symmetry

MDPI

Article

Cryptanalysis of an Image Encryption Algorithm Based on Combined Chaos for a BAN System, and Improved Scheme Using SHA-512 and Hyperchaos

Musheer Ahmad [1,*], Eesa Al Solami [2], Xing-Yuan Wang [3,4], M. N. Doja [1], M. M. Sufyan Beg [5] and Amer Awad Alzaidi [6]

1 Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India; mndoja@gmail.com
2 Department of Information Technology, University of Jeddah, Jeddah 21589, Saudi Arabia; eaalsulami@uj.edu.sa
3 School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
4 Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China; wangxy@dlut.edu.cn
5 Department of Computer Engineering, Aligarh Muslim University, Aligarh 202002, India; mmsbeg@eecs.berkeley.edu
6 Department of Information Systems, University of Jeddah, Jeddah 21589, Saudi Arabia; aalzaidi@uj.edu.sa
* Correspondence: musheer.cse@gmail.com or mahmad9@jmi.ac.in; Tel.: +91-112-698-0281

Received: 19 May 2018; Accepted: 12 June 2018; Published: 6 July 2018

Abstract: The issues of identity authentication and privacy protection of individuals in body area network (BAN) systems have raised much concern in past few years. To address the challenges of privacy protection in wireless BAN, an image encryption algorithm has been proposed recently by Wang et al. The encryption algorithm utilized two 1D chaotic maps to generate sub-chaotic matrices which are combined to perform encryption. The algorithm has good statistical encryption performance. However, a cautious inquiry finds that it has some underlying security defects. This paper evaluates the security of the Wang et al. encryption algorithm to show that it is totally breakable under proposed cryptanalysis and hence infeasible for privacy protection in BAN. It has been shown that the plain-image data can be recovered without any prior knowledge of secret key and plain-text. Furthermore, this paper also suggests an improved encryption scheme using secure hash algorithm SHA-512 for one-time keys and a 4D hyperchaotic system to subdue the security insufficiencies of the algorithm under study. The simulation results and analysis demonstrate that the improved image encryption scheme has excellent encryption quality, plain-image sensitivity, and resistance to possible cryptanalytic attacks.

Keywords: image encryption; body area networks; cryptanalysis; SHA-512; hyperchaotic system

1. Introduction

Wireless systems play pivotal role in the transmission of data and are utilized for numerous applications involving healthcare, communication, commerce, broadcasting, etc. The use of wireless networks and sensor technology facilitates the achievement of facile and swift data transmission. As an emerging area of wireless systems, body area network (BAN) systems make extensive usage of both sensor technology and wireless networks to sustain advances in several healthcare applications such as the endoscopic capsule, heart rate monitor, blood pressure monitor and clinical diagnosis [1, 2]. The BAN systems have immense potential for healthcare applications. For instance, wearable medical gadgets conduct real-time and steady vital monitoring so as to give instant alerts and updates pertinent to a patient's status. Thereafter, data is correlated with the patient's records in order to

be used in long-term care and intended clinical diagnosis. The healthcare applications involve the assemblage of large amounts of the patient's data in order to conduct their efficacious remote treatment. The accumulation of large amounts of data has raised severe security concerns regarding the privacy and reliability of individuals. Failure to sustain security may lead to an undermining of authenticity and, thus, may gravely affect the treatment process [3,4]. Hence, the sustenance of secured system is vital and perceiving innovative solutions to attain the utmost level of security is exigent for secure tele-diagnosis and treatment. Research is being performed by many scholars and academicians so as to design security methods in order to address the issues of authentication and protection of individuals in BAN [5–10].

Recently, there has been increased concern about the incorporation of chaotic systems for the design of medical image data in healthcare systems. Chaotic systems possess ergodicity, pseudo-randomness and also are profoundly dependent on a system's initial conditions and parameters [11]. Due to these features, chaotic systems are regarded as cogently fitted for the development of secure and robust image encryption methods. Therefore, the chaotic systems have been utilized to design the authentication, protection and encryption of medical data and identity of patients in healthcare systems [12–14].

The deployed security method should have the credibility to offer a high level of authentication and protection. Similarly, it should be competent to withstand possible threats. Cryptanalysis is an analytic investigation of security methods to unveil underlying defects based on which an attack procedure is designed [15,16]. Consequently, many security methods aimed at providing authentication, protection, and encryption in healthcare have been scrutinized under various attacks and found breakable. In cryptology, it is therefore advocated to design methods against possible cryptanalysis to have stronger security. Thus, the role played by cryptanalysts in spotlighting and eradicating defects in cryptosystems is indispensable for the progress of cryptology, as the cryptanalysis may results in improved security methods that overcome the existing flaws, defects, and bugs, etc., that ensure more robust and secure cryptosystems.

In [17], Alvarez et al. investigated the security strength of a medical image encryption system suggested in [18] and determined that the system does not practically work flawlessly and is breakable under the attack procedure detailed in [17]. Moreover, a more secure and practical way of protecting patient information is also suggested. Zhu gave an authentication scheme for telecare medical information systems (TMIS) [19], which was cryptanalyzed by Muhaya to show that the scheme suffers from an offline password guessing attack and smart card loss attack in [20]. To resolve the security issue of the Zhu scheme, an improved scheme with the feature of session key establishment and user anonymity was proposed. In [21], a two-factor mutual authentication scheme using elliptical curve cryptography was proposed for secure TMIS. However, Islam and Khan showed that this authentication scheme has security problems like the fact that it fails to provide strong authentication, to update the password perfectly in password change stage, and to resist a potential replay attack [22]. Islam and Khan also suggested security improvement in the authentication scheme. In [13], Fu et al. designed an image protection scheme using chaotic maps for secure delivery of radiological image data in picture archiving and communication system (PACS). However, the encryption scheme was found to be insecure and unfit for the security realization of medical image data by Zhang et al. in [23]. They successfully broke the Fu et al. scheme and, subsequently, security improvement was developed to fulfill the motives of secure transfer of data in a PACS environment. Later, the security of the same encryption scheme in [13] was re-investigated in multiple rounds by Chen and Wang in [24]. They suggested a differential cryptanalysis that can recover the permutation key and broke the multi-round encryption scheme of Fu et al. to indicate its insecurity.

In body area network systems, a large quantity of a patient's data is stored and wirelessly transmitted in the form of images. To protect the patient's information in a BAN system, Wang et al. proposed an image encryption algorithm recently in [14]. The algorithm utilized two different 1D chaotic maps to generate sub-chaotic matrices which are combined as a single matrix for the encryption

of the image data matrix and an encrypted image matrix results. The algorithm holds the merits of ample key space, high key sensitivity, uniform pixels distribution, and high entropy content in encrypted images. However, we found that the algorithm has some underlying security defects that make it weak and practically infeasible for securing medical images. The algorithm has the demerits of weak keys, fixed chaotic sub-matrices, and plain-image insensitivity. This paper reports the following main contribution to the literature.

- The security of the recent image encryption algorithm in [14] is scrutinized and some defects are unveiled.
- A total break of the algorithm is done under proposed simple cryptanalysis that recovers the plain-image and nullifies the claim of excellent attack resistance ability of the algorithm made in [14].
- An improved scheme is proposed based on SHA-512 and a 4D hyperchaotic system to settle the issues of plain-image insensitivity and weak keys with strong encryption quality.

The remaining content of the paper is arranged as follows: Section 2 gives a review of the Wang et al. image encryption algorithm. The security issues and defects are discussed in Section 3. The proposed cryptanalysis to break the algorithm and its computer simulation is provided in Section 4. Section 5 provides the improved encryption scheme with a brief of SHA-512 and hyperchaotic system; and performance analysis of proposed improved scheme is carried out in Section 6. Lastly, the conclusions of the work done in this paper are drawn in Section 7.

