quad 0 \leq j \leq n - 1
\]  

(13)

This process continues until all secret message symbols are hidden in the medical image. The stego image is transferred to the communication channel to be sent to the receiver. A practical representation of the proposed data hiding method in Figure 2 is given over RS(7, 3). When the example in Figure 2 is examined, it is seen that the proposed data hiding method does not make many changes in the pixel values. Although it is focused on the extracting performance of the hidden message from the noisy signal, the embedding capacity of the proposed method can be increased by up to 3 bits per pixel (bpp).

The data extraction process on the receiver side is performed similarly to the hiding process. The stego image which exposed to salt and pepper noise in the channel is going to the receiver. Reed Solomon decoder uses the number defined in \( GF(2^m) \). Therefore, if the noise corrupted pixels’ unit digits exceeds \( 2^m - 1 \), a pre-process must be done. With help of the pre-process, the unit digit of

---

**Figure 2.** Practical representation of the proposed data hiding method via RS(7, 3).
erroneous pixel which bigger than $2^m - 1$ set as $2^m - 1$. This process does not affect any secret data while help the working RS decode. Because, if the symbol value is not correct, it does not matter what it is. RS will correct the symbol with the decoding process anyway.

The values in the units digit of the pixel brightness in the stego image are taken until the message ends and the distorted message sequence $r(x)$ is created. In the false message array, $S(x)$ syndrome is generated for each codeword in length $n$. To detect the locations of errors in the syndrome, error location polynomial $\Delta(x)$ is created by the Berlekamp–Massey algorithm. The roots of the error location polynomial are calculated by the Chien search method. By calculating the opposite roots of the found roots, the locations of the error/-errors in the message syndrome are determined. Error amplitude polynomial $\Omega(x)$ is created for the amplitude information of the detected errors. With the help of Forney equations, the amplitude of the error is calculated by using $\Omega(x)$ and $\Delta(x)$. As a result of these operations, the error/noise model is extracted. There are $k$ hidden messages that are extracted from noisy images, as in Equation (11). Thus, $k$ hidden messages in an RS$(n, k)$ codeword are retrieved. This process continues until all the secret messages in all syndromes are cleared and separated. Each decimal element in the extracted secret message array is converted to $m$-bit numbers and a secret message bit sequence are created. By usage of this bit sequence, the pixel values of the logo are created and the secret message is retrieved by the receiver.

4. Experimental Results

The images were taken from the open source European Society of Radiology database [28]. The images are shown in Figure 3 and all are in 480×480 resolution. For ease of comparison, the gray logo of Kocaeli University is used as a secret message instead of a text message. The gray logo was set in different resolutions, hidden in medical images, and the test results were examined. In the proposed method, Reed Solomon codewords are produced by RS$(7, 3)$.

![Figure 3](image-url)

**Figure 3.** The medical images used for data hiding. (a) CT, (b) MRI, (c) US, (d) X-ray.

The primary purpose of this study is to retrieve the secret logo right from the noisy environment. However, it was also tested whether the visual quality of the proposed data hiding method gives
good results. First of all, stego images of the proposed method were evaluated in terms of quality parameters. For this purpose, the quality criteria such as mean square error (MSE), peak signal to noise ratio (PSNR) and structural similarity (SSIM) were examined in stego images. Equation (14) shows MSE calculated with $R \times C$ size original ($I_o$) and stego ($I_s$) images, and Equation (15) shows PSNR.

$$MSE = \frac{1}{R \times C} \sum_{r=1}^{R} \sum_{c=1}^{C} (I_o(r,c) - I_s(r,c))^2$$  \hspace{1cm} (14)$$

$$PSNR = 20 \times log_{10} \left( \frac{255}{\sqrt{MSE}} \right)$$  \hspace{1cm} (15)$$

