Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA

Jaishree Jain 1,2,*, Arpit Jain 1, Saurabh Kumar Srivastava 1, Chaman Verma 3, Maria Simona Raboaca 4,5,6 and Zoltán Illés 3

1 College of Computing Sciences and IT, Teerthanker Mahaveer University, Moradabad 244001, India; arpit.computers@tmu.ac.in (A.J.); saurabhs.computers@tmu.ac.in (S.K.S.)
2 Department of Computer Science and Engineering, Ajay Kumar Garg Engineering College, Ghaziabad 201009, India
3 Department of Media and Educational Informatics, Faculty of Informatics, Eötvös Loránd University, 1053 Budapest, Hungary; chaman@inf.elte.hu (C.V.); illes@inf.elte.hu (Z.I.)
4 National Research and Development Institute for Cryogenic and Isotopic Technologies—ICSI Rm, 240050 Ramnicu Valcea, Romania; simona.raboaca@icsi.ro
5 Faculty of Electrical Engineering and Computer Science, Stefan cel Mare University, 720229 Suceava, Romania
6 Doctoral School, Polytechnic University of Bucharest, 313 Splaiul Independentei, 060042 Bucharest, Romania
* Correspondence: jaishree.scholar@tmu.ac.in

Abstract: With the rapid advancements of the internet of things (IoT), several applications have evolved with completely dissimilar structures and requirements. However, the fifth generation of mobile cellular networks (5G) is unable to successfully support the dissimilar structures and requirements. The sixth generation of mobile cellular networks (6G) is likely to enable new and unidentified applications with varying requirements. Therefore, 6G not only provides 10 to 100 times the speed of 5G, but 6G can also provide dynamic services for advanced IoT applications. However, providing security to 6G networks is still a significant problem. Therefore, in this paper, a hybrid image encryption technique is proposed to secure multimedia data communication over 6G networks. Initially, multimedia data are encrypted by using the proposed model. Thereafter, the encrypted data are then transferred over the 6G networks. Extensive experiments are conducted by using various attacks and security measures. A comparative analysis reveals that the proposed model achieves remarkably good performance as compared to the existing encryption techniques.

Keywords: internet of things; e-healthcare; hyper-chaotic map; 6G; 5G

MSC: 68-04

1. Introduction

Motivated by the higher requirements of several applications, internet of things (IoT) networks are growing at a rapid rate. Due to higher demands of bandwidth and resources, 5G networks are unable to fulfill the requirements of ubiquitous connectivity, wide coverage, significantly high capacity, etc., needed by IoT devices. Therefore, to achieve the real-time processing of massive data of IoT devices, 6G cellular networks would be used. However, providing security to 6G-enabled IoT networks is still an open area of research [1–3].

In 6G enabled IoT networks, massive amounts of multimedia data will be transferred in every single second. These massive data will be communicated over public 6G cellular networks [4,5]. Therefore, these data are prone to various security threats. There are other challenges that exist while transferring e-healthcare data over the network. As one might imagine, bringing so many data together and using them to make decisions is not without its challenges. Fragmented data, ever-changing data, privacy/security regulations, and
patient expectations are four of the primary data challenges facing the healthcare industry today. In this paper, to secure such data, we have considered the use of hyper-chaotic maps to encrypt the multimedia data [6–8]. Thus, the encrypted data will be transferred over the public 6G network, and also the same encrypted data will be stored on a cloud server. Recently, many image encryption techniques have been proposed to provide secure communication of multimedia data [9].

Figure 1 shows the proposed 6G-enabled secure IoT framework for multimedia applications. Initially, data will be collected at the perception layer by different kinds of IoT sensors. The proposed encryption algorithm is applied to encrypt the sensed data. Thereafter, the encrypted multimedia data are then transmitted over the 6G public networks to the data processing and storage layer for further processing. At the network layer, the different applications and users can only retrieve the extracted data if they have the exact secret key. If the secret key is wrong, even by a single bit, then the proposed model returns completely noisy data without any kind of statistical information about the actual data.