2. Wang et al. Image Encryption Algorithm

In the Wang et al. image encryption algorithm, the 1D chaotic logistic map and skew tent map given in Equations (1) and (2) are adopted for the generation of sub-chaotic matrices.

$$x_n = \mu \times x_{n-1} \times (1 - x_{n-1}) \tag{1}$$

$$y_n = \begin{cases} \frac{y_{n-1}}{a} & 0 < y_{n-1} \leq a \\ \frac{1-y_{n-1}}{1-a} & a < y_{n-1} \leq 1 \end{cases} \tag{2}$$

where $\mu \in [3.5699456, 4]$, $a \in [0.4, 0.5]$ are their control parameters, and $x_n, y_n \in [0, 1]$ $(n > 0)$ represents the respective state of maps as per the specifications in [14]. The initial condition y_0 $(=x_k)$ is the x state of map (1) after k iterations. The Wang algorithm to encrypt a plain-image I of size $M \times N$ has the following operational steps:

$E = Wang\_Encryption(I(i, j))$	
W.1.	Read the plain-image $I(i, j)$ and form its data matrix T of dimension $M \times N$.
W.2.	Set initial values of map (1) and generates 1D chaotic sequence $X = \{x_1, x_2, \ldots, x_{n1}\}$ of length $n_1 = M \times N_1$, where $N_1 = N - \text{ceil}(N/2)$
W.3.	Create a 2D sub-chaotic matrix SI from sequence X of Logistic map of size $M \times N_1$.
W.4.	Set initial values of map (2) and generates another 1D chaotic sequence $Y = \{y_1, y_2, \ldots, y_{n2}\}$ of length $n_2 = M \times N_2$, where $N_2 = N - N_1$
W.5.	Construct another 2D sub-chaotic matrix SK from sequence Y of size $M \times N_2$.
W.6.	Combine the two sub-chaotic matrices SI and SK to get 2D chaotic matrix $EC_{M \times N} = \{SI_{M \times N1}; SK_{M \times N2}\}$.

W.7.	Perform the XOR operation on data matrix T (of plain-image I) and chaotic matrix EC to get final encrypted image E as:
	for $i = 1$ to M do
	for $j = 1$ to N do
	$E(i, j) = bitxor(T(i, j), EC(i, j))$
	endfor
	endfor

W.8.	Exit

The decryption algorithm has similar steps but in reverse fashion. For further details the readers are refer to [14].

3. Security Defects

After careful investigation of the details of adopted chaotic maps and encryption algorithm under study, the following security defects are discovered and discussed.

3.1. Weak Keys

In chaos-based encryption methods, the selection of chaotic maps has an impact on the security. The parameters of adopted chaotic maps and secret key should have carefully established links and maps do not lead to the fixed points, otherwise the maps may fall in non-chaotic regions that weaken the encryption methods.

In [14], the logistic map was used which has the non-chaotic phenomenon when $\mu < 3.5699456$. Therefore, Wang et al. restrict the control parameter $\mu \in [3.5699456, 4]$ to explore the chaotic behaviour of the map (1). However, it is worth noting that this is a necessary but not sufficient condition for a logistic map to exhibit chaotic behaviour, as the map still has some non-chaotic regions that lead to insufficient encryption performance. This claim is justified by the bifurcation plot of map (1) for $\mu \in [3.6, 4]$ shown in Figure 1 which highlights the prevailing non-chaotic windows for the set of values of parameter μ considered in [14]. All such sets of μ values cause non-random behavior of sub-matrices and are considered as weak keys. Moreover, the logistic map has two fixed points $x = 0$ and $x = 1$ and as a result $x_n = 0$ for all subsequent n. Therefore, these two values should be avoided while selecting the initial condition x_0 for map (1), but these values have been taken as part of key space in the Wang et al. encryption algorithm, as $x_n \in [0, 1]$ is specified. For the computed two fixed points, the map generates a completely fixed sequence containing only zeros. Lastly, the logistic map has symmetric dynamics whether $x_n \in (0, 0.5]$ or $x_n \in [0.5, 1)$ as the map has two terms x_n and $(1 - x_n)$ whose product is $x_n(1 - x_n)$; now when we transform x_n by $(1 - x_n)$ then the resulting terms are $(1 - x_n)$ and x_n which again gives the same expression $(1 - x_n)x_n$. This means the sequence generated with $x = 0.35$ is exactly similar to the one generated with $x = 0.65$ for unchanged μ. In general, the same sequence will be generated for x_n and $(1 - x_n)$, making 50% of the keys component due to the initial condition of x effective i.e., equal to 50% of 10^{15}. The set of weak keys for map (1) due to x_0 and μ includes $k_1 = 0.5 \times 10^{15} - \Delta_1$ (Δ_1 is the set of all those values of μ for which map (1) falls in the non-chaotic regions).

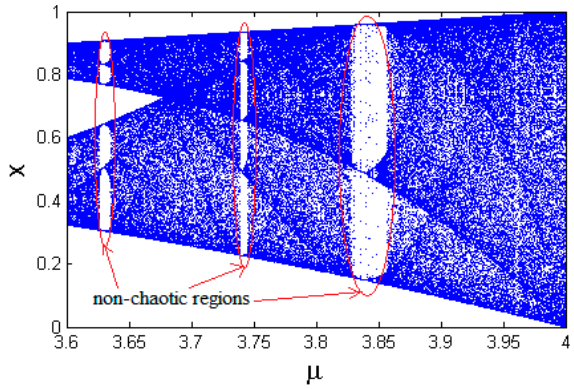


Figure 1. Bifurcation of logistic map in (1) for $\mu \in [3.6, 4]$.

The second map (2) also leads to non-chaotic behaviour under some possible practical cases. As with case A: when $y_n = a$, map (2) results to $y_{n+1} = y_n / a = 1$, thus a periodic fixed sequence of $\{y_n = a, 1, 0, 0, \ldots, 0\}$ will be generated. For case B: when $y_n \in (0, 0.5)$ and $a = 2y_n$, then a non-random

sequence $\{y_n, 0.5, 1, 0, 0, \ldots, 0\}$ is obtained from map (2). For case C: when $y_n \in (0, 1)$ and $a = 0.5$, a sequence with poor period is observed. In [14], the restriction on parameter a in interval [0.4, 0.5] reduces the key space component due to a being only 10% of 10^{15}. There are almost 10^{15} values out of possible pairs of $(y_0, a) = 10^{15} \times 10^{15}$ for case A, 0.5×10^{15} for case B, and Δ_2 for case C which must be avoided. Moreover, the x_k-th value of map (1) derives the initial condition y_0 of map (2). So, its component factor of 10^{15} should not be considered in key space. Hence, the set of weak keys for map (2) are $k_2 = 0.9 \times 10^{15} + 10^{15} + 0.5 \times 10^{15} + \Delta_2$.

In the Wang et al. encryption scheme the above analyzed two chaotic maps are adopted. Their assigned initial values derive the encryption effect. The effective key space of the encryption algorithm for components x_0, μ, a is reduced to $(4 - 3.5699456) \times 10^{45} - k_1 - k_2$ due to the above issues as a lot of weak keys $= k_1 + k_2 = 2.9 \times 10^{15} \approx 2^{52}$ out of 10^{45} may result in poor encryption quality. Hence, the algorithm in [14] has a large number of weak keys which may weaken the algorithm and the claimed key space of $(10^{15})^4 = 10^{60} \approx 2^{200}$ is impractical.

3.2. Sub-Chaotic Matrices SI and SK Are Fixed

The encryption operation in [14] depends on the set of assigned initial values of the logistic map and tent map only. If these values are kept unchanged, then the same X and Y sequences will get generated out of map (1) and (2), thereby the same 2D sub-chaotic matrices SI and SK will result. Hence, the final 2D chaotic matrix EC remains unaltered if the secret key kept is unchanged. This defect is quite serious and makes the algorithm susceptible to cryptanalysis performed in Section 4.