Equation (16) shows the structural similarity index (SSIM). If the mean values for original and stego images $\mu_o$ and $\mu_s$, variances are $\sigma_o$ and $\sigma_s$, and covariance is $\sigma_{os}$, then SSIM is calculated as,

$$SSIM = \frac{(2\mu_o\mu_s + C_1)(2\sigma_{os} + C_2)}{(\mu_o^2 + \mu_s^2 + C_1)(\sigma_o^2 + \sigma_s^2 + C_2)}$$  \hspace{1cm} (16)$$

where the $C_1$ and $C_2$ coefficients are small constants. If two images are the same, then SSIM is equal to 1. Table 1 shows the results of the proposed method for different embedding capacity in terms of bit-per-pixel (bpp). In the Table 1, it is seen that performance results of same type stego images are almost the same. The fact is that, it is deduced that results do not change too much when the number of images increases. Therefore, for simplicity, the rest of the paper shows the result for the images in the first column of Figure 3.

| Stego Image | PSNR (dB) | MSE  | SSIM  | Stego Image | PSNR (dB) | MSE  | SSIM  |
|-------------|----------|------|-------|-------------|-----------|------|-------|
| CT(1)       | 48.49    | 0.842| 0.981 | US(1)       | 48.97     | 0.527| 0.991 |
| CT(2)       | 46.76    | 1.370| 0.958 | US(2)       | 47.82     | 0.926| 0.974 |
| CT(3)       | 48.39    | 0.938| 0.974 | US(3)       | 47.15     | 1.177| 0.969 |
| CT(4)       | 47.17    | 1.235| 0.962 | US(4)       | 47.97     | 0.811| 0.979 |
| CT(5)       | 47.47    | 1.040| 0.972 | US(5)       | 47.20     | 1.204| 0.963 |
| CT(6)       | 48.01    | 0.814| 0.981 | US(6)       | 47.65     | 0.964| 0.973 |
| MRI(1)      | 48.55    | 0.870| 0.976 | X-ray(1)    | 48.99     | 0.452| 0.992 |
| MRI(2)      | 49.50    | 0.704| 0.983 | X-ray(2)    | 49.18     | 0.358| 0.993 |
| MRI(3)      | 49.34    | 0.713| 0.982 | X-ray(3)    | 48.39     | 0.938| 0.974 |
| MRI(4)      | 49.12    | 0.742| 0.980 | X-ray(4)    | 50.79     | 0.217| 0.993 |
| MRI(5)      | 50.94    | 0.159| 0.994 | X-ray(5)    | 46.76     | 1.370| 0.958 |
| MRI(6)      | 47.02    | 1.269| 0.962 | X-ray(6)    | 48.63     | 0.566| 0.987 |

Table 2 shows the average performance values of all images for different capacity sizes. The PSNR value is above 35 dB and the SSIM value is close to 1 in the images without any compression process; this shows that the visual quality does not change too much after hiding. When Table 2 is examined, it can be seen that the data hiding into the unit digit of the pixel of the cover image gives acceptable results.

In Tables 3 and 4, the quality values of stego images of the proposed method were compared with existing medical data hiding methods. In most of the medical data hiding methods extracted, message quality is more important than high embedding capacity. So, experimental results were given for the same embedding capacity for a fair comparison. On the other hand, the hidden message is extracted with similar accuracy from noisy stego images for all capacity values. In Table 3, PSNR and SSIM values are given for the stego MRI image, with 0.79 bpp or less embedding capacity. The proposed method provides superiority to the other two methods in terms of PSNR. Although [3] study is in good condition in terms of SSIM, the amount of hidden data is low. It is obvious that the [3] method will yield much lower results than the proposed method for 0.79 bpp capacity.
Table 2. Average quality parameters of the proposed method under different capacity conditions.