The main contributions of this paper are as follows:

1. We develop a hybrid technique to encrypt the confidential data related to e-healthcare.
2. The hyper-chaotic method and zero-watermarking techniques along with the Rivest–Shamir–Adleman (RSA) algorithm are hybridized to encrypt the data.
3. The proposed technique is used to secure multimedia data communications over 6G networks.

The remaining paper is organized as follows: A literature review is presented in Section 2. Section 3 discusses the proposed model. Section 4 presents the experimental analysis.

2. Literature Review

There are various multimedia data that are used for sharing over networks. Images play an important role in various fields, such as healthcare, agriculture, science, and engineering. Healthcare images contain some sensitive information or data related to patient privacy. Hence, there is several security breaching attacks that can affect the secrecy of images [11,12]. Therefore, to prevent these attacks, there are various security algorithms that can be applied.

In [13], Y. Ding et al. implemented deep learning-based biomedical image encryption techniques along with a cycle generative adversarial network (CGAN) were used to encrypt the images. In [14], Wang and Zhang designed a GPU-accelerated homomorphism encryption technique for obtaining faster results with encryption techniques. In [15], Liu et al. discussed a verifiable multi-keyword search (VMKS) encryption technique. For biomedical images, it generated an anonymous key. To scramble electronic health records, a convergence key was also utilized.

In [16], Haddad et al. used joint watermarking-encryption-JPEG-LS (J JL) for healthcare data. For encryption, bit substitution watermarking modulation with JPEG-LS was also used. In [17] Qiu et al. utilized a secure communication model by using a selective encryption technique (SET) combined with fragmentation and dispersion.

In [18], Jiang et al. outlined homomorphic encryption (SHE) for single instruction multiple data, which encrypts data with fewer overheads. In [19], Puriwat et al. invented a revocable, privacy-preserving, fine-grained data sharing technique with keyword search to encrypt the healthcare data. For data authenticity, a pseudo-identity-based signature approach was also used. In [20], Ross depicted a blind batch encryption technique to encrypt the healthcare data. It has been found that this technique can resist six typical attacks.

In [21–27], the authors found that attribute-based encryption can ensure data confidentiality and user privacy in the healthcare environment. Partially policy-hidden and large universe-based encryption techniques were also used. In [28–35], the authors designed an efficient access policy expression approach by considering 0–1 coding in CNN. In [36–39], Ma et al. designed an efficient access control technique and a fine-grained data sharing model. This approach is suitable for resource-constrained mobile devices. A couple of exploration systems were designed for image watermarking. The authors of [40–45] proposed a multi-reason image-watermarking framework for ownership checking. DWT was used to decompose the image into the wavelet domain. The authors of [46–49] presented a square-based outwardly disabled watermarking technique using DWT and DCT. Quantization index modulation was also implemented to reduce the bit error rate (BER) of expelled watermarks. Artificial bee colony-based LSB [50,51] was used to embed the watermark. Erivelton et al. presented a novel image encryption scheme based on the pseudo-orbits of a 1D chaotic map by using the difference of two pseudo-orbits to generate a random sequence. The generated sequence has been successful in all NIST tests, which implies that it has adequate randomness to be employed in encryption processes [52–55]. The fractional order Lorenz chaotic system is used to generate the chaotic sequence. The article outlines the characteristic of the chaotic sequence. Two examples with plain texts and plain images were shown for using the approach that we introduced [56–59]. According to the results of the analyses, an interesting image encryption algorithm was proposed. Multiple grayscale images were fused into a color image using different channels. Then, the color image was scrambled and diffused in order to obtain a more secure cipher image [60]. The authors compared symmetric and asymmetric discretization approaches, applying them to several examples of Hamiltonian systems. In particular, they suggested symmetric modifications.
of Chirikov and H’enon maps and show explicitly that the implied symmetric integration procedure yields reflectional symmetry in the phase space [61,62].

3. Proposed Model

In this section, the proposed encryption technique is presented for healthcare data. A hyper-chaotic system is used to obtain more chaotic keys. These keys are then used to permute and diffuse the biomedical images. Zero-watermarking temper is used to detect the attacks attempt on the biomedical data. The ‘Rivest–Shamir–Adleman’ algorithm (RSA) is used to encrypt or decrypt the confidential data of e-healthcare data in the form of images with the use of two different keys.