3.3. Lack of Sensitivity to Change in Plain-Image

To fetch strong Shannon's confusion and diffusion properties in any encryption system, the system should be able to carry perfect sensitivity to secret keys and plaintext as well. The algorithm under examination has good key sensitivity. However, it fails to provide ample sensitivity to changes in plain-image content. As desired in the encryption system, minor change in the plain image should bring drastic changes in the corresponding encrypted content. But, for Wang's encryption system if we change any pixel of the pending plain image, then the resulting encrypted image is found to have only one changed pixel at that same position as the rest of the encrypted pixels are as previously. For example, let us take a standard *Barbara* image I_1 shown in Figure 2a as plain image which is encrypted by algorithm in [14] and shown in Figure 2b as E_1. Then, we change only one pixel of I_1 at the central position and another plain image I_2 is obtained (depicted in Figure 2c); this new image I_2 is also encrypted with same algorithm and shown in Figure 2d as E_2. To our dismay, the difference between the two encrypted images is almost a black image except the central position pixel which was altered. This means that the change in plain image does not result in good confusion and diffusion, or else the difference image will be a random-like one. This defect proves that Wang's encryption algorithm has a lack of plain-image sensitivity.

(**a**) (**b**) (**c**) (**d**) (**e**)

Figure 2. Simulation of lack of plain-image sensitivity: (**a**) plain image I_1; (**b**) encrypted image E_1 of I_1; (**c**) plain image I_2; (**d**) encrypted image E_2 of I_2; (**e**) difference of two encrypted images E_1 and E_2.

4. Proposed Cryptanalysis

In [25], Schneier suggested that the attacker has to know the security flaws in a cryptosystem which can be explored by him to break the system partially or completely. Cryptanalysis can be unveiling licensed defects to prove that the method does not work as believed. A cryptographic security method deemed infeasible for secret communication and data protection if it has underlying defects that may lead to complete or partial identification of individual, or recovery of plain-text information. A cryptanalyst aims to frame methods to obtain information of either secret keys or plain text. The attack process may demand large storage or impractical images, but the computational cost of assaults ought to be not as high as a conventional exhaustive attack [15].

A Dutch cryptographer Auguste Kerckhoffs in the early 1880s annotated a principle that goes as "only secrecy of the key provides security" [26]. It is famously remarked as Kerckhoffs principle which ensures that the secrecy of only the key regulates the degree of security of any cryptosystem. Thus, most cryptanalysts accede to the fact that attacker has almost all details of cryptosystems. As a repercussion, in any case, the recovery of either the secret key or plain-text information is remarked upon as an absolute crack of a cryptosystem [25]. We highlighted and discussed a few security flaws and defects in Wang's image cryptosystem as part of our effort to break it. Here, we also propose a simple attack procedure by tapping the defects to demonstrate the complete break of image encryption in [14].

The image encryption algorithm under analysis is claimed to be feasible for privacy protection in BAN systems and excellent for resisting attacks. However, we invalidate these claims with proper evidence and justification. The shortcomings discussed in Sections 3.2 and 3.3 aid the attacker to mount the chosen plain-image attack. In [14], the encryption algorithm is operated to encrypt gray-scale images and color red-green-blue (RGB) images as well. Here, we provide the procedure to break the algorithm for gray-scale images and it can be applied for color images by handling each color components individually. To attack the algorithm, we need to have a black image—a gray-scale image in which all pixel values are zero let it be $A(i, j) = 0$ for all $i = 1{\sim}M$, $j = 1{\sim}N$. The illegal recovery of the plain image from its encrypted image C (C is the output image by algorithm in [14], let its plain image be denoted as P and unknown to us) without the secret key as follows. The black image A is now encrypted using *Wang_Encryption*() algorithm and the corresponding encrypted image is obtained as say, E. Since, for step W.7 in Section 2 the $T(i, j) = A(i, j)$, then $E(i, j) = bitxor(T(i, j), EC(i, j)) = bitxor(0, EC(i, j)) = EC(i, j)$ for all i, j. So, the encrypted image E is actually the chaotic matrix EC obtained by combining the sub-chaotic matrices SI and SK in step W.6. As a matter of fact, the matrix E is the equivalent secret key used by Wang's encryption algorithm when an image, whose encrypted-image is C, is encrypted. As merely an exclusive-bitwise XOR operation was performed during the pixels encryption stage for encrypting any image (which can be A or P or any other) by the chaotic matrix EC (which is now available to us). Hence, the plain image corresponding to encrypted image C can be recovered by performing the *bitxor*() operation on matrices E (or EC) and C. An example of the proposed attack on an arbitrary image of size 4 x 4 is illustrated below and is also simulated on a benchmark *Boat* image in Figure 3. As an attacker, we have encrypted image C and the temporary access to Wang's encryption and we need to retrieve the corresponding plain image of C without having secret keys.

$$C = \begin{pmatrix} 6 & 11 & 146 & 115 \\ 60 & 160 & 1 & 41 \\ 33 & 143 & 250 & 68 \\ 74 & 150 & 117 & 94 \end{pmatrix} \quad A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$E = Wang\_Encryption(A) = EC = \begin{pmatrix} 208 & 49 & 220 & 151 \\ 96 & 84 & 44 & 253 \\ 104 & 121 & 196 & 25 \\ 0 & 5 & 166 & 209 \end{pmatrix}$$

$$P = bitxor(C, EC) = \begin{pmatrix} 214 & 58 & 78 & 228 \\ 92 & 244 & 45 & 212 \\ 73 & 246 & 62 & 93 \\ 74 & 147 & 211 & 143 \end{pmatrix}$$

The recovered plain image corresponding to encrypted image C is P obtained above. This can be confirmed by the encrypted recovered image P with Wang's encryption and we get the same cipher image whose initial plain image was unknown to us as:

$$E = Wang\_Encryption(P) = \begin{pmatrix} 6 & 11 & 146 & 115 \\ 60 & 160 & 1 & 41 \\ 33 & 143 & 250 & 68 \\ 74 & 150 & 117 & 94 \end{pmatrix} = C$$

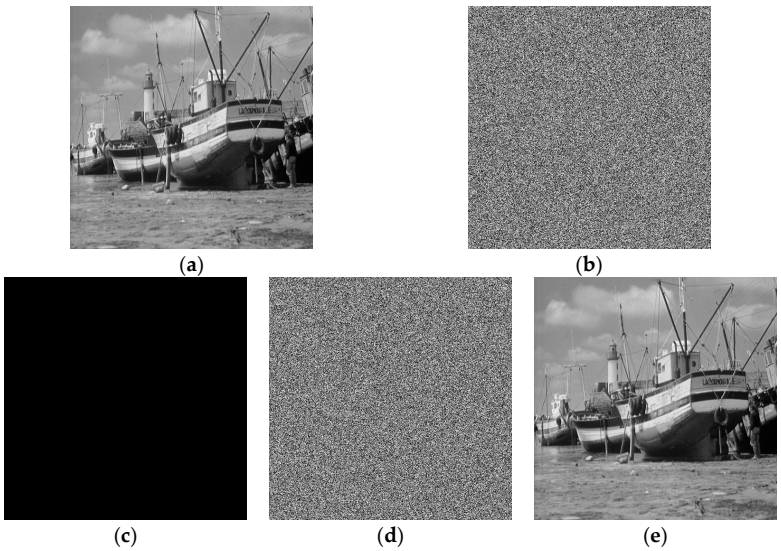


Figure 3. Simulation of attack method: (**a**) plain image P; (**b**) encrypted image C of P; (**c**) black image A; (**d**) encrypted image E (or EC) of black image A; (**e**) $bitxor(C, EC)$ the recovered plain image of encrypted image C without owning the secret key.

