symmetry

MDPI

Article

Secure Surveillance Systems Using Partial-Regeneration-Based Non-Dominated Optimization and 5D-Chaotic Map

Gopal Ghosh [1], Kavita Verma [2], Divya Anand [1], Sahil Verma [2], Danda B. Rawat [3], Jana Shafi [4,*], Zbigniew Marszałek [5,*] and Marcin Woźniak [5]

1 School of Computer Science and Engineering, Lovely Professional University, Phagwara 144401, India; gopalsrm23@gmail.com (G.G.); divyaanand.y@gmail.com (D.A.)
2 Department of Computer Science and Engineering, Chandigarh University, Mohali 140413, India; kavita@ieee.org (K.V.); sahilverma@ieee.org (S.V.)
3 Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA; db.rawat@ieee.org
4 Department of Computer Science, College of Arts and Science, Wadi Ad-Dwasir Prince Sattam Bin Abdul Aziz University, Wadi Ad-Dawasir 18510, Saudi Arabia
5 Faculty of Applied Mathematics, Silesian University of Technology, 44100 Gliwice, Poland; marcin.wozniak@polsl.pl
* Correspondence: j.jana@psau.edu.sa (J.S.); zbigniew.marszalek@polsl.pl (Z.M.)

Abstract: Due to Internet of Things (IoT), it has become easy to surveil the critical regions. Images are important parts of Surveillance Systems, and it is required to protect the images during transmission and storage. These secure surveillance frameworks are required in IoT systems, because any kind of information leakage can thwart the legal system as well as personal privacy. In this paper, a secure surveillance framework for IoT systems is proposed using image encryption. A hyperchaotic map is used to generate the pseudorandom sequences. The initial parameters of the hyperchaotic map are obtained using partial-regeneration-based non-dominated optimization (PRNDO). The permutation and diffusion processes are applied to generate the encrypted images, and the convolution neural network (CNN) can play an essential role in this part. The performance of the proposed framework is assessed by drawing comparisons with competitive techniques based on security parameters. It shows that the proposed framework provides promising results as compared to the existing techniques.

Keywords: hyperchaotic map; image encryption; convolution neural network; partial-regeneration-based non-dominated optimization; fitness function

Citation: Ghosh, G.; Verma, K.; Anand, D.; Verma, S.; Rawat, D.B.; Shafi, J.; Marszałek, Z.; Woźniak, M. Secure Surveillance Systems Using Partial-Regeneration-Based Non-Dominated Optimization and 5D-Chaotic Map. *Symmetry* **2021**, *13*, 1447. https://doi.org/10.3390/sym13081447

Academic Editor: Jan Awrejcewicz

Received: 10 June 2021
Accepted: 2 August 2021
Published: 6 August 2021

1. Introduction

Internet of Things (IoT) has changed the way of life by providing connectivity among network-enabled devices. Surveillance is a major advantage of IoT that helps people to keep an eye on the security of homes, business, and critical places. Due to this, a large volume of data is transferred over the network that is further saved on servers. These data can be in the form of images, audio, video, and text, and are further utilized in many applications, such as military communication, healthcare, identification of suspicious activities, remote sensing, etc. As these data contain valuable information, any leakage of the data may create security breaches, which can further hamper the working of government, intelligence agencies, and personal privacy. Therefore, it is necessary to create a secure surveillance framework for IoT systems. In this work, our focus is to secure the images during transmission and storage, because images play an important role in various multimedia applications. The image captured from IoT devices can be sent to a server or directly to concerned personnel for surveillance. If the images are in plain form, then they can reveal all the information to an attacker. Therefore, transmission and storage of the images should be secured. To secure the images, cryptography is the most suitable

method. In cryptography, encryption and decryption processes are used to make the images meaningless and meaningful, respectively.

So far, researchers have implemented various image encryption techniques, utilizing various technologies such as chaotic maps, compressive sensing, transformations, deoxyribonucleic acid, S-box, optics, etc. Among these, chaotic maps are widely used by researchers. To perform the encryption and decryption, a secret key is required, and the whole strength of the cryptosystem is dependent on the secret key, because even if the attacker knows the encryption and decryption algorithms, without the secret key, the attacker will not be able to recover the images. The chaotic maps are the most suitable for developing the secure secret keys due to characteristics such as sensitivity to initial values, random behavior, deterministic nature, and ergodicity. Chaotic maps generate pseudorandom numbers, which are deterministic and can be utilized as secret keys. A number of chaotic maps have been proposed in the literature, and these can be classified as one-dimensional (1D) and high-dimensional chaotic maps (HDCM). The high-dimensional chaotic maps are preferred because of their complex trajectory and secured nature. HDCMs are comprised of more than one state variable and constant that constitute the complex structure. Thus, they provide better security as compared to 1D chaotic maps. However, some studies have shown that HDMCs can be broken by estimating their initial parameters. Therefore, it is necessary to optimally select the parameters of HDMCs. The optimal selection of HDMCs' parameters can be carried out through meta-heuristic techniques. These techniques provide the optimized solutions using random initial populations that cannot be easily guessed by the attacker.

Motivated by the above factors, in this paper, an efficient image encryption technique for secure surveillance frameworks for IoT systems is proposed. The main contributions of this paper are as follows:

- The secret keys are generated by utilizing a 5D hyperchaotic map. The reason of selection is to generate more complex pseudorandom numbers that cannot be easily estimated.
- To strengthen the security of the hyperchaotic map, the initial parameters are optimized using partial-regeneration-based non-dominated optimization (PRNDO). A multi-objective fitness function is designed using correlation coefficient and entropy. These two parameters were selected after analyzing their wide acceptability in the literature. Fitness functions based on these parameters provide better optimized solutions.
- After the secret key's generation, permutation is performed to change the pixels' position. Thereafter, the diffusion process is performed on scrambled images to produce the encrypted images.
- Finally, the performance of the proposed technique is assessed through comparative analyses with competitive techniques based on security parameters.

The rest of the paper is organized as follows: The related work is discussed in Section 2, background is presented in Section 3, and Section 4 elaborates on the image encryption technique for the secure surveillance framework for IoT systems. In Section 5, the simulation results and analyses are discussed, and Section 6 concludes the paper and presents the future research directions.

2. Literature Review

The authors of [1] used a 2D logistic-sine system (2LSS) to encrypt the images generated by sensors before the transmission, where the permutation and diffusion-based framework was utilized to perform the encryption. The authors of [2] enhanced the security of surveillance systems by encrypting the images using a cosine-transform-based chaotic map (CTCM), which was generated through the combination of logistic and sine maps. In [3], the authors implemented an image encryption technique using the Chen chaotic map and discrete fractional random transform (DFRT) for secure surveillance, while in [4], the authors utilized cellular automata to encrypt the images captured from the sensor. The authors of [5] designed an encryption technique to secure the images during storage, where

DNA and hyperchaotic maps (DNA-HC) were used to encrypt the images. In [6], a secure surveillance system was designed using the sine tent cosine approach for the transmission of images, while in [7], a secure communication system was developed using compressive sensing and chaotic map (CSCM) for IoT applications. The authors of [8] encrypted the images using permutation and diffusion operations. The permutation process was carried out using a Henon map, while a chaotic restricted Boltzmann machine was used to perform the diffusion operation on the images [8]. In [9], compressive sensing was used to encrypt the images, where a 3D chaotic map was used to generate the measurement matrix and a 1D chaotic map was utilized to diffuse the pixels of the scrambled image. The authors of [10] proposed an improved fractional 1D chaotic map to perform the image encryption. The permutation and substitution steps were combined to change the position of pixels and the values of an image [10]. The authors of [11] investigated and presented current trends on IP and DS in IOT.

The authors of [12] utilized a differential equation to generate the chaotic oscillator, which is used to scramble the pixels of an image to obtain an encrypted image. In [13], a DP model was proposed for security and privacy. The authors of [14] implemented an image encryption framework: Fresnel transform. In this technique, a lens is not used, and the image is divided into three channels and each is encrypted using a separate key [14]. In [15], a time delay chaotic system was used to encrypt the images. The authors of [16] applied coupled map lattices to generate the keys. In this technique, the random-based diffusion process is implemented to encrypt the images [16]. The authors of [17] developed an image encryption scheme using a 6D chaotic map. The position of pixels of images is permuted at the bit-level to enhance the security, and the pixels are finally diffused using DNA coding. In [18], the authors encrypted the images using tent-dynamics coupled map lattices, and the cyclic shift algorithm was utilized to shift the rows and pseudorandom sequences. The above-discussed techniques involved the use of chaotic maps to generate the secret keys, and although these techniques provide secure image transmission and storage, in most of the techniques, the initial parameters of chaotic maps were not selected optimally. Thus, using parameter estimation techniques, these techniques can be broken [18]. The authors of [19] presented a deep learning model for traffic flow prediction.