3.1. Hyper-Chaotic System

In a hyper-chaotic system, there are four dimensional states that can be mathematically defined as Equation (1):

\[
\begin{align*}
    x_{i+1} &= a(y_i - x_i) \\
    y_{i+1} &= bx_i - x_i z_i - u_i \\
    z_{i+1} &= -cz_i + x_i y_i \\
    u_{i+1} &= d(x_i + y_i)
\end{align*}
\]

(1)

Here, \(x_i, y_i, z_i,\) and \(u_i\) denote the main factors of a hyper-chaotic system. There are legitimate parameters, i.e., \(a, b, c,\) and \(d\). For experimental purpose, the values of \(a, b, c,\) and \(d\) are 33.8, 43.33, 2.4, and 10.4, respectively. The corresponding chaotic behavior is shown in Figure 2.

Figure 2. Hyper-Chaotic Attractors.

3.2. Image Encryption Algorithm

To achieve better results, initially, gray code conversion is used. It has a single encoding rule which utilizes the slightest bit distinction between two contiguous codes. The
technique for changing the common parallel code of bit \( j \) to a run-of-the-mill dim code can be represented as Equation (2):

\[
G_{r}(i) = B_n(i) \quad i = j - 1 \\
G_{r}(i) = B_n(i + 1) \oplus B_n(i), \quad 0 \leq i < j - 1 \\
G_{r}(i) = B_n(i) \quad i = j - 1
\] (2)

Here, \( G_{r}(i) \) is a common dim code. \( B_n(i) \) is a characteristic paired code. \( \oplus \) represents an elite operator. An average n-bit dark code can be changed into a characteristic paired code as Equation (3):

\[
B_n(i) = G_{r}(i) \quad i = N - 1 \\
B_n(i) = G_{r}(i) \oplus B_n(i + 1), \quad 0 \leq i < N - 1
\] (3)

The main scrambled gray code cycle change times are determined by the size of the shading image, as Equation (4):

\[
S_0 = \text{mod} ((L_e + W_d), 7) + 1
\] (4)

Here, \( L_e \) and \( W_d \) denote the length and width of the image pixels, respectively.

As per the boundaries \( a, b, c, \) and \( m, \) the starting characteristics, i.e., \( x_o, y_o, z_o, \) and \( u_o, \) and the four scattered authentic worth groupings of \( x, y, z, \) and \( u \) are evaluated. Four tumult real-worth groupings are changed over into a 1D system. To diminish the impact of basic motivation on the model, the past no outcomes are avoided, and a 1D tumult progression Chi could be delivered \((C = 1, 2, \ldots, n \times m \times 3). \) It can be computed as Equation (5):

\[
n_0 = \left[ (R' + G' + B') \times r \right]
\] (5)

Here, \( R, G, \) and \( B \) represent the ordinary pixel estimations. A 3D diminish code is changed over to a 1D cross-section \( P_i; \) by then, a 1D dislocated system \( C_i \) in a state of harmony is orchestrated and \( P_i \) changes positions at the same time. It scrambles the entire image. For the spread image of Sanchi, there is a correlation among neighboring pixels and every shading segment part. The diffusion process disturbs the connection between closed pixels, and yet it modifies the association among color shading segment parts to obtain an unrivaled scrambling sway. Regardless of the way that the histograms of each shading segment part have been altered to some degree, the histogram estimations of the image with everything taken into account are not modified. The histograms of each section are not uniform; subsequently, further encryption is, up until now, required. To adjust the histogram and hide the quantifiable data of plain text, this count utilizes the progression created by a hyper-wild structure to diffuse the pixel estimation of the image. With hyper-plane succession, changing the pixel involves discretizing it as Equation (6) to obtain the key stream.

\[
D_e = \text{mod}(\text{round}(\text{abs}(C_e)), 256)
\] (6)