5. Proposed Improved Image Encryption Scheme

In this section, we present the proposed improved image encryption scheme using a 4D hyperchaotic system and SHA-512 which are described as follows.

5.1. 4D Hyperchaotic System

Most of the 1D chaotic maps suffer from problems of limited chaotic range and behaviour, non-uniform distribution of trajectory in phase space, low lyapunov exponent, and the existence of some non-chaotic windows [27]. High-dimensional, and in particular hyperchaotic, systems have larger key space (due to the great number of parameters and initial conditions), better sensitivity, more complex dynamics and high pseudo-randomness [28–31] compared to low-dimensional chaotic maps. To rule out the inadequacies of 1D chaotic maps used in [14], we employed a recent hyperchaotic

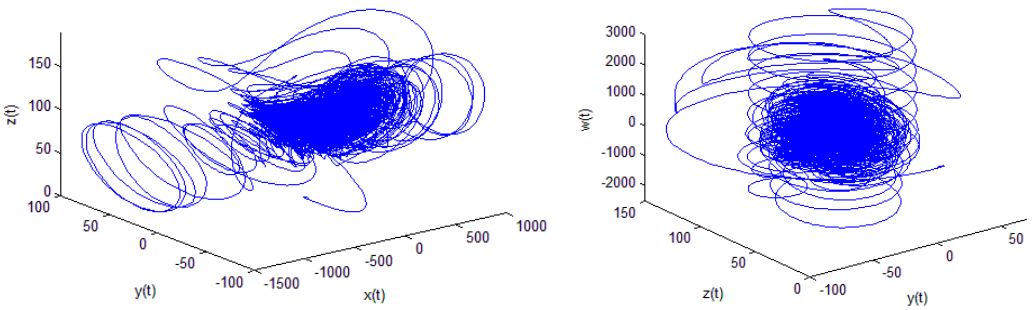
system that shows excellent complex chaotic dynamics and is suited for the design of a strong image encryption scheme. The 4D hyperchaotic system in [32] governs the following differential equations:

$$\begin{aligned} \dot{x} &= a(y - x - w) + byz \\ \dot{y} &= c(4x + y) - xz \\ \dot{z} &= dx - ez + xy \\ \dot{w} &= rx + f(3yz + y^2) \end{aligned} \tag{3}$$

where a, b, c, d, e, f, and r are system's control parameters. Interestingly, for the setting $a = 80$, $b = 45$, $c = 22$, $d = 5$, $e = 21$, $f = 8$ and $r = 100$, the four lyapunov exponents are $\lambda_1 = 25.6206$, $\lambda_2 = 11.2401$, $\lambda_3 = 1.717 \times {}^{10-5}$ and $\lambda_4 = -115.0336$. Note the presence of more than one positive lyapunov exponents which indicates the existence of hyperchaotic phenomenon in system (3). We applied the Runge–Kutta of order 4 to solve the system. This hyperchaotic system is adopted because of its following features:

- It consists of 7 system parameters, which enlarge heavily the key space of the respective security primitive and make the exhaustive attack impractical.
- It has a maximum lyapunov exponent of 25.6206 which is quite high and it is largest among all available 4D hyperchaotic systems. A larger positive lyapunov exponent shows that system trajectories vary more sharply in phase space and makes system's dynamics more complicated by establishing stronger sensitivity to initial conditions [32]. However, the lyapunov exponent of most of the 1D chaotic maps are less than 1, including the logistic map and skew tent map in (1) and (2).
- The range of Kaplan–Yorke dimensions for $60 \leq r \leq 166$ is $3.2801 \leq D_{KY} \leq 3.3241$, which is also much larger than most of the existing 4D hyperchaotic systems.
- It exhibits largest topological entropy, in hyperchaotic systems, which is not less than log(3).

The impressive lineaments of system (3) make it more distinctive than most existing hyperchaotic systems and hence more applicable for chaos-based cryptographic primitive designs. The complex dynamical behaviour of system (3) is described through its phase portraits shown in Figure 4.



(**a**) (**b**)

Figure 4. Phase portraits of hyperchaotic system (3) as (**a**) projection on x-y-z space; (**b**) projection on y-z-w space.

5.2. SHA-512

The hash algorithms SHA-2 are declared by the National Institute of Standards and Technology (NIST) as hash standards. These hash functions are primarily used as mapping that performs the compression of an input message of arbitrary length to a fixed digest. They are employed as security services for integrity protection and authentication. SHA-2 carries significant security enhancements over the previous SHA-1 family, emerging as a more robust version. It is worth mentioning that no significant attack and collisions on SHA-2 have been announced to date. The set of hash algorithms in the SHA-2 family includes SHA-224, SHA-256, SHA-384, and SHA-512 and generates digests of sizes

224, 256, 384, 512, respectively [33]. SHA-512 is one of the efficient member hash algorithm of SHA-2. It is quite unparalleled in the family as compared to other members, as it generates the largest hash digest of 512-bits, it offers the maximum attack complexity of 2^{256}, and it uses different shifts amounts and additive constant during its operation [34]. SHA-512 operates on eight 64-bit words. The message to be hashed is first padded with its length such that the result is a multiple of 1024-bits, and which is then parsed to 1024-bit message sub-blocks. The sub-blocks are treated iteratively one at a time beginning with a fixed initial hash value to return the final hash digest of 512-bits after processing all message sub-blocks.

5.3. Algorithm

In order to design an improved image encryption scheme, we used the SHA-512 hash function which is capable of generating an entirely different hash digest if infinitesimal alteration is conducted in the pending plain image due to its high sensitivity to the input image. Since, it is a highly one-way function, it is impractical to obtain the input message whose hash digest, through any means, is available to the attacker. A different hash digest will cause a different updating to the initial conditions and bifurcation parameter r of the hyperchaotic system (3). The updation of initial conditions of system (3) through the hash digest is executed to make the work of the attacker infeasible. Moreover, the pixel masking is carried out through a cipher-block chaining operation via internal variables s_{i-1}, β, g_{i-1} and the image information dependent function *circ-shift*(x, n) creates further complexity and dependency of the algorithm on image information to be encrypted for secure image transfer. This function circularly shifts the input argument x in the left direction by n number of positions and generates output. All these modifications in the algorithm make it highly robust, secure and statistically sound which will be discussed in Section 6.

The steps of operations involved in improved image encryption scheme are the following:

Step 1. Take proper input values for initial conditions $x(0)$, $y(0)$, $z(0)$, $w(0)$, parameters a, b, c, d, e, f, r.
Step 2. Read the plain image I (gray-scale or RGB image).
Step 3. Transform the input image I into 1D sequence of pixels of length say L (=MN for gray image and 3 MN for color image).
Step 4. Compute hash digest of 512-bits using SHA-512 on 1D image sequence I in Step 3, say H

$$H = H_1, H_2, H_3, \ldots, H_{63}, H_{64}$$

where, each $H_i = \{h_{i1}, h_{i2}, h_{i3}, ..., h_{i8}\}$ is i-th byte in hash H.
Step 5. Update the initial conditions of system (3) and parameter $r \in [60, 166]$ according to the following Formulas (4)–(8)

$$\hat{x}(0) = \left[x(0) + \frac{1}{256 \times 16} \left(\sum_{i=1}^{16} bin2dec(H_i) \right) \right] \mathrm{mod}(1) \tag{4}$$

$$\hat{y}(0) = \left[y(0) + \frac{1}{256 \times 16} \left(\sum_{i=17}^{32} bin2dec(H_i) \right) \right] \mathrm{mod}(1) \tag{5}$$

$$\hat{z}(0) = \left[z(0) + \frac{1}{256 \times 16} \left(\sum_{i=33}^{48} bin2dec(H_i) \right) \right] \mathrm{mod}(1) \tag{6}$$

$$\hat{w}(0) = \left[w(0) + \frac{1}{256 \times 16} \left(\sum_{i=49}^{64} bin2dec(H_i) \right) \right] \mathrm{mod}(1) \tag{7}$$

$$\hat{r} = (r)\mathrm{mod}(1) + [\lfloor r \rfloor + (H_7 \times H_{13} + H_{21} \times H_{31} + H_{37} \times H_{45} + H_{51} \times H_{62})]\mathrm{mod}(107) + 60 \tag{8}$$

where, the function $bin2dec(H_i)$ converts input binary data H_i to its equivalent decimal value.