| Stego Image Type | Capacity (bpp) | Avg. PSNR (dB) | Avg. MSE | Avg. SSIM |
|------------------|---------------|----------------|---------|----------|
| CT               | 0.083         | 50.80          | 0.519   | 0.985    |
| MRI              | 0.164         | 47.72          | 1.040   | 0.971    |
| US               | 0.332         | 44.55          | 2.135   | 0.945    |
| X-ray            | 0.656         | 41.74          | 3.905   | 0.910    |
| CT               | 3             | 35.21          | 16.89   | 0.681    |
| MRI              | 0.794         | 38.31          | 0.8992  | MRI      |
| US               | 0.600         | 37.27          | 0.9777  | MRI      |

Table 3. Stego image quality comparison with existing methods (Capacity ≤ 0.79 bpp).

| Method            | PSNR (dB) | SSIM   | Capacity (bpp) | Image Type |
|-------------------|-----------|--------|----------------|------------|
| Proposed RS-based | 41.85     | 0.9335 | 0.794          | MRI        |
| [14]              | 38.31     | 0.8992 | 0.789          | MRI        |
| [3]               | 37.27     | 0.9777 | 0.600          | MRI        |

Table 4. Stego image quality comparison with existing methods (Capacity ≤ 0.33 bpp).

| Method            | PSNR (dB) | SSIM   | Capacity (bpp) | Image Type |
|-------------------|-----------|--------|----------------|------------|
| Proposed RS-based | 46.26     | 0.9858 | 0.33           | X-ray      |
| [3]               | 37.86     | 0.9830 | 0.30           | MRI        |
| [4]               | 41.19     | 0.9905 | 0.10           | X-ray      |
| [13]              | 40.26     | 0.9627 | 0.01           | CT         |
| [29]              | 46.22     | 0.9406 | 0.01           | CT         |

In Table 4, quality comparison results are given for the different stego image with 0.33 bpp or less embedding capacity. If the embedding capacity of the other methods is equal to the proposed method, all values of these methods will decrease. Considering this situation, stego images offer better visual qualities than existing methods in terms of both PSNR and SSIM.

After data hiding, the stego image is transmitted to the receiver side through the communication channel that noiseless or contains different densities of salt and pepper noise. Secret data was extracted from the stego image in the receiver and the results were evaluated. Another data hiding (called no-RS) method was used to compare the performance of the proposed RS-based method. In this method, the secret logo is hidden directly on medical images without the RS method. Namely, the message sequence of the secret logo, which is converted into bits as a result of pre-processing, is divided into triple symbol groups and converted into decimal numbers. These elements are hidden directly to the units digit of the medical image by a similar method.
The abbreviations in the tables are as follows:

- Proposed RS-based: the proposed method of this paper that used RS-based data hiding.
- No-RS: similar to the proposed method, but without RS coding secret data embedded directly.

Figure 4 shows the logos extracted from stego images exposed to salt and pepper noise at a density of 1%. Thanks to the proposed RS-based method, the logo is exactly retrieved in the same quality in all medical image types. Figure 5 shows the logos extracted from MRI stego images that were exposed to salt and pepper noise of different densities. When Figure 5 is examined carefully, it is seen that the logos hidden by the proposed RS-based method are highly resistant to salt and pepper noises of various densities. As the logo size increases, the hidden message symbols begin to spread to the whole image, and the logo is slightly distorted.

![Figure 4](image-url)  
**Figure 4.** The logo extracted from stego images with salt and pepper noise density of 1%. (a) no-RS method, (b) Proposed RS-based method.

Besides the visual evaluations of the extracted logo, objective evaluations were made. The SSIM value is calculated for the similarity of the stego image, as well as for the similarity of the logo. Table 5 shows the SSIM results of the logo extracted from CT, MRI, X-ray and US stego images for different noise densities. The values that the proposed RS-based method reaches at 10% noise density are not reached even in 1% noise density without RS. Therefore, the message hidden by the proposed RS-based method has a high resistance to noise.