3.3. ZeroWatermarking for the Cover Image

In zero watermarking, let \( F \) be the parallel substance highlight framework of the first cover image \( I. \) In powerful zero watermarking, let \( F_m \) be the paired substance including the lattice of the first cover image \( C, \) let \( L \) be the first double watermark image, and \( F_m' \) be the twofold substance highlight grid of the assaulted cover image \( C', \) and at that point the checked, paired watermark image is \( L'. \) It can be computed as in Equation (7):

\[
L' = (L \oplus F_m) \oplus F_m' = Z_w \oplus F_m
\] (7)

This zero-watermarking computation can be portrayed by using the zero-watermark age strategy and revelation process. Disregard \( C \) and \( L, \) and let the main concealing image have a size of \( m \times n \) and the matched watermark image have the size \( R \times S, \) exclusively.
$Z_W$ is the signal of the zero-watermark technique and $\oplus$ implies the prohibition of action. The restriction of activity is utilized in the zero-watermark age process $(L \oplus F_m)$ and the robust zero-watermark proof-distinguishing procedure $(Zw \oplus F_m)$. $F_m$, $F'_m$, $L$, and $L'$ are all in all twofold structures with a comparable size. If $F_m$ and $F'_m$ are closer, by then, $L$ and $L'$ are closer. Ideally, $L'$ is undefined from $L$ when $F'_m$ is equal to $F_m$. This region delineates every movement using our proposed technique, i.e., the zero-watermarking technique. The implemented zero-watermarking computation will be depicted by two strategies: the first one is the robust zero-watermark age and the second one is the revelation method. The first hiding images, gives the images a size of $m \times n$, while the coordinated size of the watermark image/image is $R \times S$ only.

The stream diagram is represented in Figure 3, and the crucial advances are portrayed as:

- **Stage 1:** Decompose the color image into R, G, and B channels.
- **Stage 2:** With the rotting of DWT, the sub-gatherings and division, which computes the color channels, are decomposed using 2DDWT with the Haar channel and 3 related low-repeat parts, $RLL_1, GLL_1$ and $BLL_1$, with a size of $(m/2) \times (n/2)$. Thereafter, the computed DWT channels are parceled into non-covering squares $B_{i,k}$ with sizes $b \times b$ and $k = 1, 2, 3, \ldots, R \times S$, while I has a spot with the color channels. The amount of non-covering squares is $R \times S$.
- **Stage 3:** Computation of the square vitality highlights and the normal vitality highlights of the single channel: The single value decomposition (SVD) method has utilized three segments ($RLL_1, GLL_1$, and $BLL_1$) and all squares $B_{i,k}$. SVD method decomposes the RGB channels. It has some algebraic properties that give insights into linear transformations. The vitality includes the $EF_{i,k}$ of every square $B_{i,k}$, and is processed by its solitary qualities, as indicated by (8). The normal vitality feature $AEF^i$ of every part is determined by relating the solitary qualities as far as (9), which is obtained from the traditional force mean.

$$EF_{i,k} = \sqrt{\sum_{j=1}^{r} (\sigma_{i,j})^2} \quad k = 1, 2, 3; \ldots \ldots \ldots \ldots R \times S; \ \text{i} \in \{R, G, B\} \quad (8)$$

$$AEF^i = \sqrt{\sum_{i=1}^{S} (\sigma_i)^2} \quad \frac{1}{\sqrt{R \times S}} \quad \text{i} \in \{R, G, B\} \quad (9)$$

where $\sigma_j$ is the singular value of the corresponding matrix. Here, the singular numbers of the values is $R$ and $S$, which are put in the equation.