Step 6. Iterate the hyperchaotic system (3) with updated initial conditions and parameter for L times to generate four chaotic sequences $X(i)$, $Y(i)$, $Z(i)$ and $W(i)$, where $i = 1$ to L.

Step 7. Do the following to perform masking operation on 1D image sequence $I = \{I_1, I_2, I_3, \ldots, I_L\}$ for $i = 1$ to L as

$$F_1 = \left[floor(X(i)) \times 10^{15}\right] \mathrm{mod}(256)$$

$$F_2 = \left[floor(Y(i)) \times 10^{15}\right] \mathrm{mod}(256)$$

$$F_3 = \left[floor(Z(i)) \times 10^{15}\right] \mathrm{mod}(256)$$

$$r = (r \times F_2 \times F3) \mathrm{mod}(1) + \left[floor(W(i)) \times 10^{15} + r\right] \mathrm{mod}(107) + 60 //\text{re-update } r \text{ for next iteration}$$

$$Q_i = [I_i \oplus F_1 + s_{i-1}] \mathrm{mod}(256) \oplus F_3 \oplus g_{i-1}$$

$$\delta = F_1 \oplus F_3$$

$$\beta = [\delta + s_{i-1}] \mathrm{mod}(256)$$

$$E_i = circ - shift(Q_i, [\beta] \mathrm{mod}(8))$$

$$g_i = E_i \oplus F_2$$

$$s_i = s_{i-1} + g_i$$

Step 8. Perform the inverse of Step 3 on 1D sequence E to get the encrypted image.

Step 9. Exit

The structure of the decryption procedure is to be followed as above but in reverse order.

6. Performance Analysis of Improved Scheme

In this section, we analyze and investigate the encryption and robustness performance of our proposed improved image encryption scheme. To undertake a fair analysis for comparison with scheme in [14] and others, we adopted the same Lena image of size $512 \times 512 \times k$ ($k = 1$ for gray-scale and $k = 3$ for color image) for simulation. In what follows, the results are investigated with respect to analyses such as histogram analysis, correlation of adjacent pixels analysis, number of pixel change rate (NPCR) and unified average changing intensity (UACI) analysis for plain-image sensitivity, image entropy analysis, and key space analysis. The initial setting for computer simulation using MATLAB is as: $a = 80$, $b = 45$, $c = 22$, $d = 5$, $e = 21$, $f = 8$, $r = 100$, $x(0) = 0.5$, $y(0) = 0.5$, $z(0) = 0.5$, $w(0) = 0.5$, $s_0 = 0$, $g_0 = 0$. The results of the encryption for the gray-scale and color Lena images are shown in Figures 5 and 6, respectively. It can be seen that encrypted images have high indistinguishability, visual distortion and are significantly different from their respective plain images.

(**a**) (**b**)

Figure 5. *Cont.*

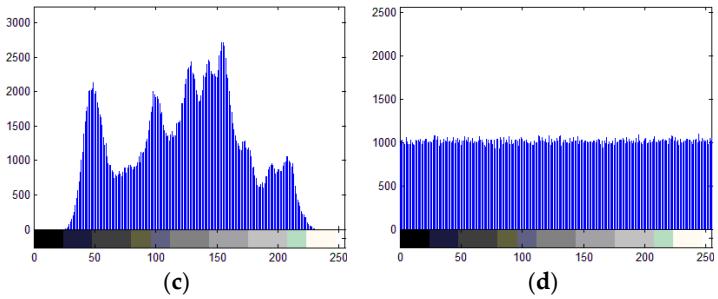


Figure 5. Encryption result for Lena gray-scale plain-image: (**a**) plain-image; (**b**) encrypted image; (**c**) histogram of plain image in (**a**); (**d**) histogram of encrypted image in (**b**).

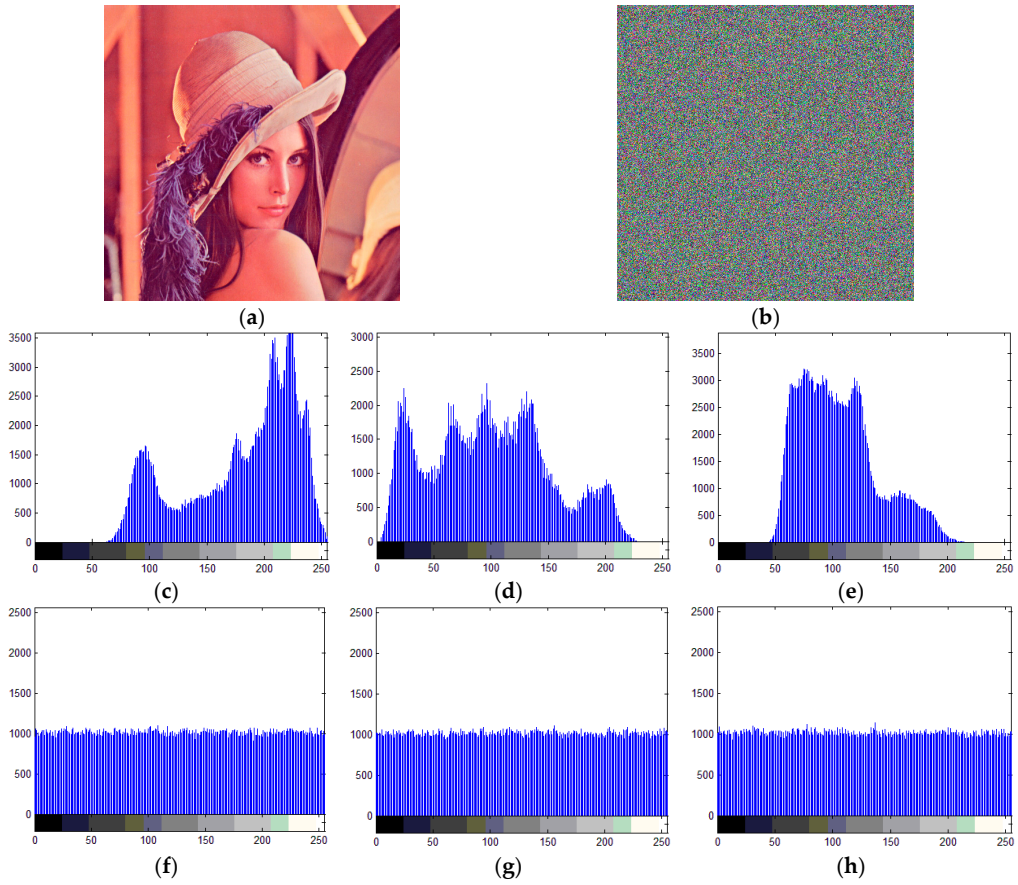


Figure 6. Encryption results for Lena color plain image: (**a**) color plain image; (**b**) encrypted color image; (**c**) histogram of plain *R* component; (**d**) histogram of plain *G* component; (**e**) histogram of plain *B* component; (**f**) histogram of encrypted *R* component; (**g**) histogram of encrypted *G* component; (**h**) histogram of encrypted *B* component.