Some of the researchers have addressed the above-stated issue by implementing the meta-heuristic techniques in image encryption. The authors of [20] developed an encryption system using DNA and the 1D logistic map for secure transmission of images. Particle swarm optimization (PSO) was utilized to select the best encrypted image based on entropy and the correlation coefficient. The non-dominated sorting genetic algorithm-II (NSGA-II) was used in [21] to optimize the intertwining logistic map, the genetic algorithm (GA) was applied in [22] to optimize the beta-chaotic map, and the Pareto evolutionary algorithm-II was implied in [23] to optimally select the parameters of the 4D chaotic map. Adaptive differential evolution (ADE) was used in [24] for tuning the hyperparameters of the Lorenz chaotic map. Grey hole and black hole attacks were presented in [25], while the 5D chaotic map was tuned in [26] using NSGA. An intertwining logistic map was optimized in [27] using memetic differential evolution, the hyperparameters of the beta-chaotic map were tuned in [28] using differential evolution, and IoT-based risk assessments were presented in [29].

3. Background

3.1. Five-Dimensional Hyperchaotic Map

The five-dimensional (5D) hyperchaotic map (5DHCM) provides significantly complex chaotic behavior [30,31]. The 5DHCM has five attributes, a cubic nonlinear product, and a better Lyapunov exponent (LE). The huge number of attributes improves the key space, the large LE provides a more dynamic 5DHCM, and the cubic nonlinear product achieves good resistance [32]. Thus, 5DHCM can achieve better encryption keys and can be computed as:

$$\begin{aligned} d'1 &= q(d2 - d1) + d2d3d4 \\ d'2 &= r(d1 + d2) + d5 - d1d3d4 \\ d'3 &= -sd2 - td3 - ud4 + d1d2d4 \\ d'4 &= -vd4 + d2d3d1 \\ d'5 &= -w(d1 + d2) \end{aligned} \tag{1}$$

Here, in Equation (1), d′1, d′2, d′3, d′4, and d′5 are initial attributes required for 5DHCM, and q, r, s, t, u, v, and w define the control attributes of 5DHCM. Chaotic attractors are represented in Figure 1 and Figure 4 for q = 30, r = 10, s = 15.7, t = 5, u = 2.5, v = 4.45, and w = 38.5. Figure 1 demonstrates the chaotic attractor in the d1-d2 plane, whereas Figure 2 shows the chaotic attractor in the d1, d2, and d3 planes. The chaotic attractor in the y1-y2-y3 plane is presented in Figure 2. The time series analysis of the state attribute d1 utilizes Equation (1), as depicted in Figure 3. It is demonstrated that d1 achieves random behavior and is non-periodic in nature. System (1) contains 5 equilibrium points, such as (0, 0, 0, 0, 0), (2.39, −2.39, −6.85, 8.76, −143.09), (1.56, −1.56, 10.50, −5.71, −93.33), (−2.39, 2.39, 6.85, −8.76, 143.09), and (−1.56, 1.56, −10.50, 5.71, 93.33). The eigenvalues of equilibrium points are positive integers. Thus, the equilibrium points of system (1) are saddle points, unstable, and hyperbolic [33].

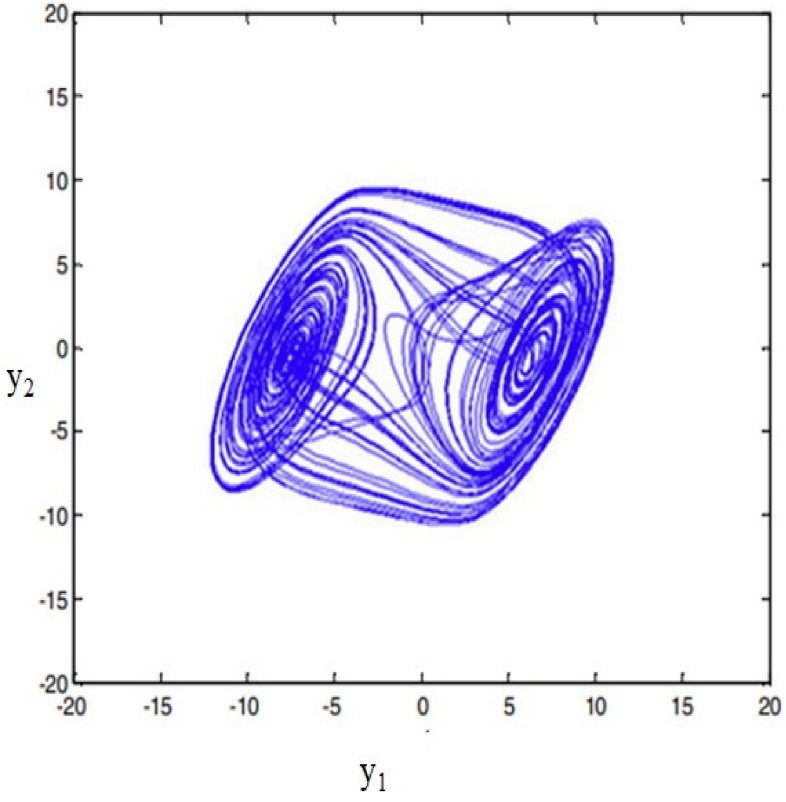

Figure 1. Chaotic attractor in the y1-y2 plane.

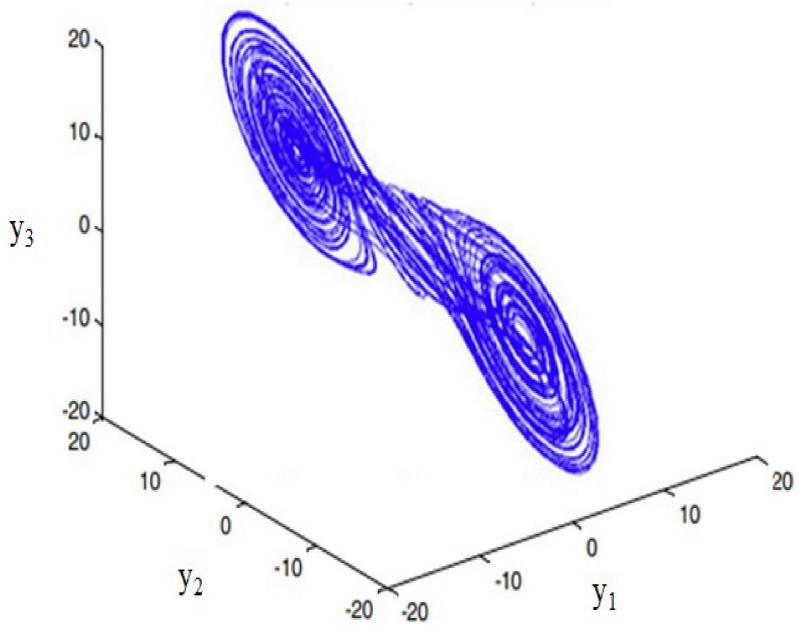

Figure 2. Chaotic attractor in the y1-y2-y3 plane.

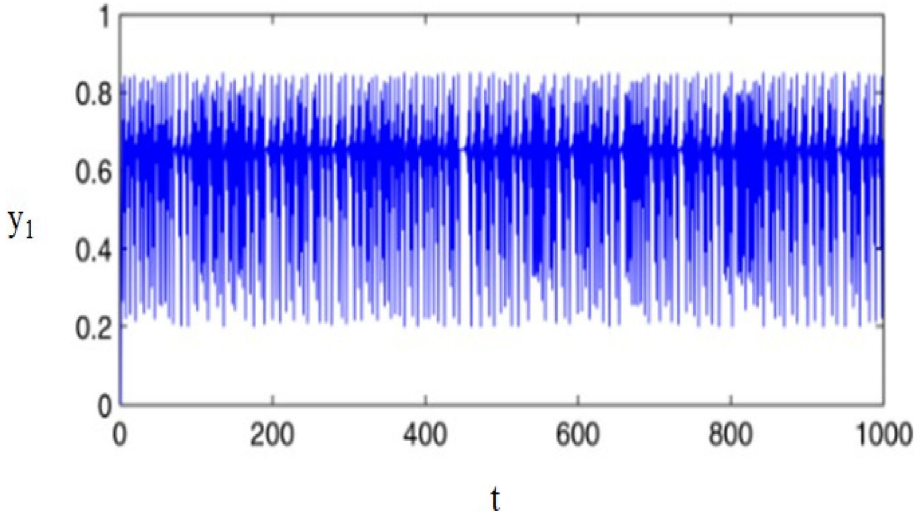

Figure 3. Time series plot for state variable y1 using system (1).

3.2. Partial-Regeneration-Based Non-Dominated Optimization

Partial-regeneration-based non-dominated optimization (PRNDO) [34] provides optimal solutions considering both the best and worst cases. This type of optimization is mainly used to solve the asymmetrical problems. In this study, a bottom-boosting methodology was utilized to reduce the number of function evaluations. It also provides a balance between better solutions and computational speed by developing a novel partial-regeneration strategy and mutation operator. Therefore, it can generate efficient solutions with good computational speed. The outline of PRNDO is shown in Figure 4. It contains population initialization, minimum heap (min-heap) construction, bottom-boosting, partial-regeneration strategy, and termination condition. Initially, a population is randomly generated with the pair consisting of solution and scenario. The other parameters are also initialized, such as control attributes, solution and scenario dimensions, and maximum number of generations. Thereafter, by using the given population, a min-heap is built in the beginning of every generation. Every solution is treated as a node of min-heap, and the objective value of it acts as a key of the node. After that, scenarios of min-heap nodes

are updated using the bottom-boosting scheme. The fitness function evaluations are also controlled by this scheme. Using fitness values of each individual, a sorted population is generated in increasing order. The trial scenario is produced from mutation and binomial recombination. The fitness value of the trial scenario is then calculated with respect to the original scenario. If the trial provides better fitness, then the original scenario of the individual will be upgraded. Otherwise, the old scenario will be used in the next generation. During the updating of scenarios, min-heap is also updated using the current population. Next, all the individuals are controlled and updated using the partial-regeneration strategy. The mutation and binomial recombination is also utilized. Finally, the termination condition (such as maximum number of generations evaluation) is tested, and optimal solutions are obtained as a result. IoT-based data analytics are presented in [34,35]. In [36] a comparative study is performed based on machine learning techniques.