- **Stage 4:** Comparison between the square vitality and normal vitality highlights of the single channel: To investigate the neural affective activations during handshakes, we demonstrated that a handshake conveying gentle or aggressive tactile vitality forms produces a stronger activation of the dorso-central insula. The dorso-central insula is activated during imagining as well as during the execution of actions conveying a gentle or rude vitality form. The insula controls autonomic functions through the regulation of the sympathetic and parasympathetic systems. It has a role in regulating the immune system. For each channel, a double trademark network is produced by looking at the vitality, including the $EF_{i,k}$ of each square and the traditional vitality highlight $AEF^i$ of the comparing channel, as in (10). The rise of convolution neural networks, accompanying residual learning, has paved the way for the development of single image super resolution (SISR). With the massive number of stacked residual blocks (RBs), the existing deep single image super resolution (SR) models have achieved a great breakthrough in accuracy. However, they cannot be easily utilized to real applications, given their high computational complexity and memory storage. Three channels can be delivered twofold attribute grids as (1) BCHR, (2) BCHG, and (3) BCHB.
\[ \text{BCH}_i = \begin{cases} 1 & \text{if } \text{EF}_{i,k} > \	ext{AEF}_i \\ 0 & \text{otherwise} \end{cases} \quad k = 1, 2, 3, \ldots \ldots \ldots \ R \times S, \ i \in R, G, B \quad (10) \]

- Stage 5: Construction of parallel element network: Two parallel attention modules are used to model the semantic interdependencies in position and channel dimensions, respectively, for scene segmentation. Due to the effectiveness of attention models, we also embed the attention mechanism into the lattice block to combine the RBs adaptively. For a unique cover image, a double component network bond fluctuation model (BFM) (Equation (11)) can be obtained by the larger part casting a ballot of three twofold trademark frameworks using the Bose–Chaudhuri–Hochquenghem code (BCH code) Equation (12). BCHR (BCH-Red), BCHG(BCH-Green), and BCHB(BCH-Blue) are used as in [19,20].

\[ \text{BCH}_{\text{mean}}(i,j) = \frac{[\text{BCH}_R(i,j) + \text{BCH}_G(i,j) + \text{BCH}_B(i,j)]}{3} \quad (11) \]

\[ \text{BFM} (i,j) = \begin{cases} 0 & \text{BCH}_{\text{mean}}(i,j) < 0.5 \\ 1 & \text{BCH}_{\text{mean}}(i,j) \geq 0.5 \end{cases} \quad (12) \]

Here, \((i,j)\) states the situation of a section in the parallel lattice. Most of Votes parts are chosen.

- Stage 6: Copyright images disarray: The parallel copyright image \(W_O\) of size \(P \times Q\) is mixed with \(W_S\) utilizing two decimal hyper-turbulent groupings produced by arrangements of the reasonable introductory states \((x_o, y_o, z_o, w_o)\) and parameter denotations \((r)\); those are viewed as keys K1 and K2.

- Stage 7: The mixed image is additionally encoded to \(W_E\) by a \(W_o\) fold hyper-disorganized succession created by appropriate introductory state \((x_o, y_o, z_o, w_o)\). Additionally, where the parameters have \((r)\), i.e., denotes the Key K3.

- Stage 8: The signal \(WZW\) of the zero watermark is delivered and checked by the performance of the elite -OR (XOR) process between the encoded watermark \(W_E\) and the equal component of the element network organizer BFM, as shown by (13). Along these lines, \(WZW\) corresponds to the primary spread image. Finally, the obtained \(WZW\), \(K_1\), \(K_2\), and \(K_3\) are selected and spared in the authorized advancement database for copyright affirmation. It can be evaluated as:

\[ W_{zw} = W_E \oplus \text{BFM} \quad (13) \]
3.4. Rivest–Shamir–Adleman (RSA) Algorithm

In 1978, a paper was distributed by R. Rivest, A. Shamir, and L. Adleman. This cryptosystem is known as the most famous cryptographic technique. This calculation method uses incredibly large numbers, which makes it safe. Today, RSA is used in cryptographic applications from banking and email security to online business on the internet.

From Figure 4, it is seen that if a cryptanalyst managed to break the key to the RSA algorithm, at that point, the subsequent stage to obtain the first image is to unravel the second encryption method, which is a chaos-based technique. This will cause the quality of the image to be guaranteed. With the use of the RSA algorithm, sensitive data are encrypted, which provides the best security from the other algorithm, and also it is very difficult to crack. The RSA involves factorization with the use of prime numbers; hence, this is more difficult to factorize as in Figure 5.