6.1. Histogram Analysis

Histogram analysis refers to the study of distribution of pixel intensities of the image, where a pixel can have any of the 256 intensity levels. The histogram reveals the nature of distribution of image pixels i.e., whether the distribution is either uniform or non-uniform. For a strong image encryption algorithm, the histogram of a plain image and encrypted image must have considerable differences. It is desired that the histogram of the encrypted image should be as uniform in nature as possible in order to prohibit the attacker from gaining any information of the plain image or key from a non-uniform histogram of the encrypted image [35]. For gray images, the histograms of plain

and encrypted images are available in Figure 5a,b. For color images, the histograms are provided in Figure 6c–h. We can notice that these histograms for encrypted images are almost flat and uniform like the distribution of some noise data, completely different from the histograms of plain images; hence, the improved scheme is able to eradicate the chance of leaking any information to an attacker through histogram-based statistical attacks.

6.2. Pixels Correlation Analysis

The correlation coefficient measures the amount of persisting correlation among adjacent pixels of an image. It informs about the amount of visual distortion present in the image. The coefficient can range from -1 to $+1$. The pixels are said to be closely correlated to each other if the coefficient is found to have a value near ± 1. Conversely, the neighboring pixels are highly uncorrelated if the coefficient is close 0. Typically, a substantial correlation persists among adjacent pixels in meaningful multimedia images. For encrypted image content, a secure encryption scheme must be credible enough to root out the existing correlation among pixels and if the coefficient is closer to zero then the better the encryption effect [36]. The coefficient for adjacent pixels correlation is calculated as:

$$\rho = \frac{Cov(u,v)}{\sqrt{D(u)} \times \sqrt{D(v)}} \tag{9}$$

$$D(u) = \frac{1}{M \times N} \sum_{i=1}^{MN} (u_i - A(u))^2$$

$$A(u) = \frac{1}{M \times N} \sum_{i=1}^{MN} (u_i)$$

$$Cov(u,v) = \frac{1}{M \times N} \sum_{i=1}^{MN} (u_i - A(u))(v_i - A(v))$$

where, u and v are intensity values of two adjacent pixels in the image. To compute coefficient of correlation for the plain image and encrypted image, we selected 10,000 vertically adjacent pairs of pixels randomly. Using the discussed procedure for correlation analysis, the coefficient found for the plain Lena gray image is 0.9761, and for components of the plain Lena color image as 0.9716 (red), 0.9731 (green), 0.9414 (blue) which are fairly close to 1 indicating high correlation among the pixels. The correlation coefficients obtained for encrypted images are listed in Tables 1 and 2 to compare the results of this analysis with some existing image encryption algorithms. Evidently, the encrypted images using our improved scheme are able to decorrelate the adjacent pixels better as it offers the smallest coefficient than image encryption schemes investigated in [14,37–41].

Table 1. Correlation coefficients of adjacent pixels in encrypted Lena gray images.

Proposed	Ref. [14]	Ref. [37]	Ref. [38]
0.000329	−0.00114	0.0045	0.005497

Table 2. Correlation coefficients of adjacent pixels in three color components of encrypted Lena color images.

Component	Proposed	Ref. [14]	Ref. [39]	Ref. [40]	Ref. [41]
Red	0.000626	0.0027	0.0017	0.0026	−0.0031
Green	0.0000219	−0.0019	0.0027	0.0051	0.0160
Blue	−0.000475	0.0003	0.0043	0.0009	−0.0190

6.3. Image Entropy Analysis

Image entropy is an idealistic measure of the amount of randomness contained in an image. It also accounts for the uncertainty rather than certainty used to describe the texture of the image and its information content. If an image adopts all possible intensity levels with almost equal likelihood, the entropy of the image will be high and near ideal. In contrast, if the image has intensity levels with substantial deviations in their frequencies of occurrences, then the entropy of image will be quite low. A gray-scale image has possible intensity values ranging from 0 to 255 which can be encoded by 8-bits. The ideal entropy value for a gray-scale image is 8 and it corresponds to a perfect noise-image. Thus, for strong image encryption, the entropy of encrypted image should be as close to 8 as possible, and again the closer the better. This is because a high randomness would make it arduous for attacker to predict the pixel values, thereby fortifying the security [35,36]. Mathematically, the entropy is computed as:

$$entropy(S) = \sum_{i=1}^{256} prob(s_i) \log_2 \left(\frac{1}{prob(s_i)} \right) \tag{10}$$

where $prob(s_i)$ represents the probability of occurrence of intensity level $s_i \in [0, 255]$ for 8-bit encoded images. The computed entropy scores of the plain Lena gray image is 7.44737, and for components of the plain Lena color image as 7.2531 (red), 7.59403 (green), 6.96842 (blue). The entropies of encrypted images by different encryption schemes are listed in Tables 3 and 4 for gray and color images, respectively. It is apparent from the two tables that all entropy values are significantly close to the ideal value 8. However, the improved scheme still shows an upright performance compared to other encryption schemes in the tables as our entropy scores are slightly higher in most cases and, hence, can resist entropy-based attacks more diligently.

Table 3. Correlation coefficients of adjacent pixels in three color components of encrypted Lena images.

Proposed	Ref. [14]	Ref. [37]	Ref. [38]
7.999419	7.9964	7.999319	7.9994

Table 4. Entropies of three color components of encrypted Lena images.

Component	Proposed	Ref. [14]	Ref. [39]	Ref. [40]	Ref. [41]
Red	7.999328	7.9974	7.9898	7.99734	7.9993
Green	7.999322	7.9969	7.9901	7.99716	7.9993
Blue	7.999277	7.9884	7.9902	7.99688	7.9993

6.4. Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) Analysis for Plain-Image Sensitivity

A naïve encryption scheme controlled by a key can provide the sensitivity to even minor alterations in any key components. However, a strong image cryptosystem should be able to have high sensitivity to a minor change in the pending plain image too in order to qualify Shannon's requirement for high security. The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are two metrics primitively meant to measure the encrypted image's resistance to differential attacks. These test the number of changing pixels in an encrypted image when the difference between two plain images is subtle. In other words, they measure the sensitivity to change in the plain image offered by the anticipated image encryption scheme. Assuming two plain images I_1 and I_2 (which

have only one pixel difference to each other) and whose corresponding encrypted images are, let say, E_1 and E_2, respectively, the NPCR and UACI metrics are defined as:

$$NPCR(I_1, I_2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100 \tag{11}$$

$$UACI(I_1, I_2) = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{E_1(i,j) - E_2(i,j)}{255}\right| \times 100 \tag{12}$$

$$D(i,j) = \begin{cases} 0 & E_1(i,j) = E_2(i,j) \\ 1 & otherwise \end{cases}$$

The optimal sensitivity of an encryption scheme is professed by an NPCR score close to 99.6% and a UACI close to 33.6% [36,37]. The results obtained to gauge the sensitivity to change in input plain images and their effect in encrypted content are shown in Tables 5 and 6. Most of the scores are quite near to the respective optimal values as all NPCR $\geq$ 99.624 and UACI $\geq$ 33.425 for the proposed anticipated scheme. The performance of our scheme is excellent compared to [14], and comparable with some recently investigated encryption algorithms in [37–41].

Table 5. Results of the number of pixel change rate (NPCR) and unified average changing intensity (UACI) for Lena gray-image sensitivity.

	Proposed	**Ref. [14]**	**Ref. [37]**	**Ref. [38]**
NPCR	99.627	nearly 0	99.62	99.6002
UACI	33.452	nearly 0	33.48	33.463

Table 6. Results of NPCR and UACI for Lena color-image sensitivity.

