# Securing Data in Wireless Body Area Network Using Hyper-Chaotic Zhou System

**Hasan Falah Hasan**
Dept. of Computer Engineering / College of Engineering/ Iraqi university.
hasanfalahh@gmail.com

**Received in: 27/November/2017, Accepted in:3/January/2018**

## Abstract

E-Health care system is one of the great technology enhancements via using medical devices through sensors worn or implanted in the patient's body. Wireless Body Area Network (WBAN) offers astonishing help through wireless transmission of patient's data using agreed distance in which it keeps patient's status always controlled by regular transmitting of vital data indications to the receiver. Security and privacy is a major concern in terms of data sent from WBAN and biological sensors. Several algorithms have been proposed through many hypotheses in order to find optimum solutions. In this paper, an encrypting algorithm has been proposed via using hyper-chaotic Zhou system where it provides high security, privacy, efficiency and capacity in terms of long key space that ensures high resistance possibly obtained by any threat attack, key sensitivity is too high to any slight of change could be made in the encryption key and finally good statistical characteristic's analysis where the software has been used is Microsoft visual studio version 10.

**Keywords:** WBAN, Security, Hyper-chaotic Zhou System, Encryption Algorithm.

https://doi.org/10.30526/31.1.1833

# Introduction

Wireless body area network (WBAN) is an advanced technology that mainly aims to improve E-healthcare systems. It is a promising emerging technology that provides accuracy, availability and efficiency of medical treatment via the advancements in wireless communications and electronics in which it is offering small and intelligent WBAN sensors as a potential and important in the delivery and monitoring of healthcare data [1 & 2]. WBAN considering a miniaturized low power devices and biological sensors in order to be accompanied with patients via several methodologies like to be worn or implanted in the patient's body. The evolution of WBAN is providing such great E-healthcare services in terms of collecting and processing biological data [3 & 4]. It can be classified as an embedded technology due to its implantable ability without hassling patients and even, it keeps their health condition always under control via sending patients sensitive information to the receiver in agreed transmitted distance while all biological signs are being measured regularly. WBAN sensors provides several indications like body temperature, blood pressure, hart pulse ratio…etc. it can be used in the medical and non-medical applications where it optimizes sensor nodes performance [3 & 5]. In order to get the maximum benefits from WBAN information provided the flow of data must be in continuous mode and treated in a real-time mode. This information must be observed and sorted by authorized personnel only like medical staff, insurance companies and governmental parties to be able to achieve such decision might be required [6]. Users are producing vital sign information where they are very special and can only be accessed by licensed agencies. Security is a sensitive point in WBAN, which it supports identity authentication, privacy protection and information integrity [1,2 & 6]. Security and privacy of patient’s data is a major challenge facing WBAN where it needs to be seriously considered. Several encryption techniques to increase security and privacy have been applied where the at most significant method can be used is chaos-based encryption due to its special properties. Chaos based encryption have been introduced in the late of eighties in the last century; since then; several researchers have obtained researches and analyzing huge number of chaos based encryption algorithms; they have been encouraged by the chaotic features such as topological transitivity, orbit inscrutability, sensitivity to initial conditions and control parameters, pseudo-randomness. Traditional encrypting algorithms are sensitive to keys in which, few detailed constructions are demanded in order to approach secured and satisfied chaos based encryption [7 & 8] Hyper-chaotic systems can be appointed to enhance the Security cases into any proposed cryptosystem [7, 8 & 9]. Better chaotic features can be provided from higher dimensional chaotic systems with higher dimensional attractors. Hyper-chaotic system earns more than one positive Lyapunov exponent show ever; it is improving security of encryption via producing more complexity, sensitivity to initial parameter and randomness [10, 11 & 12]. As this system can be as dynamics of continuous described by nonlinear differential equation and integrate to obtain trajectories however, there are several methods to solve it. Fourth order Runge Kutta (RK4) is the best numerical mode used to resolve the continuity in hyper-chaotic system models due to, it produces a precise solution evaluation [9,13,14 & 15]. In this paper, we using hyper-chaotic Zhou system for producing chaotic encryption key schema for sensitive data encryption of WBAN which can obtain a large key space, high key sensitivity and excellent ability of resistance to attacks. This article remainder is formed in an accurate order. In part 2, the hyper-chaotic Zhou systems are described. Part 3 presents the proposed encryption algorithm. In part 4, we evaluate the empirical results of real images with different metrics. Part 5 draws conclusions.