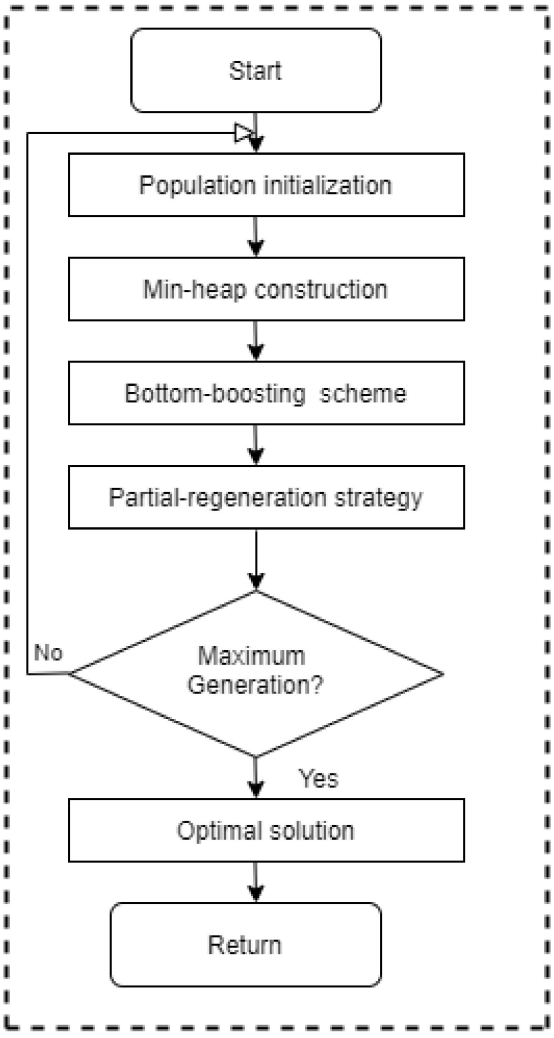

Figure 4. Flowchart of PRNDO.

4. Proposed Image Encryption Technique for Secure Surveillance Frameworks

An image encryption technique for secure surveillance frameworks for IoT systems is shown in Figure 5.

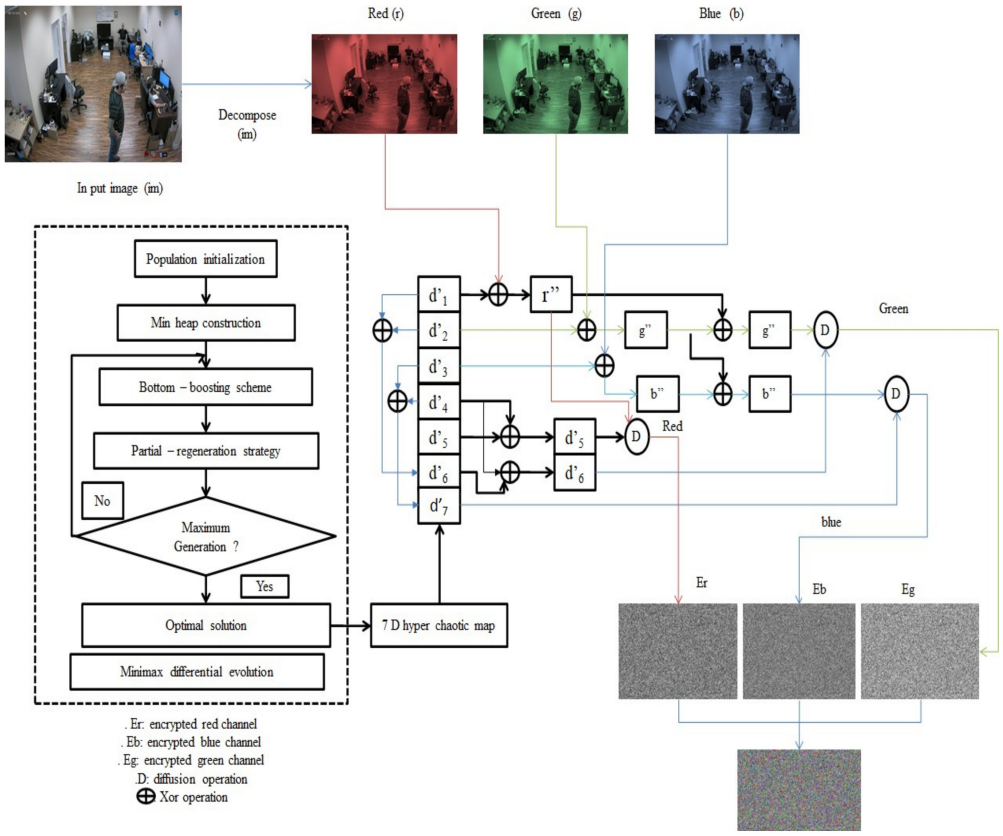

Figure 5. Applied model of encryption.

The obtained images from surveillance cameras are initially encrypted by the proposed technique, then transmitted over the network. The obtained image is firstly decomposed into red (R), green (G), and blue (B) channels. The secret keys, such as d′1, d′2, d′3, d′4, and d′5, are obtained from 5DHCM (Algorithm 5). The required initial parameters of 5DHCM are optimized using PRNDO (Algorithm 2). All three channels are permuted using Arnold transform. Then, pixels of permuted channels R, G, and B are diffused utilizing d′1, d′2, and d′3, with the ($\oplus$) operator, respectively. The obtained images are δR, G′, and B′. G′ and B′ are further diffused using $\oplus$ operation using δR, and produce δG and δB. Two more keys (d′6 and d′7) are generated.

d′6 is generated from d′1 and d′2 using $\oplus$ operation, d′7 is generated from d′3 and d′4 using $\oplus$ operation, and d′4 is then utilized to update d′5 and d′6. Encrypted color channels, i.e., ϵR, ϵG, and ϵB, are obtained by diffusing δR, δG, and B″ with d′5′, d′6′, and d′7, and the η operator, respectively. Finally, the encrypted image (EM) is obtained by concatenating the ϵR, ϵG, and ϵB.

The step-by-step approach is shown in Algorithm 1.

Algorithm 1 Image encryption technique for surveillance systems

Input: *im* as image for processing
Output: result of applied encryption *EM*
/ input image im process on three channels, red (R), green (G), and blue (B) */*
$R = im(:, :, 1)$;
$G = im(:, :, 2)$;
$B = im(:, :, 3)$;
Apply Arnold transform to permute color channels *R*, *G*, and *B;*
Use Algorithm 2 to calculate optimal parameters ($z_k(k = 1: SolD\hat{}$));
Use Algorithm 5 to generate secret keys $d'u$, for $u = 1, \ldots, 7$;
//Use $d'1$, $d'2$, and $d'3$ $\delta_R = \text{mod}\ (R \oplus d'_1, 256)$ to diffuse processed color channels;
$G' = \text{mod}\ (G \oplus d'_2, 256)$; $\delta_G = \text{mod}\ (G' \oplus R'', 256)$; $B' = \text{mod}\ (B \oplus d'_3, 256)$; $B'' = \text{mod}\ (B' \oplus G', 256)$;
//Update $d_{5'}$ and $d_{6'}$ using $d_{4'}$ $d_5'' = d'5 \oplus d'4$;
$d_6'' = d'6 \oplus d'4$;
//Encrypt R'', G'', and B'' using $d'5'$, d_6'', and $d_{7'}$ $\eta = u_{lM}$;
$\epsilon_R = \text{mod}\ (d_5'' \times R'' + (1 - \eta) \times d_5'', 256)$;
$\epsilon_G = \text{mod}\ (d_6'' \times G'' + (1 - \eta) \times d_6'', 256)$;
$\epsilon_B = \text{mod}\ (d_{7'} \times B'' + (1 - \eta) \times d_{7'}, 256)$;
//As a result of processing the output, an encrypted image is generated as a combination of applied color channels;
$EM = \text{cat}\ (\epsilon_R, \epsilon_G, \epsilon_B)$; return *EM*

4.1. PRNDO-Based Optimal Parameters

The parameters of 5DHCM are d1, d2, d3, d4, d5, q, r, s, t, u, v, and w, and they need to be initialized. Manual selection of the above parameters is a computationally expensive task. For better key generation, these parameters are selected optimally by using PRNDO optimization. The procedure to generate the optimal parameters for 5DHCM using PRNDO is outlined in Algorithm 2.