Component		**Proposed**	**Ref. [14]**	**Ref. [39]**	**Ref. [40]**	**Ref. [41]**
Red	NPCR	99.627	≈0	99.613	99.647	99.60
	UACI	33.473	≈0	33.439	33.425	33.25
Green	NPCR	99.631	≈0	99.611	99.623	99.60
	UACI	33.496	≈0	33.465	33.275	33.28
Blue	NPCR	99.624	≈0	99.615	99.594	99.60
	UACI	33.478	≈0	33.469	33.439	33.31

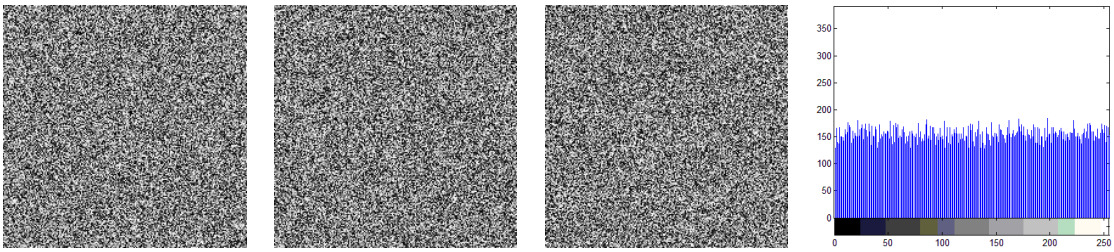


Figure 7. Simulation of sensitivity to one pixel change in the plain image for the proposed improved encryption scheme: (**a**) encrypted image of plain image in Figure 2a; (**b**) encrypted image of one pixel changed plain image in Figure 2c; (**c**) difference of two encrypted images in (**a**,**b**); (**d**) histogram of difference image obtained in (**c**).

As discussed earlier in Section 3.3, the Wang et al. algorithm [14] has a lack of plain-image sensitivity which is justified by their respective experimental scores provided in two Tables. We also performed the simulation analysis for plain-image sensitivity of the improved scheme similar to the one undertaken in Section 3.3. Therefore, we executed the improved scheme for two plain images shown in Figure 2a,c, differing by just one pixel, and as a result the encrypted images shown in Figure 7a,b are obtained. The difference between these two encrypted images is evaluated and shown as an image in Figure 7c. As we can observe, the difference image is like a random image in which pixels are uniformly distributed as in the case of any other encrypted image, see Figure 7d, which confirms the existence of excellent sensitivity of the improved scheme to a change in pending plain images.

As far as key sensitivity analysis is concerned, we confirmed that the improved scheme satisfies the optimal value of NPCR and UACI for a minute change of 10^{-10} in all floating-point components and +1 in integer components of the key, and the values are consistent with the values of Wang's algorithm.

The high sensitivity to plain images is due to the application of SHA-512 updating the initial conditions and the incorporation of some algorithm internal variables and operations that make it so vivid. SHA-512 offers the capability of exploring the idea of one-time keys that are entirely plain-image dependent that make the scheme resist the chosen plain image, known plain image, or chosen cipher image attacks. Thus, our improved image encryption scheme has strong power to thwart differential attacks through either a change in the key or a change in the plain image.

6.5. Key Space Analysis

The effective key space of the Wang et al. encryption algorithm is less than 10^{45} as analyzed in Section 3.1. Whereas the components of the secret key for our proposed improved scheme includes the four initial conditions, $x(0)$, $y(0)$, $z(0)$, $w(0)$, seven parameters a, b, c, d, e, f, r, all are floating-point numbers, and integers s_0, $g_0 \geq 0$. In order to avoid the problem of dynamic degradation, we carried out all floating point computation as per the IEEE-754 floating point standard of double-floating point arithmetic. Hence, for the working precision of 10^{-15}, our key space is found to be more than $10^{165} \approx 2^{548}$. Key space for our improved encryption scheme is decently large compared to key space of 10^{45} in [14], 2^{199} in [37,38], 2^{256} in [41,42], 2^{390} in [43], and 2^{203} in [44], and can withstand any exhaustive search attack more comfortably.

6.6. Computation Efficiency

It has been made evident that the computational resources involving time and storage required for an image encryption scheme is mainly dependent on floating point arithmetics [45]. The computational efficiency can be quantified by computing the average number of chaotic variables needed to achieve a robust and efficient security performance. In the proposed improved image encryption scheme, the hyperchaotic system is executed for L number of times which is equal to size 512×512 of the pending plain image and only one round of the encryption process is sufficient for strong performance. So, on average 4 chaotic variables are engaged to encrypt one pixel of image. This average count of 4 in our case is quite optimal compared to the average chaotic variable count of 9 in [46], 6 in [47], and 7 in [48] needed to encrypt only one pixel of image. Hence, our improved scheme also offers considerably good computation efficiency as compared to some state-of-the art image encryption schemes.

7. Conclusions

This paper evaluates the security of a recent image encryption algorithm which was primarily designed to support privacy protection in body area network systems. Our analysis scrutinizes the security unwrap to identify some underlying serious defects. Based on highlighted defects, we propose a complete break of the image encryption algorithm and affirm that the algorithm is not practically feasible to resolve the security issues in a critical BAN system. As a remedy, an improved image encryption scheme is suggested to overcome the defects of the algorithm under study. The improved scheme employs the features of the 4D hyperchaotic system and SHA-512. The hash function SHA-512

generates a hash digest for the pending plain image. This digest is used to revise the initial conditions of the hyperchaotic system and acts as one-time keys to make the algorithm statistically strong, robust and competent. Simulation analyses based on histograms, pixels correlations, image entropy, NPCR/UACI, and key space are conducted to quantify the encryption quality and robustness of the improved scheme. The performance results are also compared with some recent encryption algorithms. The simulation and comparative results show that improved scheme has strong security, high robustness and a better performance than some recent encryption algorithms. Hence, based on the outcomes of this paper, we recommend our improved image encryption algorithm over the Wang et al. algorithm for privacy protection of a patient's sensitive image data in BAN systems.

Author Contributions: This paper is the result of collaboration among all the authors in all aspects.

Funding: This research received no external funding.

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

References

1. Patel, M.; Wang, J. Applications, challenges, and prospective in emerging body area networking technologies. *IEEE Wirel. Commun.* **2010**, *17*, 80–88. [CrossRef]
2. Jovanov, E.; Milenkovic, A. Body Area Networks for Ubiquitous Healthcare Applications: Opportunities and Challenges. *J. Med. Syst.* **2011**, *35*, 1245–1254. [CrossRef] [PubMed]
3. Milenkovic, A.; Otto, C.; Jovanov, E. Wireless sensor networks for personal health monitoring: Issues and an implementation. *Comput. Commun.* **2006**, *29*, 2521–2533. [CrossRef]
4. Javadi, S.S.; Razzaque, M.A. Security and Privacy in Wireless Body Area Networks for Health Care Applications. *Signals Commun. Technol. Wirel. Netw. Secur.* **2013**, 165–187. [CrossRef]
5. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *IEEE Wirel. Commun.* **2010**, *17*, 51–58. [CrossRef]
6. Poon, C.; Zhang, Y.-T.; Bao, S.-D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun. Mag.* **2006**, *44*, 73–81. [CrossRef]
7. Ahmad, M.; Ahmad, T. A Framework to Protect Patient Digital Medical Imagery for Secure Telediagnosis. *Procedia Eng.* **2012**, *38*, 1055–1066. [CrossRef]
8. Zhang, Z.; Wang, H.; Vasilakos, A.V.; Fang, H. ECG-Cryptography and Authentication in Body Area Networks. *IEEE Trans. Inf. Technol. Biomed.* **2012**, *16*, 1070–1078. [CrossRef] [PubMed]
9. Shi, L.; Li, M.; Yu, S.; Yuan, J. BANA: Body area network authentication exploiting channel characteristics. *IEEE J. Sel. Areas Commun.* **2013**, *9*, 1803–1816. [CrossRef]
10. Zhao, Z. An Efficient Anonymous Authentication Scheme for Wireless Body Area Networks Using Elliptic Curve Cryptosystem. *J. Med. Syst.* **2014**, *38*. [CrossRef] [PubMed]
11. Carmen, P.-L.; Ricardo, L.-R. *Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem*; Applied Cryptography and Network Security: Intechopen, UK, 2012.
12. Sufi, F.; Han, F.; Khalil, I.; Hu, J. A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. *Secur. Commun. Netw.* **2010**, *4*, 515–524. [CrossRef]
13. Fu, C.; Meng, W.-H.; Zhan, Y.-F.; Zhu, Z.-L.; Lau, F.C.; Tse, C.K.; Ma, H.-F. An efficient and secure medical image protection scheme based on chaotic maps. *Comput. Biol. Med.* **2013**, *43*, 1000–1010. [CrossRef] [PubMed]
14. Wang, W.; Si, M.; Pang, Y.; Ran, P.; Wang, H.; Jiang, X.; Liu, Y.; Wu, J.; Wu, W.; Chilamkurti, N.; et al. An encryption algorithm based on combined chaos in body area networks. *Comput. Electr. Eng.* **2018**, *65*, 282–291. [CrossRef]
15. Ahmad, M.; Alam, M.Z.; Ansari, S.; Lambić, D.; Alsharari, H.D. Cryptanalysis of an image encryption algorithm based on PWLCM and inertial delayed neural network. *J. Intell. Fuzzy Syst.* **2018**, *34*, 1323–1332. [CrossRef]
16. Bard, G.V. *Algebraic Cryptanalysis*; Springer: Berlin, Germany, 2009.
17. Alvarez, G.; Li, S.; Hernandez, L. Analysis of security problems in a medical image encryption system. *Comput. Biol. Med.* **2007**, *37*, 424–427. [CrossRef] [PubMed]