| Noise Density | Proposed RS-Based Method | No-RS Method |
|---------------|--------------------------|--------------|
|               | CT | MRI | US | X-ray | CT | MRI | US | X-ray |
| 0%            | 1  | 1   | 1  | 1     | 1  | 1   | 1  | 1     |
| 1%            | 1  | 1   | 1  | 1     | 0.95 | 0.96 | 0.95 | 0.94  |
| 5%            | 1  | 0.99 | 0.99 | 0.99 | 0.80 | 0.80 | 0.82 | 0.81  |
| 10%           | 0.95 | 0.96 | 0.97 | 0.96 | 0.70 | 0.72 | 0.70 | 0.68  |
| 20%           | 0.76 | 0.80 | 0.79 | 0.79 | 0.58 | 0.56 | 0.58 | 0.59  |
| 50%           | 0.32 | 0.31 | 0.34 | 0.33 | 0.29 | 0.29 | 0.28 | 0.30  |

The bit error rate (BER) value is used to determine the rate of distortion in the hidden message, which indicates the ratio of the number of bits broken to the total number of bits. In Equation (17), a calculation is made for the embedded \( L_{emb} \) and extracted \( L_{ext} \) bit values of the \( M \times N \) size logo.
The higher the amount of distortion of the secret message, the higher the BER value; the lower BER value means better results.

\[
BER(\%) = 100 \times \left( \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} \{L_{emb}(m, n) \oplus L_{ext}(m, n)\}}{M \times N} \right)
\]  

(17)

Figure 5. Extraction of hidden message in stego MRI image for different logo size. (a) Salt and pepper noise density, (b) Proposed RS-based method, logo size: 45 × 45, (c) no-RS method, logo size: 45 × 45, (d) Proposed RS-based method logo size: 64 × 64, (e) no-RS method logo size: 64 × 64.
Table 6 shows the BER value in the logo, retrieved from the stego images. According to Table 6, the message hidden by the no-RS method was extracted with a higher error rate than the message hidden by the proposed RS method. Despite the noise, the message hidden by the proposed RS method can be obtained with very few errors.

Table 6. Bit error rate (BER) (%) value of secret message for logo size: 45 × 45.

| Noise Density | Proposed RS-Based Method | No-RS Method |
|---------------|--------------------------|--------------|
|               | CT | MRI | US | X-ray | CT | MRI | US | X-ray |
| 0%            | 0  | 0   | 0  | 0     | 0  | 0   | 0  | 0     |
| 1%            | 0  | 0   | 0  | 0     | 0.7| 0.5 | 0.7| 0.6   |
| 5%            | 0.1| 0.1 | 0.2| 0.1   | 3  | 2.8 | 2.7| 2.7   |
| 10%           | 0.5| 0.5 | 0.5| 0.6   | 5.9| 5.6 | 5.6| 6     |
| 20%           | 3.9| 3.1 | 3.8| 3     | 11.5|11.1|11.1|10.7   |
| 50%           | 24.9|25.1|24.9|24.6   | 28 | 28.5|28.2|28.1   |

The results of the proposed RS-based method and no-RS methods for all images are given in Tables 5 and 6. There are two more striking aspects in the results in Table 6. First, the hidden message in data hiding by the proposed RS-based method is almost error-free, even at 10% density noise. However, in hiding without RS, the message is erroneously extracted, even at the lowest noise. Second, the proposed method gives very superior results at all noise values. However, when the noise density approaches 50%, the values of the proposed method begin to decrease very much. The main reason for this is that loud noise completely changes the RS codewords. This is because it is not possible to extract the correct information in the completely distorted codewords.

In Figure 6, the BER and SSIM results of the hidden message extracted from the stego image for different salt and pepper noise intensities are presented with comparative graphics.

Finally, the proposed method was compared with the existing methods in this study. In Table 7, the BER values of the secret message are compared with similar methods in the literature. All of the methods in Table 7 evaluated the extracted secret message from the stego image that contains salt and pepper noise, with a density of 1%. The proposed method recovers the message without loss at 1% noise density, while other methods give up to a quarter of the message losses.