Algorithm 2 PRNDO-based optimal parameters' generation

Input: Solution dimension Sol_o, scenario dimension S_o, maximum generation N_h, and population size M_l
Output: Optimized population: Set generation $u = 0$;
//population initialization
$P_a = \{(z_{1,u}, I_{1,u}), (z_{2,u}, I_{2,u}), \ldots, (z_{M,u}, I_{M,u})\}$,
where $z_{k,u} = \{z^1, S^2, \ldots, S^{Sol}d\}$
for $y = 1$ *to* M_s **do**
fitness of individual $(z_{k,u}, I_{k,u})$ is evaluated using Algorithm **6**; **end**
for $u = 1$ *to* N_h **do**
Min heap is built for each individual in q_u;
Use (Algorithm 3) to implement the bottom-boosting approach on min-heap;
for $k = 1$ *to* M_l **do**
//Individual (z_e, I_e) stored as a root node in the min-heap
$zk,u = ze$, $Ik,u = Ie$;
Extract root node from min-heap;
end
$zbest = z1, u$;
Use partial-regeneration strategy for D_u updating (Algorithm 4);
$D_{u+1} = D_u$;
end

In Algorithm 2, firstly, the parameters' solution dimension Sol_o, scenario dimension S_o, maximum generation N_h, and population size M_l are initialized. Using normal distribution, initial population D_u is generated randomly. Each individual (zk,u, Ik,u) represents a set consisting of solution and scenario. Fitness of (zk,u, Ik,u) is evaluated using Algorithm 6. A min-heap is built using D_u. The scenarios are updated using Algorithm 3. The current population is updated by extracting the root node of min-heap. Then, the nodes are arranged in increasing order on the basis of fitness. The initial solution of a given

population is utilized as a global best solution. Thereafter, a partial-regeneration strategy is utilized to further update the current population (Algorithm 4). The entire steps are iteratively implemented until the stopping criteria are not met.

Algorithm 3 Bottom-boosting approach

Input: Scaling factor F, a min-heap constructed using D_u, crossover rate Ie, and number of fitness evaluations H_w, **Output:** Min-heap $EE = 0$;
while $EE < H_w$ **do**
//Consider each ($z_{k,u}$, $I_{k,u}$) stored in the root, visit root of min-heap;
Mutant is developed as
$Iw_{k,u} = I_e1, u + H(I_e2, u–I_e3, u)$;//where e_1, e_2, and e_3 are elected on a random basis from $\{1, \ldots, M_l\}$
Trial scenario $IV_{k,u}$ is produced using binomial recombination on $I_{k,u}$ and $IU_{k,u}$;
if F ($z_{k,u}$, $IV_{k,u}$) > F ($z_{k,u}$, $I_{k,u}$) **then** extract the root node of min-heap; $Ik,u = IVk,u$;
Update min-heap using ($z_{k,u}$, $I_{k,u}$);
end
$EE = EE + 1$;
end

Algorithm 4 Partial-regeneration approach

Input: Sorted population D_u, scaling factor F, crossover rate Ie, and number of updated individuals β
Output: Updated population D_u $y = 1$;
while $y \leq \beta$ **do**
$X_{k,u} = z_{k,u} + H(Y_r1, a - z_l2, u)$;//Here, $k \in \{1, 2, \ldots, \beta\}$
Trail solution $\phi_{k,u}$ is produced using binomial recombination on $z_{k,u}$ and $X_{k,u}$; $zM_l + 1 - y,u = \phi k,u$;
Reinitialize $I_Ml + 1 - y,u$, randomly;
Evaluate the fitness of ($z_Ml + 1 - y,u$, $z_Ml + 1 - y,u$) using Algorithm 6;
$y = y + 1$;
end

Algorithm 5 Generation of secret keys using 5DHCM

Input: Optimized parameters $z_k(k = 1: SolD\hat{})$
Output: Secret keys $d'1$, $d'2$, $d'3$, $d'4$, $d'5$, $d'6$, and $d'7$
//In $z_k(k = 1: SolD\hat{} - 1)$, $SolD\hat{} = 18$.
//$z_k(k = 1: SolD\hat{} - 1)$ denotes d_1, d_2, d_3, d_4, d_5, q, r, s, t, u, v, and w, respectively.
$d'1 = z_6(z_2 - z_1) + z_2z_3z_4$;
$d'2 = z_7(z_1 + z_2) + z_5 - z_1z_3z_4$;
$d'3 = -z_8z_2 - z_9z_3 - z_{10}z_4 + z_1z_2z_4$; $d'4 = -z_{11}z_4 + z_2z_3z_1$;
$d'5 = -z_{12}(z_1 + z_2)$; $d'6 = z_1 \oplus z_2$;
$d'7 = z_3 \oplus z_4$;
return $d'1$, $d'2$, $d'3$, $d'4$, $d'5$, $d'6$, and $d'7$

4.2. Secret Keys

The process of secret keys' generation using 5DHCM is elaborated in Algorithm 5. It uses the optimized parameters obtained from Algorithm 2. The keys such as d1, d2, d3, d4, d5, d6, and d7 are generated using Algorithm 5. To diffuse the image, these keys are utilized by Algorithm 1 to obtain the encrypted image.

4.3. Fitness Evaluation

To compute the individuals, the following fitness function is utilized

Correlation and entropy are widely accepted parameters to obtain the optimal solutions because in image encryption, there is a need to reduce the relationship between the pixels. In the case of maximum entropy, each pixel carries the same amount of information. Both parameters hide the statistical behavior of the images from the attacker. The desired value of correlation and entropy should be near 0 and 8, respectively. The fitness function is described in Algorithm 6.

Algorithm 6 Fitness function

Input: solution $z_k(k = 1: SolD\hat{})$, input image, *im*
Output: Fitness value, *F*
Encrypted image, *EM*, is obtained using Algorithm 1
II = correlation (*EM*);
ϵ_x = entropy (*EM*);
if $\epsilon_x > 7.9990 \;\&\&\; -0.05 \leq CC \leq 0.05$ **then**
end
return *F* (ϕ)

Algorithm 7 Image decryption process

Input: Encrypted image, *EM*, and values of d_1, d_2, d_3, d_4, d_5, q, r, s, t, u, v, w, and η
Output: Decrypted image (D_I); Decompose *EM* into ϵ_R, ϵ_G, and ϵ_B.
Obtain keys $d'1$, $d'2$, $d'3$, $d'4$, $d'5$, $d'6$, and $d'7$ by using Algorithm 5;
$d'5' = d'5 \oplus d'4$; $d'6' = d'6 \oplus d'4$;
//Decrypt ϵ_R, ϵ_G, and ϵ_B by $d'5'$, $d'6'$, and $d'7$
$\delta R = \epsilon_R - (1-\eta) \times \overline{d'5'}^{\eta}$;
$\delta G = \epsilon_G - (1-\eta) \times \overline{d'6'}^{\eta}$;
$\delta B = \epsilon_B - (1-\eta) \times \overline{d'7}^{\eta}$;
//Decrypt δ_R, δ_G, and δ_B by $d'1$, $d'2$, and $d'3$, $R = \delta_R \oplus d'1$;
$G' = R \oplus \delta_G$; $G = G' \oplus d'2$; $B' = B'' \oplus \delta_G$; $B = B' \oplus d'3$;
Apply inverse Arnold transform on *R*, *G*, and *B*;
//Concatenate the decrypted channels
$D_I = [R, G, B]$;
return D_I

4.4. Image Decryption Algorithm

The encrypted image is decrypted using Algorithm 7 to obtain the original image. The initial values of d1, d2, d3, d4, d5, q, r, s, t, u, v, w, and η attributes are needed to decrypt the image.

5. Comparative Analysis

Simulations were performed using MATLAB 2020a with the help of the image processing toolbox. The proposed encryption model is compared with five well-known competitive approaches by using various performance metrics. The initial parameters of PRNDO are assigned as F = 0.6, Cr = 0.2, N = 50, KS = 170, and T = 5. Four surveillance camera images were used, with 256 × 256 size.

5.1. Visual Analysis

Input and the respective encrypted surveillance images are shown in Figure 6. It clearly indicates that the obtained encrypted surveillance images seem like purely noisy images in nature. Therefore, no attacker can obtain any kind of details of the encrypted images.