By applying RSA algorithm on a watermarked image, the robustness of the image becomes enhanced. The experimental results also proved the high PSNR value. Hence, RSA enhanced the security of the sensitive data shared over the network.
Figure 4. Encryption process of RSA.

Figure 5. Decryption process of RSA.

4. Performance

The proposed method is implemented in MATLAB 2021a with 16GB RAM on an i7 processor. The main role is to encrypt the confidential data. If any government/private department or any group wants to share their confidential data with the service of a CSP, the security level will go down or become worthless. With our implemented technique, we can share our data securely over the cloud and no hacker can crack or destroy/update the data.

Hence, by following our implemented technique, anyone can share their confidential data. Therefore, sharing images should be encrypted by our implemented technique.

To obtain the best results to share the data over the cloud securely, first, we downloaded different collections of images, those that are freely available through the internet, and we filtered the images, and we then selected the compatible image to use with the selected tools that are used in the research.

4.1. Performance Parameters

Peak signal-to-noise ratio (PSNR) is utilized to quantify the quality of the watermarked images. It can be computed as in Equation (14):

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}}$$  \hspace{1cm} (14)
Here, the mean-squared error (MSE) can be computed as in Equation (15):

\[
\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2
\]  

(15)

Here, I shows the input image. K shows the encrypted image. (i, j) denotes the pixel coordinates, and m, n shows size of the input image. Entropy is a well-known measure which indicates the degree of randomness in the image. The entropy (E) of an image can be computed as in Equation (16):

\[
E = \sum_{i=0}^{m-1} p(m_i) \log_2 \frac{1}{p(m_i)}
\]  

(16)

where, mᵢ, e, E, and mᵢ together denote the probability of image occasion mᵢ.

The attackers sometimes explore the relation among the adjacent pixels of an image for statistical attacks. Actually, the adjacent pixels of the plain image are highly correlated to each other in all three directions, such as horizontally (HC), vertically (VC), and diagonally (VC). This relation should be minimum so that no statistical information should be disclosed to the attackers. The relation among the adjacent pixels can be calculated as:

\[
r = \frac{\sum (x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum (x_i - \mu_x)^2(y_i - \mu_y)^2}}
\]  

(17)

Here, r is the correlation coefficient. x and y represent the adjacent pixels. \(\mu_x\) and \(\mu_y\) are the means of x and y, respectively. For this experiment, we randomly selected 3000 pairs of adjacent pixels (x; y) from plain and encrypted images. A palm X-ray image is taken for this test, as shown in Figure 6.

![Figure 6. Correlation analyses of encrypted palm X-ray watermarked image.](image)

### 4.2. Visual Analysis

This sub-portion shows the exploratory examination of the spread image. Figure 7 shows the spread image that was used for the image embeddings and isolating procedure. Figure 7a is the Sanchi image, which is considered to be as spread image. Figure 7b is the watermark image that is considered as a transmit image. The hyper-scattered key planned shading watermark image is shown in Figure 7c. The zero watermarking is performed on
the hyper-turbulent vital planned watermark image and the encoded Sanchi image, which is shown in Figure 7d. Figure 7e shows the mixed image in the wake of executing the RSA encryption estimation for the zero-watermarked image.

![Visual analysis: (a) Sanchi spread image, 512×512, (b) watermarked image, 256×256, (c) chaotic calculated planned watermarked image, (d) Sanchi watermarked image, (e) RSA-encrypted image.](image)

Figure 7. Visual analysis: (a) Sanchi spread image, 512 × 512, (b) watermarked image, 256 × 256, (c) chaotic calculated planned watermarked image, (d) Sanchi watermarked image, (e) RSA-encrypted image.

To test the robustness with standard grayscale medical images, palm X-ray, brain tumor, ultrasound, and chest X-ray images of size 256 × 256 are considered as the experimental images, as shown in Figure 8.

![Experimental images](image)

Figure 8. (a) Palm X-ray; (b) brain tumor; (c) ultrasound; (d) chest X-ray.