Table 7. Comparison of BER (%) value of the secret message with existing methods.

| Noise Density | Proposed RS-Based | [13] | [14] | [15] | [30] | [29] |
|---------------|-------------------|------|------|------|------|------|
| 1%            | 0                 | 8.2  | 0.15 | 5.1  | 0.14 | 28.4 |

While the noise density is 1%, there are two methods with the BER value closest to the proposed method. In Table 8, a second comparison was made for these two methods for different noise densities. Table 8 shows the BER and SSIM comparison results of the secret message. When Table 8 is evaluated, it is seen that the proposed method has better BER values compared to [30]. At noise densities of 5% and 10%, the proposed RS-based method is superior to the [14] methods, which proposed that one uses a noise filtering block. Although the BER value of the proposed RS-based method at 20% noise density is superior, the SSIM value is lower. At 50% noise density, both methods give bad results.
Figure 6. Evaluation of the retrieved secret message according to the salt and pepper noise density. (a) SSIM-Noise Density, (b) BER-Noise Density.
Table 8. Comparison of BER (%) value of the secret message with existing methods (n/a: not available).

| Noise Density | Proposed RS-Based | [14] | [30] |
|---------------|------------------|------|------|
|               | BER (%) | SSIM | BER (%) | SSIM | BER (%) | SSIM |
| 1%            | 0       | 1    | 0.15    | 0.9127 | 0.14   | n/a  |
| 5%            | 0.1     | 0.9811 | 1.06   | 0.9069 | 0.48   | n/a  |
| 10%           | 0.6     | 0.9033 | 2.47   | 0.9002 | n/a    | n/a  |
| 20%           | 4.1     | 0.7033 | 5.77   | 0.8875 | n/a    | n/a  |
| 50%           | 26      | 0.3144 | 21.6   | 0.8368 | n/a    | n/a  |

Finally, the performance of the proposed method is tested against different noises. Three types of noises added to the stego images and test results were evaluated in terms of BER. The normal distributed Gaussian noise and uniform distributed additive uniform and multiplicative speckle noises are applied to the stego images with different variance sizes. The test results are given in Table 9. As stated above, the proposed method is resistant to an amount of noise density. So, Gaussian and uniform noises are set to one fifth of the stego images. The mean values for all noise types are zero. From Table 9 it is seen that the hidden message is extracted, with lower error for Gaussian and uniform noise.

Table 9. Comparison of BER (%) value of the secret message for different noise types.

| Noise Type | Variance | Proposed RS-Based Method | No-RS Method |
|------------|----------|--------------------------|--------------|
|            |          | CT          | MRI | US  | X-ray | CT | MRI | US | X-ray |
| Gaussian   | 0.005    | 0.9     | 0.8  | 1.1 | 1     | 5.4 | 6   | 6  | 6.4  |
|            | 0.01     | 1.7     | 1.7  | 2.2 | 2.1   | 7.5 | 7.3 | 8.3| 8.2  |
|            | 0.005    | 6.4     | 1.3  | 32.4| 42    | 9.1 | 5.9 | 31.3| 43.1 |
| Speckle    | 0.01     | 10.8    | 5    | 32.8| 42.4  | 14.4| 11.2| 33.5| 42.5 |
| Uniform    | 0.1      | 2.5     | 2.7  | 2.5 | 2.4   | 9.9 | 9   | 9.5| 9    |

On the other hand, speckle noise affects stego images more than other noises. So, hidden messages in the CT and MRI are extracted correctly, while an important part of secret messages in the US and X-ray is lost. Therefore, the proposed RS-based method has also resisted against Gaussian and uniform noises for all images.