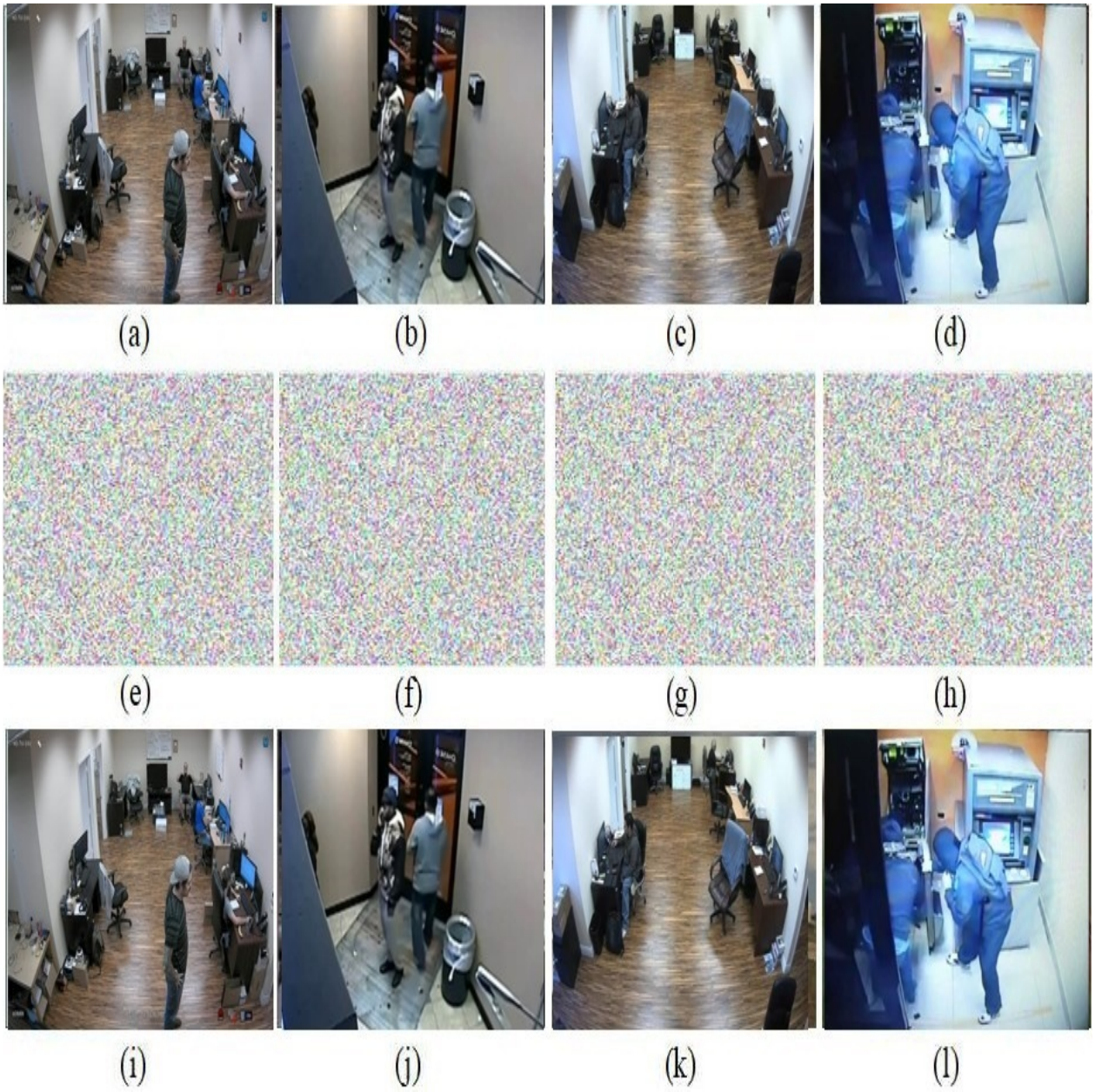

Figure 6. Input images: (**a**–**d**) input surveillance images. Encrypted images: (**e**–**h**) encrypted surveillance images. Decrypted images: (**i**–**l**) decrypted surveillance images.

5.2. Quantitative Analysis

5.2.1. Entropy

Entropy [29] computes the degree of randomness in images. In encrypted images, it is desirable to have 8 degrees of randomness. An entropy analysis of the proposed secure surveillance system is depicted in Table 1. It shows that the entropy values of all the techniques on surveillance images (SIk), where k = 1, 2, 3, or 4, were near to 8, but the proposed secure surveillance system achieved higher values than the existing techniques.

Table 1. Entropy analysis of the proposed secure surveillance system.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	7.9968	7.9836	7.9986	7.9886
CTCM [2]	7.9986	7.9846	7.9925	7.9860
DFRT [3]	7.9936	7.9959	7.9845	7.9899
HDNA-HC [5]	7.9880	7.9956	7.9836	7.9836
CSCM [7]	7.9972	7.9862	7.9969	7.9885
Proposed	7.9980	7.9982	7.9986	7.9984

5.2.2. Peak Signal-to-Noise Ratio

Peak signal-to-noise ratio (PSNR) [37] analysis is depicted in Table 2. It was found that the proposed secure surveillance system outperformed the existing approaches. Block scrambling methodologies are used for image encryption process [38].

Table 2. PSNR analysis of the proposed snecure surveillance system.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	71.3826	71.7675	69.9256	69.3956
CTCM [2]	69.7869	70.4040	68.8362	70.9381
DFRT [3]	69.4288	69.1983	70.7452	71.9038
HDNA-HC [5]	70.6257	71.3539	69.9062	69.3482
CSCM [7]	69.9282	69.9264	70.9636	71.8936
Proposed	80.9261	82.3689	80.8362	80.3782

5.2.3. Mean Absolute Error

Mean absolute error (MAE) analysis is shown in Table 3. It revealed that the proposed model obtained significantly better values than the existing models.

Table 3. Mean absolute error analysis of the proposed secure surveillance system.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	79.4834	81.8382	79.3623	82.8262
CTCM [2]	83.8052	82.3617	84.3854	81.3822
DFRT [3]	81.8826	83.9083	81.8669	82.4837
HDNA-HC [5]	83.7068	81.1898	84.7656	84.0944
CSCM [7]	83.6945	85.6065	87.8084	86.8636
Proposed	88.2847	90.8742	91.3508	90.6820

5.3. Security Analysis

In this section, we will test the proposed secure surveillance system model against various security attacks. The objective was to evaluate whether or not the proposed secure surveillance system model can resist various security threats.

5.3.1. Histogram Analysis

To evaluate the performance of the proposed secure surveillance system model against an attack, we used histogram analysis. It was found that the histograms of the encrypted images should be uniform. Histogram analysis of the proposed model is shown in Figure 7, and it was found that the histograms of encrypted images obtained from the proposed secure surveillance system model were evenly distributed.

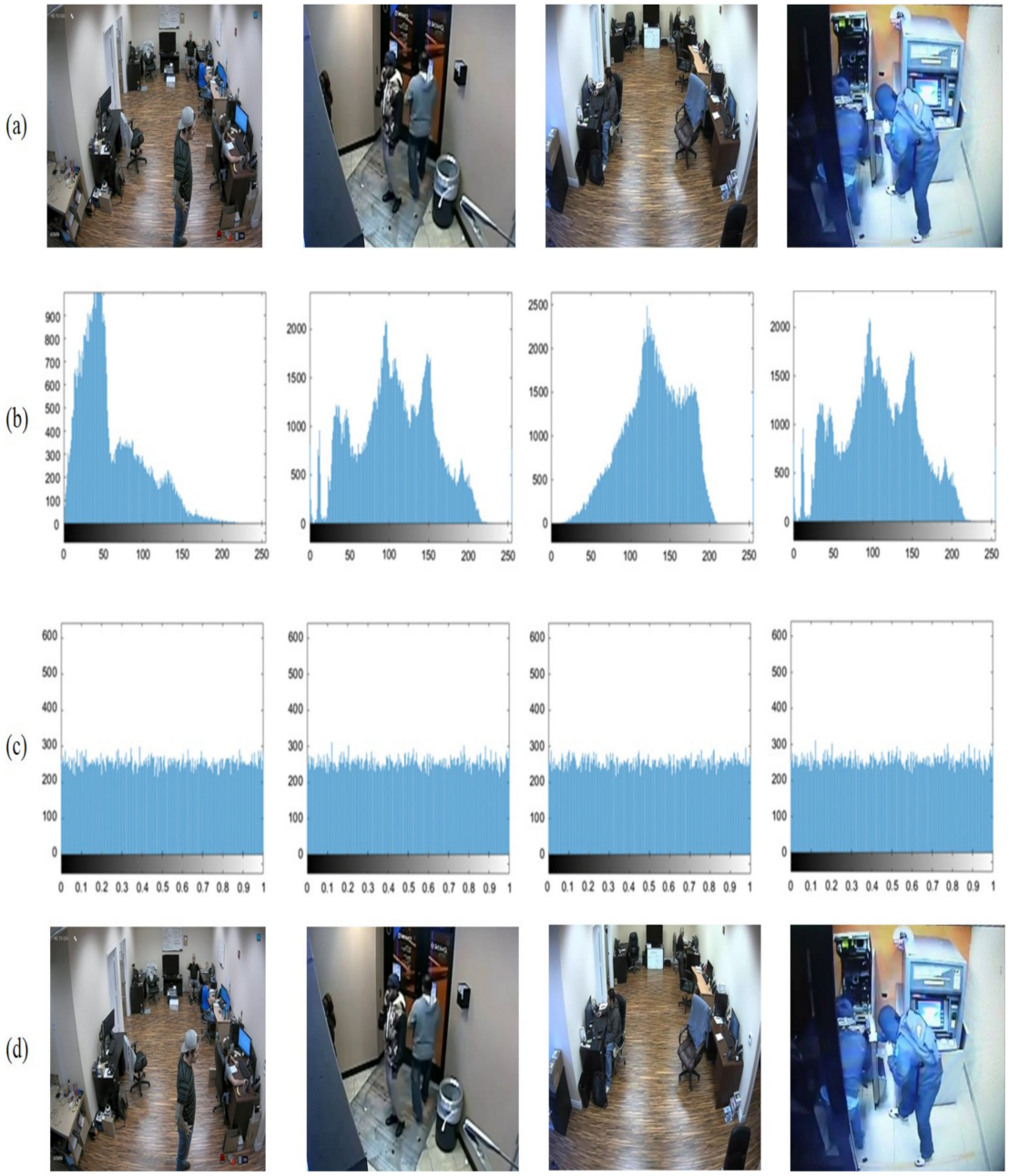

Figure 7. Histogram analysis: (**a**) surveillance images, (**b**) histogram of surveillance images, (**c**) histogram of encrypted surveillance images, and (**d**) encrypted surveillance images.

