mathematics

MDPI

Article

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, Ștefan cel Mare University, 720229 Suceava, Romania
[6] Doctoral School, Polytechnic University of Bucharest, 313 SplaiulIndependentei, 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

Citation: Jain, J.; Jain, A.; Srivastava, S.K.; Verma, C.; Raboaca, M.S.; Illés, Z. Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA. *Mathematics* **2022**, *10*, 1071. https://doi.org/10.3390/math10071071

Academic Editor: Angel Martín-del-Rey

Received: 17 February 2022
Accepted: 22 March 2022
Published: 26 March 2022

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.

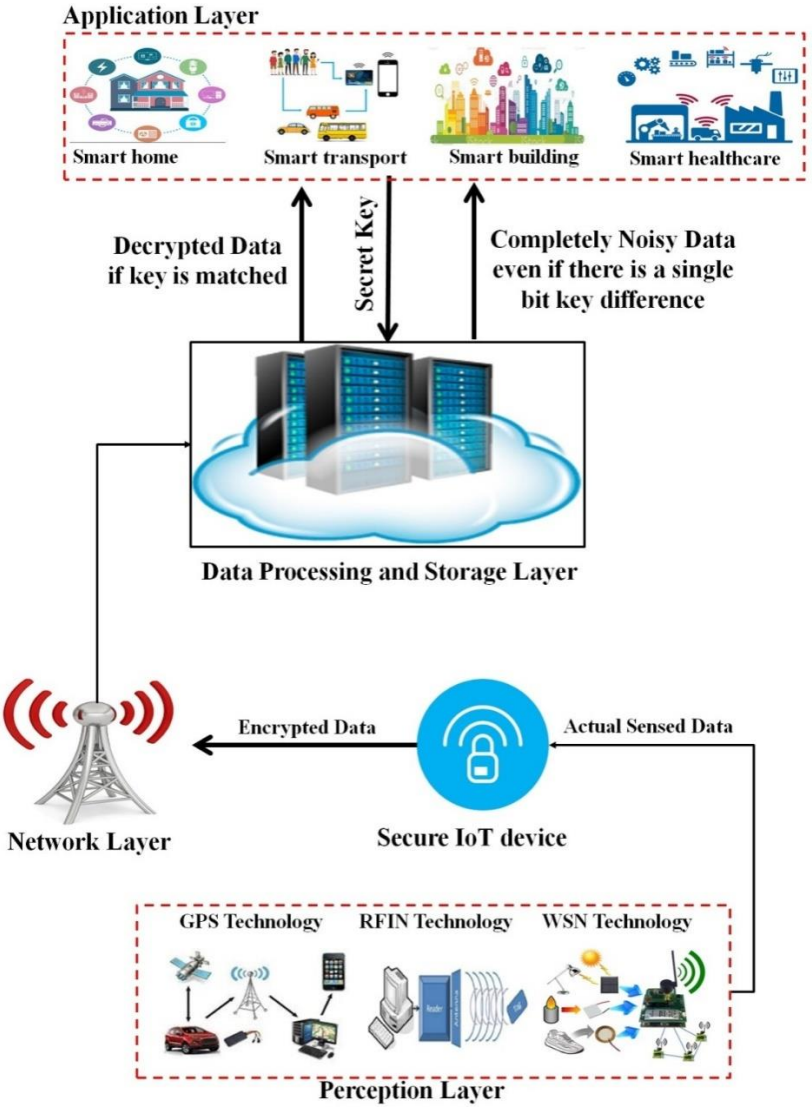

Figure 1. Proposed 6G-enabled secure IOT network [10].

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], Hadded et al. used joint watermarking-encryption-JPEG-LS (JJL) 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 usedto 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):

$$\begin{aligned} x_{i+1} &= a(y_i - x_i) \\ y_{i+1} &= bx_i - x_i z_i - u_i \\ z_{i+1} &= -cz_i + x_i y_i \\ u_{i+1} &= d(x_i + y_i) \end{aligned} \tag{1}$$

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.