5. Conclusions

In this study, a new data hiding method based on Reed Solomon error control coding is proposed for medical images. The proposed method was tested with several medical images. Image quality results of the same type of medical images are almost the same. Stego images of the proposed method give remarkably better results compared to existing medical data hiding methods in terms of PSNR and SSIM for similar capacities. On the other hand, the secret message extracting the performance of the proposed method is compared with the results of a second method, which does not contain the proposed RS block. Salt and pepper noises of different densities were added to stego images, and the state of the retrieval of the secret message was examined. The proposed RS-based method is almost error-free, even at 10% density noise, and BER values are also almost 0. At 20% noise density, the proposed method reduces BER by 70% and increases SSIM by 30%. Hence, the RS-based data hiding shows a superior performance compared to the direct hiding algorithm up to an amount of noise density. Moreover, the proposed method tested against low density of other noises. The RS-based method reduce BER by about 70% for Gaussian and uniform noises, when speckle noise applied stego images BER reduced 27% for CT and 10% for MRI. Unfortunately, the proposed method was not reduced the BER values for speckle noise corrupted US and X-ray stego images. When the noise rate increases too much, it is no longer possible to obtain correct symbols in some codewords, because the entire codeword is broken. The performance results of the extracted secret message were compared to
existing medical data hiding methods that tested the resistance to salt and pepper noise. Consequently, the proposed method provides very superior performance at different salt and pepper noise densities.