5.3.2. Correlation Analysis

Correlation can also be used to evaluate the statistical information of surveillance images. Thus, it is desirable that the correlation between the adjacent pixels vertically, diagonally, and horizontally should be minimum. The horizontal correlation analysis is depicted in Table 4. It shows that the correlation among horizontal pixels was minimum compared to the existing encryption models. Vertical and diagonal correlation analyses are shown in Tables 5 and 6. The minimum correlation values of the proposed secure surveillance system indicate that the proposed model can resist correlation attacks.

Table 4. Horizontal correlation analysis.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	0.0028	0.0029	0.0038	−0.0022
CTCM [2]	0.0090	0.0060	0.0040	0.0022
DFRT [3]	−0.0050	0.0123	0.0090	0.0040
HDNA-HC [5]	0.0040	0.0070	−0.0090	0.0036
CSCM [7]	0.0072	0.0038	−0.0050	0.0055
Proposed	−0.009	0.0016	0.0019	0.0021

Table 5. Vertical correlation analysis.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	0.0036	0.0030	−0.0026	0.0016
CTCM [2]	−0.0066	0.0068	0.0026	0.0042
DFRT [3]	0.0026	0.0015	0.0022	0.0019
HDNA-HC [5]	0.0028	0.0016	−0.0025	0.0014
CSCM [7]	0.0016	−0.0024	0.0028	0.0024
Proposed	0.0014	−0.0010	0.0013	0.0009

Table 6. Diagonal correlation analysis.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	−0.0118	0.0072	0.0058	0.0028
CTCM [2]	0.0046	0.0034	0.0060	0.0032
DFRT [3]	0.0062	0.0044	0.0028	0.0026
HDNA-HC [5]	−0.0044	0.0034	0.0056	0.0038
CSCM [7]	0.0042	0.0050	0.0044	−0.0062
Proposed	0.0019	0.0021	0.0018	0.0020

5.3.3. Differential Analysis

The differential analysis can be computed using the Number of Pixel Change Rates (NPCR) and Unified Average Change Intensity (UACI). The NPCR and UACI analyses of the proposed secure surveillance system are depicted in Tables 7 and 8. It was found that the proposed model achieved better NPCR and UACI values than the competitive models. Thus, the proposed model is sensitive towards the tiny modification in input surveillance images.

Table 7. NPCR analysis of the proposed secure surveillance system.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	99.40	99.52	99.48	99.50
CTCM [2]	99.44	99.40	99.50	99.52
DFRT [3]	99.46	99.50	99.54	99.48
HDNA-HC [5]	99.45	99.52	99.48	99.50
CSCM [7]	99.59	99.56	99.58	99.46
Proposed	99.65	99.70	99.69	99.72

Table 8. UACI analysis of the proposed secure surveillance system.

Model	SI_1	SI_2	SI_3	SI_4
2LSS [1]	33.25	33.33	33.35	33.30
CTCM [2]	33.39	33.40	33.38	33.36
DFRT [3]	33.30	33.37	33.40	33.38
HDNA-HC [5]	33.38	33.42	33.42	33.48
CSCM [7]	33.40	33.50	33.50	33.49
Proposed	33.55	33.58	33.64	33.62

5.3.4. Robustness against Various Attacks

- Noise attack

Robustness of the proposed secure surveillance system was evaluated against salt and pepper and Gaussian noise attacks with various densities of noise.

Figure 8 shows noisy encrypted images for which Gaussian noise with ($\mu1 = 0.1$, $\sigma1 = 0.1$), ($\mu2 = 0.3$, $\sigma2 = 0.3$), and ($\mu3 = 0.5$, $\sigma3 = 0.5$) were used. The corresponding decrypted images are depicted in Figure 8d–f. The corresponding PSNR values among actual and decrypted images were 27.58, 21.39 and 13.84 dB. The visual analysis shows that the proposed model can preserve details from the attacked images.

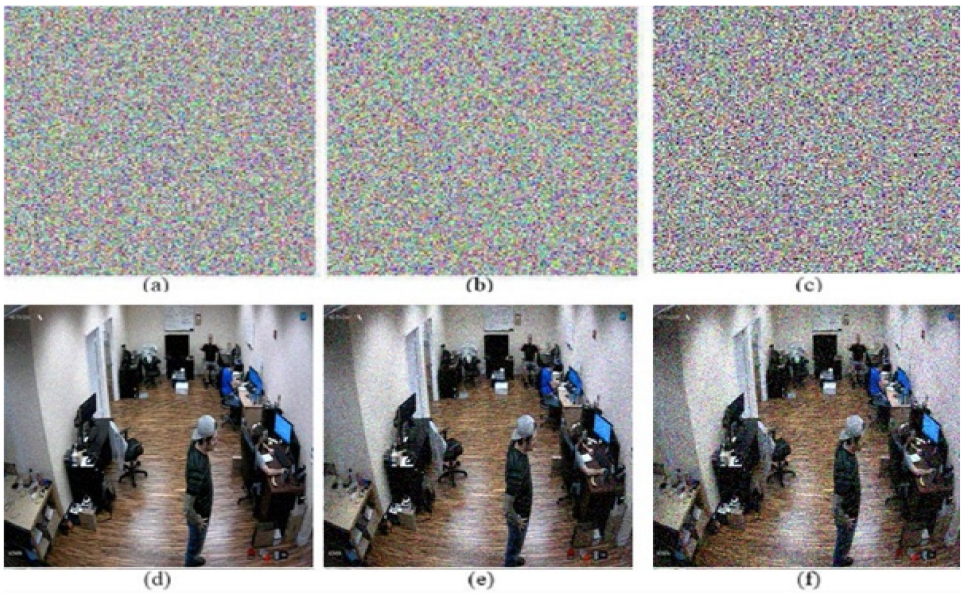

Figure 8. Gaussian noise attack-based encrypted images: (**a**) with $\mu = 0.1$ and $\sigma2 = 0.1$, (**b**) with $\mu = 0.3$ and $\sigma2 = 0.3$, and (**c**) with $\mu = 0.5$ and $\sigma2 = 0.5$. Corresponding decrypted images: (**d**) evaluated using (**a**), (**e**) evaluated using (**b**), and (**f**) evaluated using (**c**).

Figure 9 shows salt and pepper noise-affected encrypted images, with density = 0.1, 0.3, and 0.6, respectively. Figure 9d–f demonstrates decrypted images evaluated from the respective noisy images.

The corresponding PSNR among SI1 and decrypted SI1 were 32.13, 23.73, and 17.25 dB. The decrypted images show that the proposed model can decrypt images even from high-density noise

- Enhancement attack

Attackers may utilize image enhancement to damage the encrypted images. Attacked encrypted images obtained from various enhancement attacks such as gamma correction, histogram equalization, and adaptive histogram equalization are shown in Figure 10a–c. The corresponding decrypted images are depicted in Figure 10d–f. The corresponding PSNR values were 27.35, 19.72, and 14.93 dB. Visual analysis also revealed that the proposed model can provide potential information of actual images.

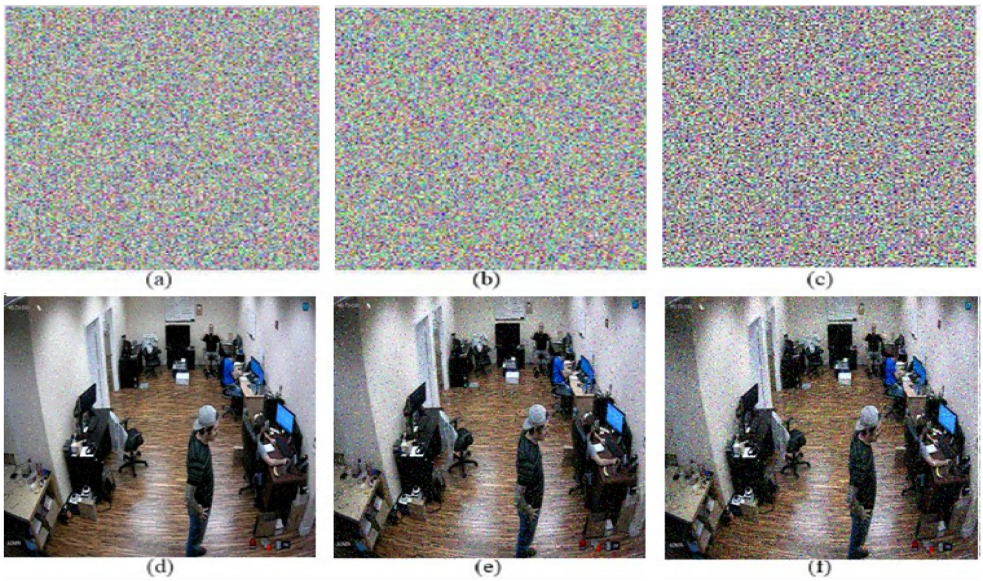

Figure 9. Salt and pepper noise-based encrypted images (**a**) with density = 0.1, (**b**) with density = 0.3, and (**c**) with density = 0.6. Corresponding encrypted images: (**d**) evaluated using (**a**), (**e**) evaluated using (**b**), and (**f**) evaluated using (**c**).