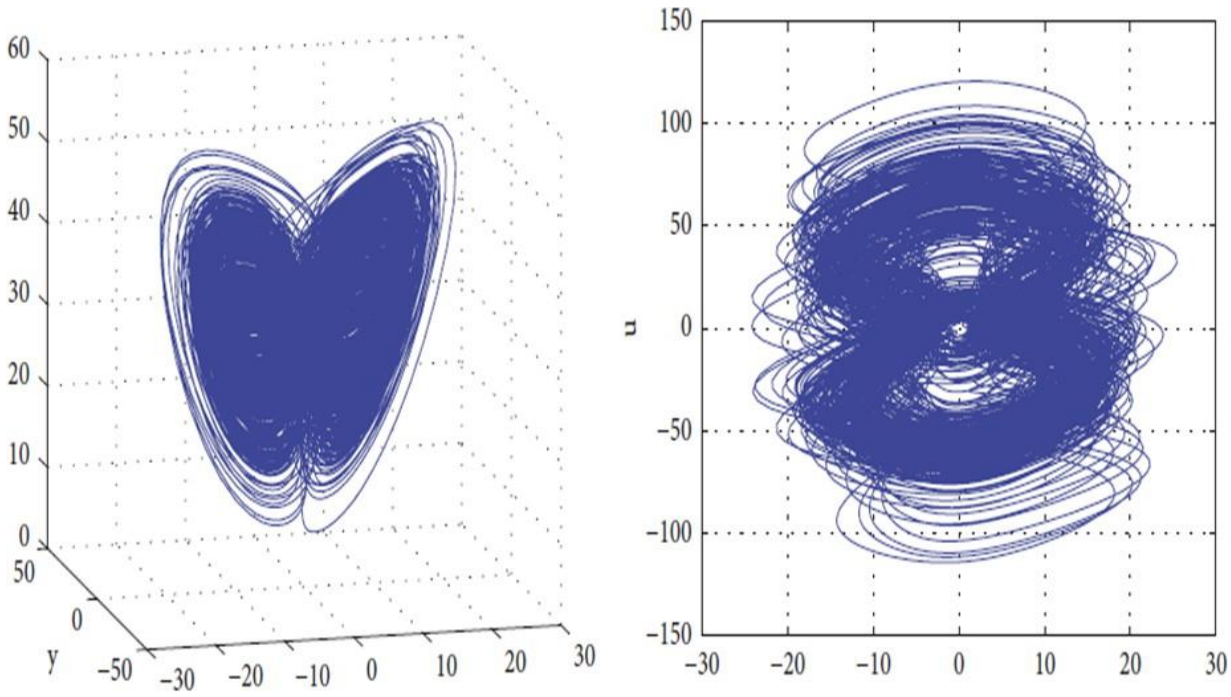

Figure 2. Hyper-Chaotic Attractors.

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):

$$\begin{array}{cc} G_r(i) = B_n(i) & i = j - 1 \\ G_r(i) = B_n(i+1) \oplus B_n(i), & 0 \leq i < j - 1 \\ G_r(i) = B_n(i) & i = j - 1 \end{array} \quad (2)$$

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):

$$\begin{array}{cc} B_n(i) = G_r(i) & i = N - 1 \\ B_n(i) = G_r(i) \oplus B_n(i+1), & 0 \leq i < N - 1 \end{array} \quad (3)$$

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

$$S_o = \text{mod}\ ((L_e + W_d), 7) + 1 \quad (4)$$

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,....., n × m × 3). It can be computed as Equation (5):

$$n_o = [(R' + G' + B') \times ro] \quad (5)$$

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.

$$D_e = \text{mod}((\text{round}(\text{abs}(Ce)), 256) \quad (6)$$

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 Fm′ 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):

$$L' = (L \oplus F_m) \oplus F_{m'} = Z_w \oplus F_m \quad (7)$$

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 × n and the matched watermark image have the size R × 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 $\oplus$Fm) and the robust zero-watermark proof-distinguishing procedure (Zw$\oplus$ Fm). Fm, F′m, L, and L′ are all in all twofold structures with a comparable size. If Fm and F′ m are closer, by then, L and L′ are closer. Ideally, L′ is undefined from L when F′m is equal to Fm. 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 × n, while the coordinated size of the watermark image/image is R × 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) × (n/2). Thereafter, the computed DWT channels are parceled into non-covering squares $B_{i,k}$ with sizes b × b and k = 1, 2, 3,..., R × S, while I has a spot with the color channels. The amount of non-covering squares is R × 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 (RLL1, GLL1, and BLL1) 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.

$$EF^{ik} = \sqrt{\sum_{ij}^{r} (\sigma_j^{ik})^2}\ k = 1,\ 2,\ 3; \ldots\ldots\ldots\ldots\ldots R \times S;\ i\varepsilon\{R, G, B\} \tag{8}$$

$$AEF^i = \frac{\sqrt{\sum_{j=1}^{5} (\sigma_j^i)^2}}{\sqrt{R \times S}}\ i\ \varepsilon\{R,\ G,\ B\} \tag{9}$$

where σ_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.

$$BCH_i = \begin{cases} 1 & \text{if } EF^{i,k} > AEF^i \\ 0 & \text{otherwise} \end{cases} \qquad k = 1, 2, 3, \ldots\ldots\ldots R \times S,\ i \in R, G, B \quad (10)$$

- 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].

$$BCH_{mean(i,j)} = [BCH_R(i,j) + BCH_G(i,j) + BCH_B(i,j)]/3 \quad (11)$$

$$BFM\ (i,j) = \begin{cases} 0 & BCH_{mean(i,\ j)} < 0.5 \\ 1 & BCH_{mean(i,\ j)} \geq 0.5 \end{cases} \quad (12)$$