Author Contributions: Conceptualization, M.Z.K. and S.Ö.; methodology, M.Z.K. and S.Ö.; software, M.Z.K.; validation, M.Z.K. and S.Ö.; formal analysis, S.Ö.; investigation, M.Z.K.; resources, M.Z.K.; data curation, M.Z.K.; writing—original draft preparation, M.Z.K.; writing—review and editing, S.Ö.; visualization, M.Z.K.; supervision, S.Ö.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Fallahpour, M.; Megias, D.; Ghanbari, M. High capacity reversible data hiding in medical images. In Proceedings of the 16th IEEE International Conference on Image Processing (ICIP), Cairo, Egypt, 7–10 November 2009; pp. 4241–4244.
2. Er, F.; Yalman, Y. Adaptive Multiple Peak and Histogram based Reversible Data Hiding. In Proceedings of the Ninth International Conference on Image Processing Theory, Tools and Applications (IPTA), Istanbul, Turkey, 6–9 November 2019; pp. 1–5.
3. Yang, Y.; Zhang, W.; Liang, D.; Yu, N. Reversible data hiding in medical images with enhanced contrast in texture area. *Digit. Signal Process.* 2016, 52, 13–24. [CrossRef]
4. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* 2003, 13, 890–893. [CrossRef]
5. Lou, D.C.; Hu, M.C.; Liu, J.L. Multiple layer data hiding scheme for medical images. *Comput. Stand. Interfaces* 2009, 31, 329–335. [CrossRef]
6. Al-Qershi, O.M.; Khoo, B.E. High capacity data hiding schemes for medical images based on difference expansion. *J. Syst. Softw.* 2011, 84, 105–112. [CrossRef]
7. Mousavi, S.M.; Naghsh, A.; Hejazi, S.A.; Abu-Bakar, S.A.R. A Comparative Analysis on Reversible Watermarking Techniques in Medical Images. *J. Teknol.* 2015, 72, 119–123. [CrossRef]
8. Zain, J.M.; Clarke, M. Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images. *Int. J. Comput. Sci. Netw. Secur.* 2007, 7, 19–28.
9. Memon, N.A.; Gilani, S.A.M. Watermarking of chest CT scan medical images for content authentication. *Int. J. Comput. Math.* 2011, 88, 265–280. [CrossRef]
10. Memon, N.A.; Chaudhry, A.; Ahmad, M.; Keerio, Z.A. Hybrid watermarking of medical images for ROI authentication and recovery. *Int. J. Comput. Math.* 2011, 88, 2057–2071. [CrossRef]
11. Badran, E.F.; Sharkas, M.A.; Attallah, O.A. Multiple Watermark Embedding Scheme in Wavelet-Spatial Domains Based on ROI of Medical Images. In Proceedings of the 2009 National Radio Science Conference, New Cairo, Egypt, 17–19 March 2009; pp. 1–8.
12. Al-Dmour, H.; Al-Ani, A. A Medical Image Steganography Method Based on Integer Wavelet Transform and Overlapping Edge Detection. In *Neural Information Processing ICONIP 2015, Lecture Notes in Computer Science*; Arik, S., Huang, T., Lai, W., Liu, Q., Eds.; Springer: Cham, Switzerland, 2015; Volume 9492.
13. Parah, S.A.; Sheikh, J.A.; Ahad, F.; Loan, N.A.; Bhat, G.M. Information hiding in medical images: A robust medical image watermarking system for E-healthcare. *Multimed. Tools Appl.* 2017, 76, 10599–10633. [CrossRef]
14. Mousavi, S.M.; Naghsh, A.; Manaf, A.A.; Abu-Bakar, S.A.R. A robust medical image watermarking against salt and pepper noise for brain MRI images. *Multimed. Tools Appl.* 2017, 76, 10313–10342. [CrossRef]
15. Parah, S.A.; Ahad, F.; Sheikh, J.A.; Bhat, G.M. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *J. Biomed. Inform.* 2017, 66, 214–230. [CrossRef]
16. Hajjaji, M.A.; Mtibaa, A.; Bourennane, E. A Watermarking of Medical Image: New Approach Based On Multi-Layer Method. *Int. J. Comput. Sci.* 2011, 8, 33–41.
17. Fontaine, C.; Galand, F. How Reed-Solomon Codes Can Improve Steganographic Schemes. *EURASIP J. Inf. Secur.* 2009, 274845, 1–10.
18. Diop, I.; Farssi, S.M.; Khouma, O.; Diof, H.B.; Tall, K.; Sylla, K. New Steganographic scheme based of Reed-Solomon codes. *Int. J. Distrib. Parallel Syst.* 2012, 3, 81–89. [CrossRef]
19. Konyar, M.Z.; Akbulut, O.; Ozturk, S. Matrix Encoding based High Capacity and High Fidelity Reversible Data Hiding in HEVC. *Signal Image Video Process.* 2020. [CrossRef]
20. Ishengoma, F.R. The Art of Data Hiding with Reed-Solomon Error Correcting Codes. *Int. J. Comput. Appl.* 2014, 106, 28–31.
21. Jebin, P.S.; Shyni, K. Implementation of Reed Solomon Algorithm over Data Hiding in Video Streams. *Int. J. Innov. Res. Comput. Commun. Eng.* 2017, 5, 8534–8540.
22. Kim, S. Reversible data-hiding systems with modified fluctuation functions and reed-solomon codes for encrypted image recovery. *Symmetry* 2017, 9, 61. [CrossRef]
23. Banerjee, A.; Jana, B. A robust reversible data hiding scheme for color image using reed-solomon code. *Multimed. Tools Appl.* 2019, 78, 24903–24922. [CrossRef]
24. Reed, I.S.; Solomon, G. Polynomial Codes over Certain Finite Fields. *J. Soc. Ind. Appl. Math. (SIAM)* 1960, 8, 300–304. [CrossRef]
25. Gravano, S. *Introduction to Error Control Codes*; Oxford University Press: Oxford, UK; New York, NY, USA, 2001; pp. 154–228.
26. Moon, T.K. *Error Correction Coding: Mathematical Methods and Algorithms*; John Wiley & Sons: Hoboken, NJ, USA, 2005; pp. 235–280.
27. Solak, S.; Altınısk, U. Image steganography based on LSB substitution and encryption method: Adaptive LSB+3. *J. Electron. Imaging* 2019, 28, 043025. [CrossRef]
28. Eurorad by European Society of Radiology. Available online: https://www.eurorad.org/ (accessed on 19 January 2020).
29. Rahimi, F.; Rabbani, H. A dual adaptive watermarking scheme in contourlet domain for DICOM images. *BioMed. Eng. OnLine* 2011, 10, 1–18. [CrossRef] [PubMed]
30. Singh, A.; Dave, M.; Mohan, A. Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimed. Tools Appl.* 2015, 75, 8381–8401. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).