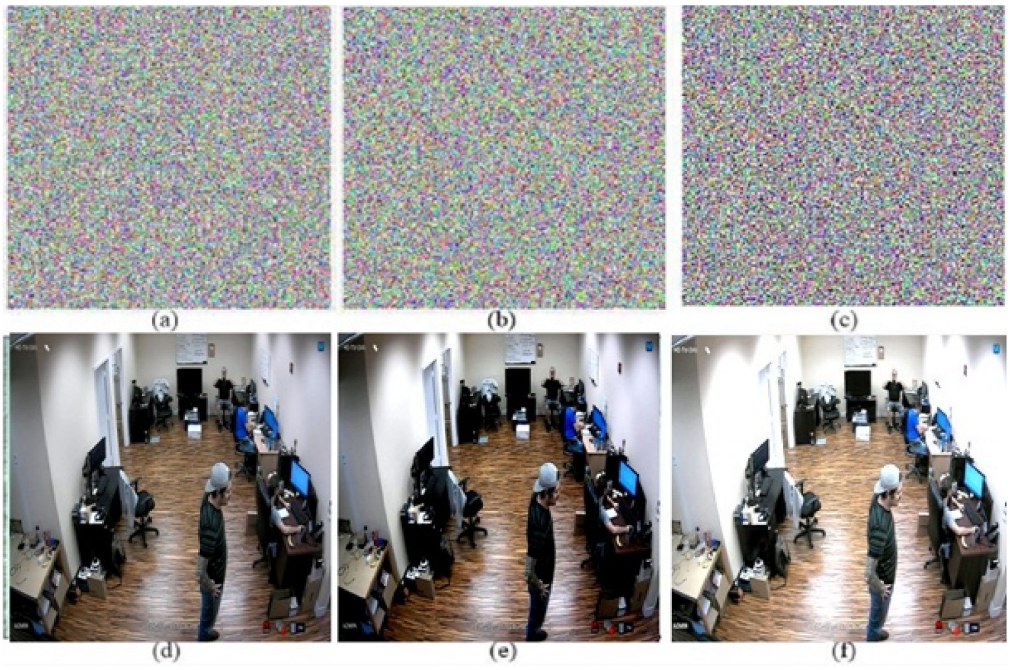

Figure 10. Enhancement-based encrypted images: (**a**) gamma correction, (**b**) histogram equalization, and (**c**) adaptive histogram equalization. Corresponding decrypted images: (**d**) evaluated using (**a**), (**e**) evaluated using (**b**), and (**f**) evaluated using (**c**).

5.3.5. Key Analysis

To evaluate the performance of the proposed secure surveillance system against brute-force attack, key sensitivity and key space analysis were considered.

- Secret key space

The proposed secure surveillance system computes the secret keys by 5DHCM. It requires 7 state attributes (i.e., d1, d2, d3, d4, d5, d6, and d7) and 7 control attributes (i.e., q, r, s, t, u, v, and w). Assume that the precision of attributes is 10−16. Thus, each attribute has 1016 possible values. Thus, the proposed secure surveillance system has key space:

$$(KS) \approx 10{,}119$$

$$KS = d1 \times d2 \times d3 \times d4 \times d5 \times d6 \times d7 \times q \times r \times s \times t \times u \times v \times w$$

$$= 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016 \times 1016$$

$$\approx 1016\hat{}14$$

Since the key space > 1030 (≈ 2100), therefore, the proposed encryption model can resist a brute-force attack.

- Secret key sensitivity analysis

It is desirable for the secret keys to be more sensitive towards tiny changes. Seven keys were evaluated to implement the proposed encryption. These 7 keys were computed by Equation (1) with the help of initial state (i.e., u1, u2, u3, u4, u5, u6, and u7) and control (i.e., s, r, t, i, q1, p, n, e, g, and q2) attributes. Assume that a tiny change is made in the bits of u1. To verify the key sensitivity, we will encrypt the surveillance images using an actual key and with a tiny change in the same key. The encrypted surveillance images with actual and modified keys are shown in Figure 11b,c. Figure 11d shows the error between Figure 11b and c. The computed error seems to be a completely random image. We have also decrypted Figure 11b by utilizing both keys. The evaluated results are depicted in Figure 11e,f. If the identical key is used for decryption, then the obtained image is similar to the actual image. The decrypted image obtained using a tiny change in the actual key seems to be a completely noisy image. Thus, the proposed model is very sensitive towards the encryption key.

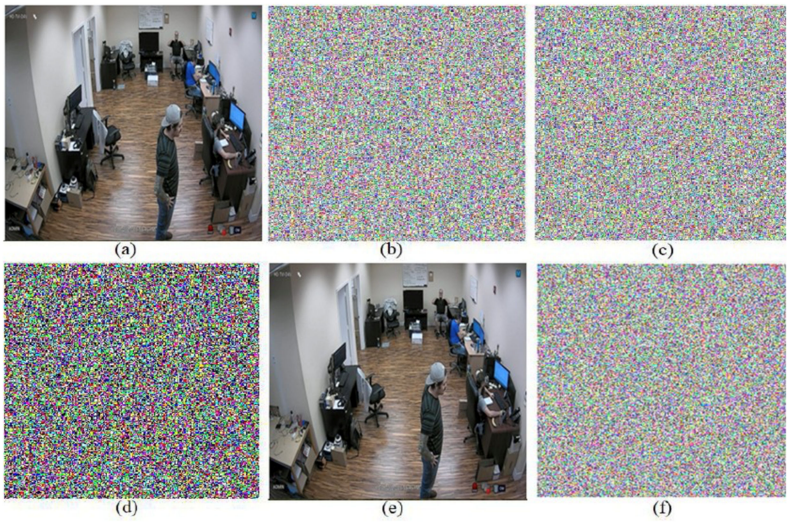

Figure 11. Sensitivity analysis: (**a**) actual surveillance image, (**b**) actual key-based encrypted image, (**c**) same key with tiny changes-based encrypted image, (**d**) error between (**b**) and (**c**), (**e**) actual key-based decrypted image, and (**f**) tiny changed key-based decrypted image.

Table 9 shows the error between a modified and an actual key-based encrypted image. It demonstrates that the proposed secure surveillance system is sensitive towards initial key values.

Table 9. Error between actual and modified key-based encrypted images.

	SI_1	SI_2	SI_3	SI_4
Error	99.9965	99.9958	99.9969	99.9971

5.3.6. Execution Time

Encryption and decryption execution time analyses are shown in Tables 10 and 11. These tables reveal that the proposed model can encrypt and decrypt images at a higher speed, as it requires less time than the existing models.

Table 10. Encryption time analysis.

Image	Dimensions	2LSS [1]	CTCM [2]	DFRT [3]	DNA-HC [5]	CSCM [7]	Proposed Approach
SI_1	256 × 256	11.3	15.4	12.4	12.6	11.1	10.3
SI_2	512 × 512	58.8	60.8	56.8	55.6	58.6	39.4
SI_3	1024 × 1024	648.6	601.6	626.8	611.8	598.8	592.6
SI_4	2048 × 2048	2368.8	2658.8	2358.4	2261.2	1996.2	1872.1

Table 11. Decryption time analysis.

Image	Dimensions	2LSS [1]	CTCM [2]	DFRT [3]	DNA-HC [5]	CSCM [7]	Proposed Approach
SI_1	256 × 256	0.062	0.051	0.042	0.039	0.041	0.034
SI_2	512 × 512	0.049	0.051	0.043	0.052	0.046	0.037
SI_3	1024 × 1024	0.061	0.051	0.046	0.051	0.045	0.037
SI_4	2048 × 2048	0.064	0.051	0.043	0.052	0.039	0.035

6. Conclusions

An image encryption technique for secure surveillance for IoT systems has been proposed in this paper. The image was made secure before the transmission from the surveillance system. A hyperchaotic map was utilized to obtain the pseudorandom sequences. The initial parameters of the hyperchaotic map were produced using PRNDO. The permutation was carried out through Arnold transform. Thereafter, a diffusion process was implemented to generate the encrypted images. The performance of the proposed framework was assessed by drawing the comparisons with competitive techniques based on security parameters. It was found that the proposed framework provides promising results as compared to the existing techniques. The proposed technique is able to resist against different attacks, such as noise and enhancement attacks. Experimental analyses showed that the proposed technique outperformed the competitive techniques in terms of visual analysis, quantitative analysis, security analysis, and execution time. As the proposed technique can encrypt and decrypt images at higher speeds, therefore, the proposed technique can be used for real-time secure surveillance systems.