Using a secret key, a zero watermark is extracted from the attacked medical image and then compared with the original watermark for authenticity. To match the extracted zero watermark, normalized correlation coefficients (r) are estimated between the original and extracted zero watermarks, as shown in Equation (17).

4.3. Quantitative Analysis

Table 1 shows the performance evaluation of the proposed technique in terms of the PSNR between the actual and decrypted images. The PSNR between the actual and
decrypted images should be a maximum. It is clearly found that the proposed technique achieves remarkably better PSNR values as compared to the existing techniques. The proposed techniques show an average improvement in terms of PSNR of 3.4587%.

**Table 1.** Performance evaluation of color images in terms of PSNR between actual and decrypted images.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Palm X-ray</th>
<th>Brain Tumor</th>
<th>Ultrasound</th>
<th>Chest X-ray</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGAN [13]</td>
<td>56.62</td>
<td>47.31</td>
<td>40.16</td>
<td>51.86</td>
</tr>
<tr>
<td>VMKS [15]</td>
<td>56.52</td>
<td>43.77</td>
<td>47.51</td>
<td>52.99</td>
</tr>
<tr>
<td>PEC [4]</td>
<td>44.37</td>
<td>50.18</td>
<td>59.02</td>
<td>57.04</td>
</tr>
<tr>
<td>JJL [16]</td>
<td>58.21</td>
<td>52.55</td>
<td>51.12</td>
<td>59.32</td>
</tr>
<tr>
<td>SET [17]</td>
<td>57.12</td>
<td>56.94</td>
<td>43.53</td>
<td>57.02</td>
</tr>
<tr>
<td>SHE [18]</td>
<td>56.76</td>
<td>48.92</td>
<td>45.59</td>
<td>59.22</td>
</tr>
<tr>
<td>Proposed</td>
<td>59.41</td>
<td>58.14</td>
<td>60.22</td>
<td>60.52</td>
</tr>
</tbody>
</table>

Table 2 demonstrates the performance evaluation of the proposed technique in terms of PSNR between the actual and encrypted images. The PSNR between actual and decrypted images should be a minimum. It is clearly found that the proposed technique achieves remarkably lower PSNR values as compared to the existing techniques. The proposed techniques show an average reduction in terms of PSNR of 1.6478%.

**Table 2.** Performance evaluation of color images in terms of PSNR between actual and encrypted images.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Palm X-ray</th>
<th>Brain Tumor</th>
<th>Ultrasound</th>
<th>Chest X-ray</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGAN [13]</td>
<td>6.18</td>
<td>4.25</td>
<td>2.44</td>
<td>3.73</td>
</tr>
<tr>
<td>VMKS [15]</td>
<td>4.32</td>
<td>5.12</td>
<td>2.17</td>
<td>2.42</td>
</tr>
<tr>
<td>JJL [16]</td>
<td>1.64</td>
<td>3.45</td>
<td>5.99</td>
<td>8.55</td>
</tr>
<tr>
<td>SET [17]</td>
<td>5.05</td>
<td>6.92</td>
<td>4.61</td>
<td>4.32</td>
</tr>
<tr>
<td>SHE [18]</td>
<td>3.29</td>
<td>4.94</td>
<td>5.31</td>
<td>2.08</td>
</tr>
<tr>
<td>Proposed</td>
<td>1.44</td>
<td>2.25</td>
<td>1.97</td>
<td>1.88</td>
</tr>
</tbody>
</table>

Table 3 shows the performance evaluation of the proposed technique in terms of the entropy of the encrypted images. It should be at its maximum. It is clearly found that the proposed technique achieves remarkably better entropy values as compared to the existing techniques. The proposed techniques show an average improvement in terms of entropy of 0.8978%.