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 × Q is mixed with W_S utilizing two decimal hyper-turbulent groupings produced by arrangements of the reasonable introductory states (xo, yo, zo, and wo) 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 W_{ZW} 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, W_{ZW} corresponds to the primary spread image. Finally, the obtained W_{ZW}, K_1, K_2, and K_3 are selected and spared in the authorized advancement database for copyright affirmation. It can be evaluated as:

$$W_{zw} = W_E \oplus BFM \quad (13)$$

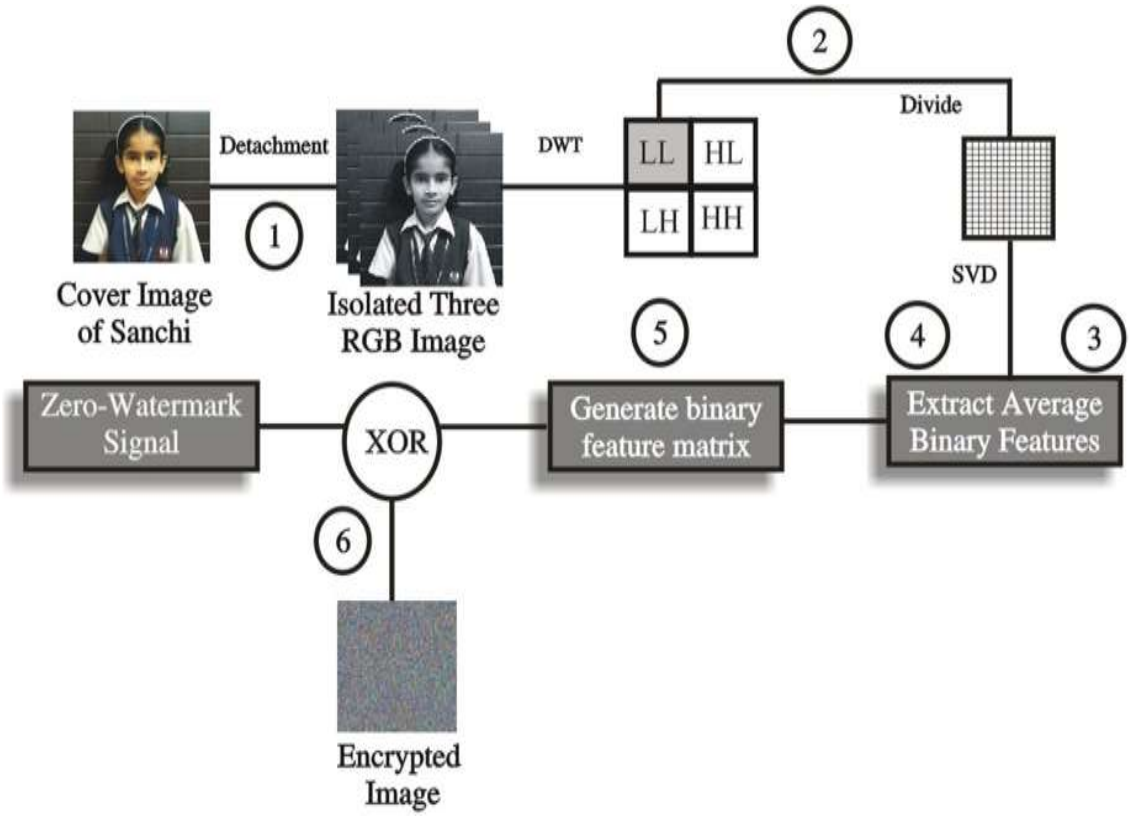

Figure 3. Block Diagram of Watermark Detection Process.

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.