Author Contributions: Conceptualization, G.G., K.V., D.A., S.V., D.B.R. and M.W.; data curation, K.V., D.A., S.V., D.B.R. and J.S.; formal analysis, G.G., K.V., D.A., S.V. and D.B.R.; funding acquisition, J.S. and M.W.; investigation, G.G., K.V. and D.A.; methodology, G.G., K.V., D.A., S.V. and D.B.R.; project administration, M.W., S.V., D.B.R. and J.S.; resources, K.V., D.A., S.V., D.B.R. and Z.M.; software, K.V., D.A. and S.V.; supervision, S.V., J.S. and M.W.; validation, S.V., D.B.R., J.S. and Z.M.; visualization, G.G., K.V. and D.A.; writing—review and editing, G.G., K.V., D.A., S.V., D.B.R. and J.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge contribution to this project from the Rector of Silesian University of Technology, Gliwice, Poland under the proauality grant no. 09/020/RGJ21/0007.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Jana Shafi would like to thank the Deanship of Scientific Research, Prince Sattam bin Abdul Aziz University, for supporting this work.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.H.G.; Baik, S.W. Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3679–3689. [CrossRef]
2. Khan, J.; Li, J.P.; Ahamad, B.; Parveen, S.; Haq, A.U.; Khan, G.A.; Sangaiah, A.K. SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption. *IEEE Access* **2020**, *8*, 15747–15767. [CrossRef]
3. Hamza, R.; Hassan, A.; Patil, A.S. A Lightweight Secure IoT Surveillance Framework Based on DCT-DFRT Algorithms. In Proceedings of the International Conference on Machine Learning for Cyber Security, Xi'an, China, 19–22 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 271–278.
4. Roy, S.; Shrivastava, M.; Pandey, C.V.; Nayak, S.K.; Rawat, U. Ievca: An efficient image encryption technique for iot applications using 2-d von-neumann cellular automata. *Multimed. Tools Appl.* **2020**, 1–39. [CrossRef]
5. Hussain, A.; Nazir, S.; Khan, F.; Nkenyereye, L.; Ullah, A.; Khan, S.; Verma, S.; Kavita. A Resource Efficient hybrid Proxy Mobile IPv6 extension for Next Generation IoT Networks. *IEEE Internet Things J.* **2021**, *1*, 3058982. [CrossRef]
6. Singh, A.P.; Pradhan, N.R.; Luhach, A.K.K.; Agnihotri, S.; Jhanjhi, N.Z.; Verma, S.; Kavita; Ghosh, U.; Roy, D.S. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5779–5789. [CrossRef]
7. Li, L.; Wen, G.; Wang, Z.; Yang, Y.-X. Efficient and Secure Image Communication System Based on Compressed Sensing for IoT Monitoring Applications. *IEEE Trans. Multimed.* **2019**, *22*, 82–95. [CrossRef]
8. Feixiang, Z.; Mingzhe, L.; Kun, W.; Hong, Z. Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain. *Opt. Laser Technol.* **2021**, *135*, 106610. [CrossRef]
9. Brahim, A.H.; Pacha, A.A.; Said, N.H. Image encryption based on compressive sensing and chaos systems. *Opt. Laser Technol.* **2020**, *132*, 106489. [CrossRef]
10. Talhaoui, M.Z.; Wang, X. A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Inf. Sci.* **2021**, *550*, 13–26. [CrossRef]
11. Yang, G.; Jan, M.A.; Rehman, A.U.; Babar, M.; Aimal, M.M.; Verma, S. Interoperability and Data Storage in Internet of Multimedia Things: Investigating Current Trends, Research Challenges and Future Directions. *IEEE Access* **2020**, *8*, 124382–124401. [CrossRef]
12. Javeed, A.; Shah, T. Attaullah Lightweight secure image encryption scheme based on chaotic differential equation. *Chin. J. Phys.* **2020**, *66*, 645–659. [CrossRef]
13. Sumit, K.; Ravishankar; Sahil, V. Context Aware Dynamic Permission Model: A Ret-rospect of Privacy and Security in Android System. In Proceedings of the International Conference on Intelligent Circuits and Systems, Phagwara, India, 19–20 April 2018; Springer: Berlin/Heidelberg, Germany, 2018.
14. Logeswaran, T.; Kalaivani, S.; Karunakaran, S.; Anand, L.V.; Kumar, K.V. The generalized non-linear fresnel transform and its application to image encryption. *Mater. Today Proc.* **2020**, *1*, 1.
15. Wang, B.; Zhang, B.; Liu, X. An image encryption approach on the basis of a time delay chaotic system. *Optik* **2021**, *225*, 165737. [CrossRef]
16. Tao, Y.; Cui, W.; Zhang, Z. Spatiotemporal chaos in multiple dynamically coupled map lattices and its application in a novel image encryption algorithm. *J. Inf. Secur. Appl.* **2020**, *55*, 102650. [CrossRef]
17. Wang, T.; Wang, M.-H. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. *Opt. Laser Technol.* **2020**, *132*, 106355. [CrossRef]
18. Wang, X.; Xue, W.; An, J. Image encryption algorithm based on tent-dynamics coupled map lattices and diffusion of house-hold. *Chaos Solitons Fractals* **2020**, *141*, 110309. [CrossRef]
19. Vijayalakshmi, B.; Ramar, K.; Jhanjhi, N.Z.; Verma, S.; Kaliappan, M.; Vijayalakshmi, K.; Vimal, S.; Kavita; Ghosh, U. An Attention Based Deep Learning Model For Traffic Flow Prediction Using Spatio Temporal Features Towards Sustainable Smart City. *Int. J. Commun. Syst.* **2021**, *34*, e4609. [CrossRef]
20. Wang, X.; Li, Y. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Opt. Lasers Eng.* **2021**, *137*, 106393. [CrossRef]
21. Kaur, M.; Kumar, V. Parallel non-dominated sorting genetic algorithm-II-based image encryption technique. *Imaging Sci. J.* **2018**, *66*, 453–462. [CrossRef]
22. Kaur, M.; Kumar, V. Beta Chaotic Map Based Image Encryption Using Genetic Algorithm. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850132. [CrossRef]
23. Kaur, M.; Singh, D.; Uppal, R.S. Parallel strength Pareto evolutionary algorithm-II based image encryption. *IET Image Process.* **2020**, *14*, 1015–1026. [CrossRef]
24. Kaur, M.; Kumar, V. Adaptive Differential Evolution-Based Lorenz Chaotic System for Image Encryption. *Arab. J. Sci. Eng.* **2018**, *43*, 8127–8144. [CrossRef]
25. Rani, P.; Kavita; Verma, S.; Nguyen, G.N. Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network. *IEEE Access* **2020**, *8*, 121755–121764. [CrossRef]
26. Kaur, M.; Singh, D.; Sun, K.; Rawat, U. Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. *Futur. Gener. Comput. Syst.* **2020**, *107*, 333–350. [CrossRef]

27. Kaur, M.; Kumar, V.; Li, L. Color image encryption approach based on memetic differential evolution. *Neural Comput. Appl.* **2019**, *31*, 7975–7987. [CrossRef]
28. Kaur, M.; Kumar, V. Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain. *IET Image Process.* **2018**, *12*, 1273–1283. [CrossRef]
29. Radanliev, P.; De Roure, D.C.; Nurse, J.R.C.; Montalvo, R.M.; Cannady, S.; Santos, O.; Maddox, L.; Burnap, P.; Maple, C. Future developments in standardisation of cyber risk in the Internet of Things (IoT). *SN Appl. Sci.* **2020**, *2*, 1–16. [CrossRef]
30. Fan, B.; Tang, L.-R. A new five-dimensional hyperchaotic system and its application in DS-CDMA. In Proceedings of the 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 29–31 May 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 2069–2073.
31. Yuan, H.-M.; Liu, Y.; Lin, T.; Hu, T.; Gong, L.-H. A new parallel image cryptosystem based on 5D hyper-chaotic system. *Signal Process. Image Commun.* **2017**, *52*, 87–96. [CrossRef]
32. Dang, H.-G. Parameter Identification of a New Hyper-chaotic System. In Proceedings of the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, China, 16–17 January 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 785–787.
33. Qiu, X.; Xu, J.-X.; Xu, Y.H.; Tan, K.C. A New Differential Evolution Algorithm for Minimax Optimization in Robust Design. *IEEE Trans. Cybern.* **2018**, *48*, 1355–1368. [CrossRef] [PubMed]
34. Mondal, B.; Mandal, T. A light weight secure image encryption scheme based on chaos & DNA computing. *J. King Saud Univ. Comput. Inf. Sci.* **2017**, *29*, 499–504.
35. Batra, I.; Verma, S.; Malik, A.; Kavita; Ghosh, U.; Rodrigues, J.J.P.C.; Nguyen, G.N.; Hosen, A.S.M.S.; Mariappan, V. Hybrid Logical Security Framework for Privacy Preservation in the Green Internet of Things. *Sustainability* **2020**, *12*, 5542. [CrossRef]
36. Li, W.; Chai, Y.; Khan, F.; Jan, S.R.U.; Verma, S.; Menon, V.G.; Kavita; Li, X. A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System. *Mob. Netw. Appl.* **2021**, *26*, 234–252. [CrossRef]
37. Rawat, N.; Kim, B.; Kumar, R. Fast digital image encryption based on compressive sensing using structurally random matrices and arnold transform technique. *Optik* **2016**, *127*, 2282–2286. [CrossRef]
38. Ramasamy, P.; Ranganathan, V.; Kadry, S.; Damaševičius, R.; Blažauskas, T. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map. *Entropy* **2019**, *21*, 656. [CrossRef] [PubMed]