18. Acharya, U.R.; Bhat, P.S.; Kumar, S.; Min, L.C. Transmission and storage of medical images with patient information. *Comput. Biol. Med.* **2003**, *33*, 303–310. [CrossRef]
19. Zhu, Z. An Efficient Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* **2012**, *36*, 3833–3838. [CrossRef] [PubMed]
20. Muhaya, F.T.B. Cryptanalysis and security enhancement of Zhu's authentication scheme for Telecare medicine information system. *Secur. Commun. Netw.* **2014**, *8*, 149–158. [CrossRef]
21. Xu, X.; Zhu, P.; Wen, Q.; Jin, Z.; Zhang, H.; He, L. A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. *J. Med. Syst.* **2013**, *38*, 1–7. [CrossRef] [PubMed]
22. Islam, S.H.; Khan, M.K. Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems. *J. Med. Syst.* **2014**, *38*, 1–16. [CrossRef] [PubMed]
23. Zhang, L.-B.; Zhu, Z.-L.; Yang, B.-Q.; Liu, W.-Y.; Zhu, H.-F.; Zou, M.-Y. Cryptanalysis and Improvement of an Efficient and Secure Medical Image Protection Scheme. *Math. Probl. Eng.* **2015**, *2015*, 1–11. [CrossRef]
24. Chen, L.; Wang, S. Differential cryptanalysis of a medical image cryptosystem with multiple rounds. *Comput. Biol. Med.* **2015**, *65*, 69–75. [CrossRef] [PubMed]
25. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*; John Wiley & Sons: Indianapolis, IN, USA, 2015.
26. Kerckhoffs's Principle. Available online: http://crypto-it.net/eng/theory/kerckhoffs.html (accessed on 13 February 2018).
27. Hua, Z.; Zhou, B.; Zhou, Y. Sine-Transform-Based Chaotic System with FPGA Implementation. *IEEE Trans. Ind. Electr.* **2018**, *65*, 2557–2566. [CrossRef]
28. Wang, X.-Y.; Zhang, H.-L. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. *Nonlinear Dyn.* **2016**, *83*, 333–346. [CrossRef]
29. Li, P.; Wang, X.-Y.; Fu, H.-J.; Xu, D.-H.; Wang, X.-K. A New Color Image Encryption Based On High-Dimensional Chaotic Systems. *Int. J. Mod. Phys. B* **2014**, *28*, 1450024. [CrossRef]
30. Ahmad, M.; Ahmad, T. Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys. *Int. J. Commun. Netw. Distributed Syst.* **2014**, *12*, 113. [CrossRef]
31. Liu, H.; Wang, X.-Y.; Kadir, A. Color image encryption using Choquet fuzzy integral and hyper chaotic system. *Optik* **2013**, *124*, 3527–3533. [CrossRef]
32. Chen, L.; Tang, S.; Li, Q.; Zhong, S. A new 4D hyperchaotic system with high complexity. *Math. Comput. Simul.* **2018**, *146*, 44–56. [CrossRef]
33. Maashri, A.A.; Pathuri, L.; Awadalla, M.; Ahmad, A.; Ould-Khaoua, M. Optimized Hardware Crypto Engines for XTEA and SHA-512 for Wireless Sensor Nodes. *Indian J. Sci. Technol.* **2016**, *9*, 1–7. [CrossRef]
34. Ahmad, I.; Das, A.S. Hardware implementation analysis of SHA-256 and SHA-512 algorithms on FPGAs. *Comput. Electr. Eng.* **2005**, *31*, 345–360. [CrossRef]
35. Wang, X.-Y.; Zhang, Y.-Q.; Bao, X.-M. A colour image encryption scheme using permutation-substitution based on chaos. *Entropy* **2015**, *17*, 3877–3897. [CrossRef]
36. Ahmad, M.; Alam, M. Z.; Umayya, Z.; Khan, S.; Ahmad, F. An image encryption approach using particle swarm optimization and chaotic map. *Int. J. Inf. Technol.* **2018**, *10*, 247–255. [CrossRef]
37. Chen, J.; Zhu, Z.; Fu, C.; Yu, H.; Zhang, L. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. *Commun. Nonlinear Sci. Numer. Simul.* **2015**, *20*, 846–860. [CrossRef]
38. Bashir, Z.; Wątróbski, J.; Rashid, T.; Zafar, S.; Sałabun, W. Chaotic Dynamical State Variables Selection Procedure Based Image Encryption Scheme. *Symmetry* **2017**, *9*, 312. [CrossRef]
39. Dong, C. Color image encryption using one-time keys and coupled chaotic systems. *Signal Process. Image Commun.* **2014**, *29*, 628–640. [CrossRef]
40. Liu, H.; Kadir, A.; Gong, P. A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise. *Opt. Commun.* **2015**, *338*, 340–347. [CrossRef]
41. Chai, X.-L.; Gan, Z.-H.; Lu, Y.; Zhang, M.-H.; Chen, Y.-R. A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. *Chin. Phys. B* **2016**, *25*, 100503. [CrossRef]
42. Chai, X.; Gan, Z.; Yang, K.; Chen, Y.; Liu, X. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process. Image Commun.* **2017**, *52*, 6–19. [CrossRef]

43. Zhu, C.; Sun, K. Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps. *IEEE Access* **2018**, *6*, 18759–18770. [CrossRef]
44. Wu, X.; Wang, K.; Wang, X.; Kan, H.; Kurths, J. Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Process.* **2018**, *148*, 272–287. [CrossRef]
45. Wong, K.-W.; Kwok, B.S.-H.; Yuen, C.-H. An efficient diffusion approach for chaos-based image encryption. *Chaos Solitons Fractals* **2009**, *41*, 2652–2663. [CrossRef]
46. Mao, Y.; Chen, G.; Lian, S. A Novel Fast Image Encryption Scheme Based On 3D Chaotic Baker Maps. *Int. J. Bifurc. Chaos* **2004**, *14*, 3613–3624. [CrossRef]
47. Zhang, W.; Wong, K.-W.; Yu, H.; Zhu, Z.-L. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 2066–2080. [CrossRef]
48. Wang, Y.; Wong, K.-W.; Liao, X.; Xiang, T.; Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos Solitons Fractals* **2009**, *41*, 1773–1783. [CrossRef]