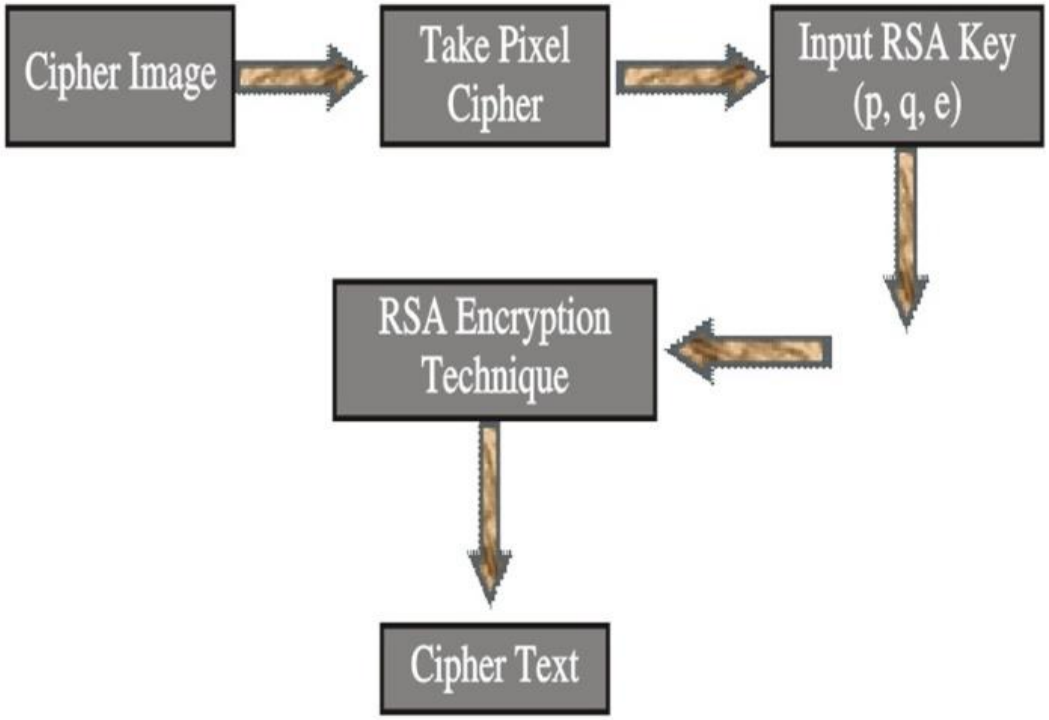

Figure 4. Encryption process of RSA.

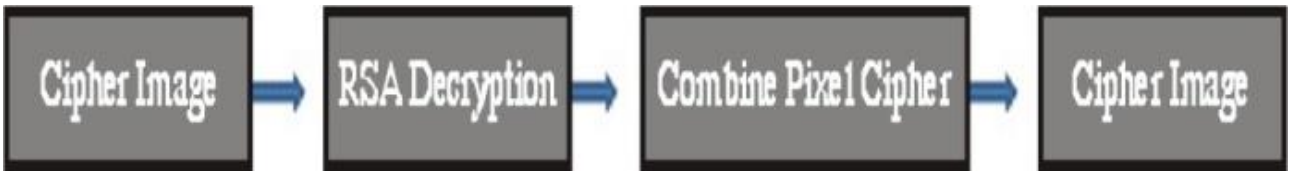

Figure 5. Decryption process of RSA.

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):

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \tag{14}$$

Here, the mean-squared error (MSE) can be computed as in Equation (15):

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (15)$$

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 thedegree of randomness in the image. The entropy (E) of an image can be computed as in Equation (16):

$$E = \sum_{i=0}^{m-1} p(m_i) \log_2 \frac{1}{p(m_i)} \quad (16)$$

where, m_i, ε, E, and m_i together denote the probability of image occasion m_i.

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:

$$r = \frac{\sum (x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum (x_i - \mu_x)^2 (y_i - \mu_y)^2}} \quad (17)$$

Here, r is the correlation coefficient. x and y represent the adjacent pixels. μ_x and μ_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.

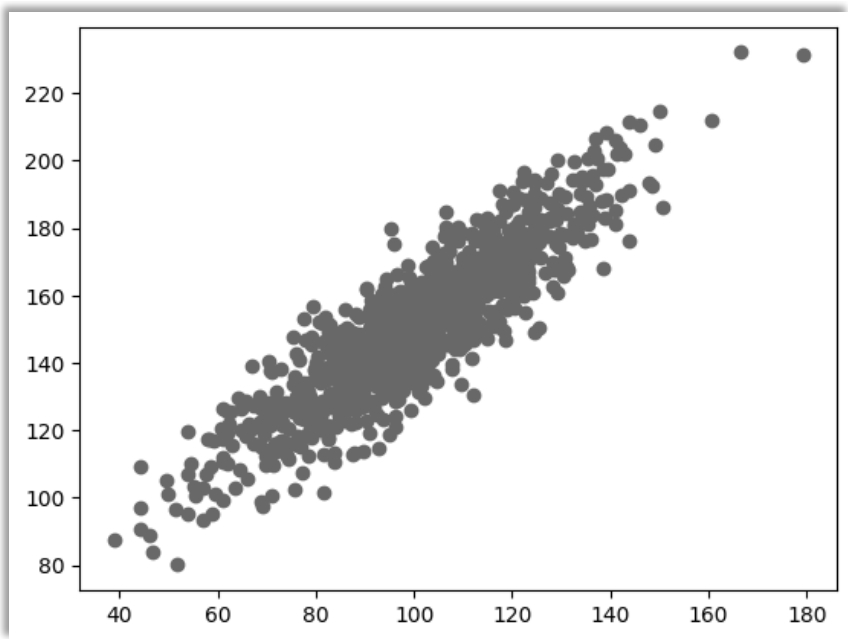

Figure 6. Correlation analyses of encrypted palm X-ray watermarked image.