**Table 3.** Performance evaluation of color images in terms of entropy.

<table>
<thead>
<tr>
<th>Technique</th>
<th>Palm X-ray</th>
<th>Brain Tumor</th>
<th>Ultrasound</th>
<th>Chest X-ray</th>
</tr>
</thead>
<tbody>
<tr>
<td>CGAN [13]</td>
<td>7.76</td>
<td>7.26</td>
<td>7.54</td>
<td>7.6</td>
</tr>
<tr>
<td>PEC [4]</td>
<td>7.21</td>
<td>7.72</td>
<td>7.5</td>
<td>7.07</td>
</tr>
<tr>
<td>JJL [16]</td>
<td>7.65</td>
<td>7.37</td>
<td>7.03</td>
<td>7.43</td>
</tr>
<tr>
<td>SET [17]</td>
<td>7.6</td>
<td>7.7</td>
<td>7.52</td>
<td>7.53</td>
</tr>
<tr>
<td>SHE [18]</td>
<td>7.16</td>
<td>7.53</td>
<td>7.55</td>
<td>7.14</td>
</tr>
<tr>
<td>Proposed</td>
<td>7.59</td>
<td>7.53</td>
<td>7.38</td>
<td>7.43</td>
</tr>
</tbody>
</table>

Table 4 shows that there is no correlation among the adjacent pixels of the encrypted medical grayscale images. It can be seen that the pixels are loosely correlated to each other. Hence, no attacker can extract the statistical information to recover the encrypted images.
Table 4. Correlation coefficient of the encrypted medical images.

<table>
<thead>
<tr>
<th>Encrypted Images</th>
<th>Horizontal Correlation</th>
<th>Vertical Correlation</th>
<th>Diagonal Correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Palm X-ray</td>
<td>0.0045</td>
<td>0.0056</td>
<td>0.0034</td>
</tr>
<tr>
<td>Brain Tumor</td>
<td>0.0021</td>
<td>0.0015</td>
<td>0.0010</td>
</tr>
<tr>
<td>Ultrasound</td>
<td>0.0005</td>
<td>0.0013</td>
<td>0.0036</td>
</tr>
<tr>
<td>Chest X-Ray</td>
<td>0.0037</td>
<td>0.0088</td>
<td>0.0078</td>
</tr>
</tbody>
</table>

5. Conclusions

In this paper, we have proposed a hybrid technique to encrypt the confidential data related to e-healthcare. The hyper-chaotic method and zero-watermarking techniques along with RSA are hybridized to encrypt the data. The proposed technique has been used to secure the communication of multimedia data over 6G networks. Initially, multimedia data are encrypted by using the proposed model. Thereafter, the encrypted data are then transferred over the 6G networks. The proposed techniques have significantly increased the key size. Therefore, the proposed technique can resist various security attacks. Extensive experimental analysis reveals that the proposed technique outperforms the competitive techniques in terms of entropy and PSNR.

In future we will apply deep learning applications for developing secure and efficient image encryption, authentication, and good imperceptibility of the watermarked images.

Author Contributions: J.J. proposed the methodology and its implementation, A.J. conducted the literature work and conceptualization, S.K.S. validated the proposed work and led the project administration, C.V. performed the quantitative analysis of the proposed work, Z.I. performed the qualitative investigation of the proposed work, and M.S.R. led the funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This project is funded by the Ministry of Research, Innovation and Digitization through Program 1-Development of the national research and development system, Subprogram 1.1. Institutional performance-Projects to finance excellence in RDI, Contract No. 19PFE/30.12.2021 and a grant of the National Center for Hydrogen and Fuel Cells (CNHPC) — Installations and Special Objectives of National Interest (IOSIN).


Informed Consent Statement: Not Applicable.


Acknowledgments: The work of Chaman Verma and Zoltán Illés was supported under “ÚNKpv MIT (Ministry of Innovation and Technology) and National Research, Development and Innovation (NRDI) Fund, Hungarian Government” and Co-financed by the European Social Fund under the project “Talent Management in Autonomous Vehicle Control Technologies (EFOP-3.6.3-VEKOP-16-2017-00001).”

Conflicts of Interest: The authors declare that they have no conflict of interest to report regarding the present study.

References


35. Yoo, Y.; Baek, J.G. A novel image feature for the remaining useful life time prediction of bearings based on continuous wavelet transform and convolutional neural network. *Appl. Sci.* 2018, 8, 1102. [CrossRef]