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.

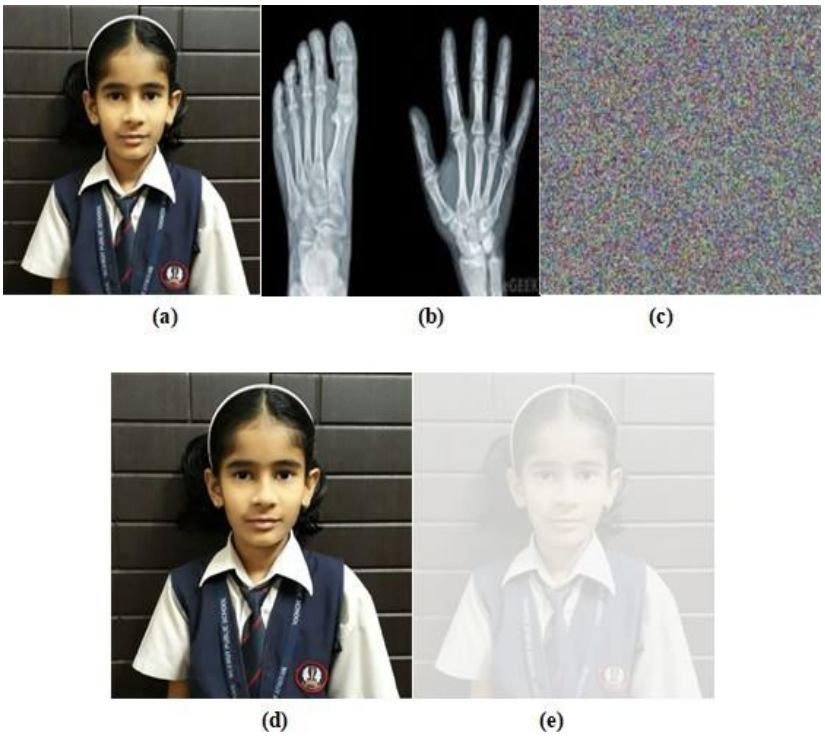

Figure 7. Visual analysis: (**a**) Sanchi spread image, 512 × 512, (**b**) watermarked image, 256 × 256, (**c**) chaotic calculated planned watermarked image, (**d**) Sanchi watermarked image, (**e**) RSA-encrypted image.

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.

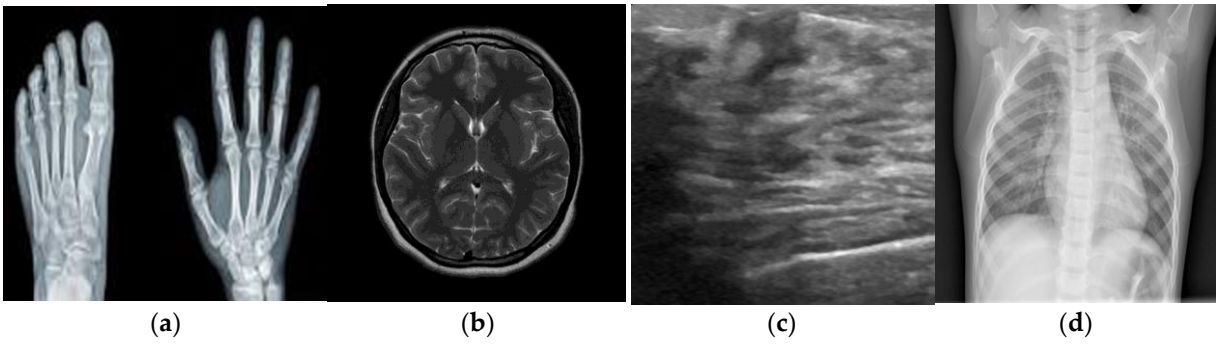

Figure 8. (**a**) Palm X-ray; (**b**) brain tumor; (**c**) ultrasound; (**d**) chest X-ray.

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 185 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.

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

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.

Technique	Palm X-ray	Brain Tumor	Ultrasound	Chest X-ray
CGAN [13]	6.18	4.25	2.44	3.73
VMKS [15]	4.32	5.12	2.17	2.42
PEC [4]	4.57	4.55	6.58	3.61
JJL [16]	1.64	3.45	5.99	8.55
SET [17]	5.05	6.92	4.61	4.32
SHE [18]	3.29	4.94	5.31	2.08
Proposed	1.44	2.25	1.97	1.88

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.

Technique	Palm X-ray	Brain Tumor	Ultrasound	Chest X-ray
CGAN [13]	7.76	7.26	7.54	7.6
VMKS [15]	7.51	7.59	7.45	7.39
PEC [4]	7.21	7.72	7.5	7.07
JJL [16]	7.65	7.37	7.03	7.43
SET [17]	7.6	7.7	7.52	7.53
SHE [18]	7.16	7.53	7.55	7.14
Proposed	7.59	7.53	7.38	7.43

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.

Encrypted Images	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Palm X-ray	0.0045	0.0056	0.0034
Brain Tumor	0.0021	0.0015	0.0010
Ultrasound	0.0005	0.0013	0.0036
Chest X-Ray	0.0037	0.0088	0.0078

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).

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: In this research, the image chosen as the cover image is my daughter's image, and other datasetsare freely available at https://www.istockphoto.com/photos/palm-x-ray; https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia; https://www.kaggle.com/navoneel/brain-mri-images-for-brain-tumor-detection; https://www.kaggle.com/aryashah2k/breast-ultrasound-images-dataset.

Acknowledgments: The work of Chaman Verma and Zoltán Illés was supported under "ÚNKP, 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

1. He, D.; Chan, S.; Tang, S. A novel and light weight system to secure wireless medical sensor networks. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 316–326. [CrossRef] [PubMed]
2. Jain, J.; Singh, A. Quantum-based rivest–shamir–adleman (rsa) approach for digital forensic reports. *Mod. Phys. Lett. B* **2020**, *34*, 2050085. [CrossRef]
3. Kaur, M.; Singh, D.; Kumar, V.; Gupta, B.B.; El-Latif, A.A.A. Secure and energy efficient- based e-healthcare framework for green internet of things. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 1223–1231. [CrossRef]

4. Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy protection for wireless medical sensor data. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 369–380. [CrossRef]
5. Jain, J.; Singh, A. Structure of cloudsim toolkit with cloud. *Int. J. Eng. Adv. Technol.* **2019**, *8*, 4644–4649. [CrossRef]
6. Kaur, M.; Singh, D.; Uppal, R.S. Parallel strength pare to evolutionary algorithm-ii based image encryption. *IET Image Processing* **2020**, *14*, 1015–1026. [CrossRef]
7. Ribeiro, L.S.; Viana-Ferreira, C.; Oliveira, J.L.; Costa, C. Xds-I outsourcing proxy: Ensuring confidentiality while preserving interoperability. *IEEE J. Biomed. Health Inform.* **2014**, *18*, 1404–1412. [CrossRef]
8. Jain, J.; Singh, A. Modern and advanced direction on green cloud. *J. Eng. Adv. Technol.* **2019**, *9*, 3090–3095. [CrossRef]
9. Dargan, S.; Kumar, M.A. Comprehensive survey on the biometric recognition systems based on physiological and behavioralmodalities. *Expert Syst. Appl.* **2020**, *143*, 113114. [CrossRef]
10. Drozdowski, P.; Rathgeb, C.; Dantcheva, A.; Damer, N.; Busch, C. Demographic bias in biometrics: A survey on an emerging challenge. *IEEE Trans. Technol. Soc.* **2020**, *1*, 89–103. [CrossRef]
11. Alonso-Fernandez, F.; Farrugia, R.A.; Bigun, J.; Fierrez, J.; Gonzalez-Sosa, E.A. Survey of super- resolution in iris biometrics with evaluation of dictionary-learning. *IEEE Access* **2019**, *7*, 6519–6544. [CrossRef]
12. Czajka, A.; Bowyer, K.W. Presentation attack detection for iris recognition: An assessment of the state-of-the art. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 1–35. [CrossRef]
13. Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. Deepedn: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [CrossRef]
14. Wang, F.; Feng, J.; Zhao, Y.; Zhang, X.; Zhang, S.; Han, J. Joint activity recognition and indoor localization with wifi fingerprints. *IEEE Access* **2019**, *7*, 80058–80068. [CrossRef]
15. Liu, X.; Yang, X.; Luo, Y.; Zhang, Q. Verifiable multi- keyword search encryption scheme with anonymous key generation formedical internet of things. *IEEE Internet Things J.* **2021**, 1. [CrossRef]
16. Haddad, S.; Coatrieux, G.; Moreau-Gaudry, A.; Cozic, M. Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2556–2569. [CrossRef]
17. Qiu, H.; Qiu, M.; Liu, M.; Memmi, G. Secure health data sharing for m edical cyber-physical systems for the healthcare 4.0. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2499–2505. [CrossRef]
18. Jiang, L.; Chen, L.; Giannetsos, T.; Luo, B.; Liang, K.; Han, J. Towards practical privacy-preserving processing over encrypted data in IOT: An assistive healthcare use case. *IEEE Internet Things J.* **2019**, *6*, 10177–10190. [CrossRef]
19. Puriwat, W.; Tripopsakul, S. Explaining an adoption and continuance intention to use contactless payment technologies: During the COVID-19 pandemic. *Emerg. Sci. J.* **2021**, *5*, 85–95. [CrossRef]
20. Park, U.; Ross, A.; Jain, A.K. Periocular biometrics in the visible spectrum: A feasibility study. In Proceedings of the 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, Washington, DC, USA, 28–30 September 2019; IEEE: Piscataway, NJ, USA, 2009; pp. 1–6.
21. Park, U.; Jillela, R.R.; Ross, A.; Jain, A.K. Periocular biometrics in the visible spectrum. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 96–106. [CrossRef]
22. Alonso-Fernandez, F.; Bigun, J. Eye detection by complex filtering for periocular recognition. In Proceedings of the 2nd International Workshop on Biometrics and Forensics, Valletta, Malta, 27–28 March 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 1–6.
23. Kumari, P.; Seeja, K. Periocular biometrics: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2019**, *91*, 11. [CrossRef]
24. Nigam, I.; Vatsa, M.; Singh, R. Ocular biometrics: A survey of modalities and fusion approaches. *Inf. Fusion* **2015**, *26*, 1–35. [CrossRef]
25. Tiong, L.C.O.; Teoh, A.B.J.; Lee, Y. Periocular recognition in the wild with orthogonal combination of local binary coded patternindual-stream convolutional neural network. In Proceedings of the 2019 International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
26. Raffei, A.F.M.; Sutikno, T.; Asmuni, H.; Hassan, R.; Othman, R.M.; Kasim, S.; Riyadi, M.A. Fusion iris and periocular recognitions in non-cooperative environment. *Indones. J. Electr. Eng. Inform.* **2019**, *7*, 543–554.
27. Kumar, K.K.; Pavani, M. Periocular region-based age-invariant face recognition using local binary pattern. In *Microelectronics, Electromagnetics and Telecommunications*; Springer: Andhra Pradesh, India, 2019; pp. 713–720.
28. Bshi, S.; Sa, P.K.; Wang, H.; Barpanda, S.S.; Majhi, B. Fast periocular authentication in handheld devices with reduced phase intensive local pattern. *Multimed. Tools Appl.* **2018**, *77*, 17595–17623.
29. Castrillon-Santana, M.; Lorenzo-Navarro, J.; Ramon-Balmaseda, E. On using periocular biometric for gender classification in the wild. *Pattern Recognit. Lett.* **2016**, *82*, 181–189. [CrossRef]
30. Zhao, Z.; Kumar, A. Accurate periocular recognition under less constrained environment using semantics assisted convolutional neural network. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1017–1030. [CrossRef]
31. Mustaqeem Kwon, S. ACNN-assisted enhanced audio signal processing for speech emotion recognition. *Sensors* **2020**, *20*, 183. [CrossRef]
32. Merkow, J.; Jou, B.; Savvides, M. A nexploration of gender identification using only the periocular region. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 1–5.

33. Chahla, C.; Snoussi, H.; Abdallah, F. Dornaika, Discriminant quaternion local binary pattern embedding for personre-identification through prototype formation and colorcategorization. *Eng. Appl. Artif. Intell.* **2017**, *58*, 27–33. [CrossRef]
34. Zhou, Q.; Fan, H.; Yang, H.; Su, H.; Zheng, S.; Wu, S.; Ling, H. Robust and efficient graph correspondence transfer for personre-identification. *IEEE Trans. Image Processing* **2021**, *30*, 1623–1638. [CrossRef]
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]
36. Tan, X.; Triggs, B. Fusing gabor and lbp features ets for kernel-based face recognition. In Proceedings of the International Workshop on Analysis and Modeling of Faces and Gestures, Rio de Janeiro, Brazil, 20 October 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 235–249.
37. Koushkaki, H.R.; Salehi, M.R.; Abiri, E. Color-based feature extraction with application of facial recognition using tensor-matrix and tensor-tensor analysis. *Multimed. Tools Appl.* **2020**, *79*, 5829–5858. [CrossRef]
38. Li, M.; Yuan, X. Adaptive segmentation-based feature extraction and S-STDM watermarking method for color image. *Neural Comput. Appl.* **2019**, *32*, 9181–9220. [CrossRef]
39. Akter, M.S.; Islam, M.R.; Iimura, Y.; Sugano, H.; Fukumori, K.; Wang, D.; Tanaka, T.; Cichocki, A. Multiband entropy-based feature-extraction method for automatic identification of epileptic focus based on high-frequency components inninterictalieeg. *Sci. Rep.* **2020**, *10*, 7044. [CrossRef] [PubMed]
40. Huang, D.; Shan, C.; Ardabilian, M.; Wang, Y.; Chen, L. Local binary patterns and its application to facial image analysis: A survey. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2011**, *41*, 765–781. [CrossRef]
41. Koh, J.E.; Acharya, U.R.; Hagiwara, Y.; Raghavendra, U.; Tan, J.H.; Sree, S.V.; Bhandary, S.V.; Rao, A.K.; Sivaprasad, S.; Chua, K.C.; et al. Diagnosis of retinal health in digital fundus images using continuous wavelet transform(cwt) and entropies. *Comput. Biol. Med.* **2017**, *84*, 89–97. [CrossRef]
42. Kiranyaz, S.; Avci, O.; Abdeljaber, O.; Ince, T.; Gabbouj, M.; Inman, D.J. 1d convolutional neural networks and applications: A survey. *Mech. Syst. Signal Processing* **2021**, *151*, 107398. [CrossRef]
43. LeCun, Y.; Bottou, L.; Bengio, Y.; Haffner, P. Gradient-based learning applied to document recognition. *Proc. IEEE* **1998**, *86*, 2278–2324. [CrossRef]
44. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. Imagenet classification with deep convolutional neural networks. *Adv. Neural Inf. Processing Syst.* **2012**, *25*, 1097–1105. [CrossRef]
45. Shamsaldin, A.S.; Fattah, P.; Rashid, T.A.; Al-Salihi, N.K. A study of the applications of convolutional neural networks. *J. Sci. Eng.* **2019**, *3*, 31–39.
46. Hosseini, M.S.; Araabi, B.N.; Soltanian-Zadeh, H. Pigmentmelanin: Pattern for iris recognition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 792–804. [CrossRef]
47. Proença, H.; Filipe, S.; Santos, R.; Oliveira, J.; Alexandre, L.A. The UBIRIS. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. *IEEE Trans. Pattern Anal. Mach. Intell.* **2009**, *32*, 1529–1535. [CrossRef] [PubMed]
48. Nordstrom, M.M.; Larsen, M.; Sierakowski, J.; Stegmann, M.B. The IMM face database. *Environment* **2003**, *22*, 1319–1331.
49. Haddad Paouh, H.; Dehghantanha, A.; Khayami, R.; Choo, K.K.R. A deep recurrent neural network-based approach for internet of thing small ware threat hunting. *Future Gener. Comput. Syst.* **2018**, *85*, 88–96. [CrossRef]
50. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *78*, 544–546. [CrossRef]
51. Tan, C.-W.; Kumar, A. Towards online iris and periocular recognition under relaxed imaging constraints. *IEEE Trans. Image Processing* **2013**, *22*, 3751–3765. [CrossRef] [PubMed]
52. Jain, A.; Mittal, P.; Goswami, G.; Vatsa, M.; Singh, R. Person identification at a distance vacuolar biometrics. In Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015), Hong Kong, China, 23–25 March 2015; IEEE: Hyderabad, India, 2015; pp. 1–6.
53. Gangwar, A.; Joshi, A.; Sharma, R.; Saquib, Z. Person identification based on fusion of left and right periocular region. In Proceedings of the International ConferenceonSignal, ImageandVideoProcessing(ICSIVP2012), Daejeon, Korea, 13–15 January 2012; pp. 13–15.
54. Proenca, H.; Neves, J.C. A re mini scence of mastermind": Iris periocular biometrics by in-set cnn iterative analysis. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1702–1712. [CrossRef]
55. Kwon, S. Att-Net: Enhance demotion recognition system using light weight self-attention module. *Appl. Sci.* **2021**, *11*, 107101.
56. Jain, A.; Kumar, A. Desmogging of still smoggy images using a novel channel prior. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 1161–1177. [CrossRef]
57. Kumar, S.; Jain, A.; Kumar Agarwal, A.; Rani, S.; Ghimire, A. Object-Based Image Retrieval Using the U-Net-Based Neural Network. *Comput. Intell. Neurosci.* **2021**, *2021*, 4395646. [CrossRef]
58. Nepomuceno, E.G.; Nardo, L.G.; Arias-Garcia, J.; Butusov, D.N.; Tutueva, A. Image encryption based on the pseudo-orbits from 1 D chaotic map. *Chaos Interdiscip. J. Nonlinear Sci.* **2019**, *29*, 061101. [CrossRef]
59. Nard, L.G.; Nepomuceno, E.G.; Arias-Garcia, J.; Butusov, D.N. Image encryption using finite-precision error. *Chaos Solitons Fractals* **2019**, *123*, 69–78. [CrossRef]
60. Gao, X.; Yu, J.; Banerjee, S.; Yan, H.; Mou, J. A new image encryption scheme based on fractional-order hyper chaotic system and multiple image fusion. *Sci. Rep.* **2021**, *11*, 15737. [CrossRef] [PubMed]

61. Butusov, D.; Karimov, A.I.; Pyko, N.S.; Bogachev, M. Discrete chaotic maps obtained by symmetric integration. *Theory Tools Digit. Chaos Gener. Des.* **2018**, *509*, 955–970. [CrossRef]
62. Alshahrani, H.M. CoLL- IoT: A Collaborative Intruder Detection System for Internet of Things Devices. *Electronics* **2021**, *10*, 848. [CrossRef]