https://doi.org/10.30526/31.1.1833

## Hyper-chaotic Zhou System

Hyper-chaotic Zhou System is the most significant model of hyper-chaotic systems. The hyper-chaotic Zhou continuous nonlinear differential is described by system's equation (1), [15,16]:

$$\left.\begin{aligned} &\dot{X}_1 = a\,(X_2 - X_2) + X_4 \\ &\dot{X}_2 = c\,X_2 - X_1X_3(1) \\ &\dot{X}_3 = -bX_3 + X_1X_2 \\ &\dot{X}_4 = d\,X_1 - 0.5X_2X_3 \end{aligned}\right\} \qquad 1$$

the cases are $X_1$; $X_2$; $X_3$ and $x_4$meanwhile constants are $a$; $b$; $c$ and $d$, considered as the positive values of the system. The Zhou system show hyper-chaotic conduct when the parameter values are going to be:
a = 35; b = 3; c = 12; 0 < d < 34,5.

The hyper-chaotic is stating portrait of the system equation.1 is illustrated in figure (1), where d has been chosen to equal 1 [12].

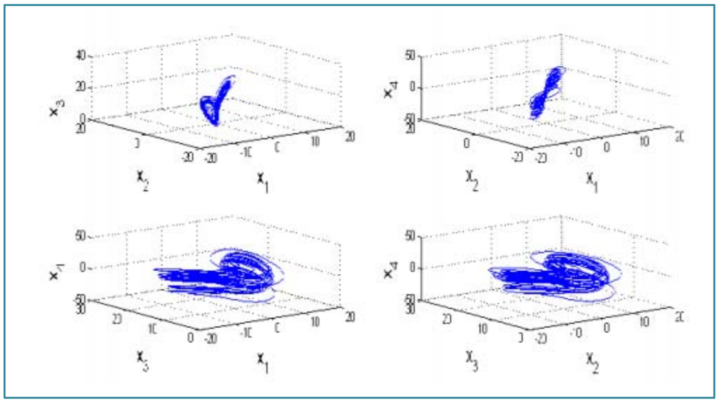

**Figure (1): Hyper-chaotic Zhou system**

## Proposed Algorithm

Huge amount of sensitive biological data resulted from transmitting process via node sensors is stored as image, therefore, the use of image form is a demand to be used in order to describe and experiment the encryption algorithm. The proposed algorithm consists of two main stages, chaotic key producing based on (HZS) and image encryption. Figure (2) presented the main stages of proposed algorithm.

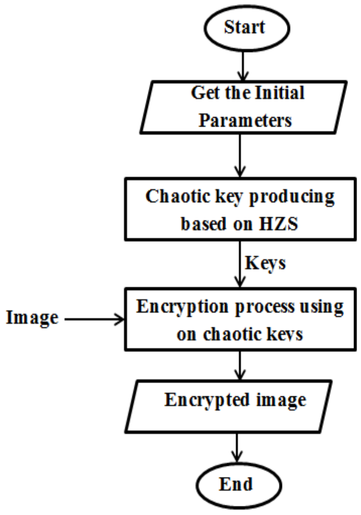
Start
Get the Initial Parameters
Chaotic key producing based on HZS
Keys
Image
Encryption process using on chaotic keys
Encrypted image
End

**Figure (2): Main stages of proposed algorithm.**

## Chaotic key producing based on HZS

Chaotic key produced by Hyper-chaotic Zhou System as this system has large positive Lyapunov exponent more than hyper-chaotic systems where complexity and unpredictability is high. This system consists of four non linear continuous differential equations.In order to solve these equations, we have used fourth order runge-kutta method in which this method is a numerical method that used for resolving continuous nonlinear differential hyperchaotics equation due to producing more accurate solution estimated. Producing chyaotic key is explained based on **(HZS)** and solved via fourth order Runge Kutta(Rk 4) in details via multi steps asexpressed below:

***Step1*:**

pre-round equation (1) for r time, r is constant to calculate the following hyper-chaotic Zhou solution values. Defined by the following system equations (2):

$$\left.\begin{aligned} x_{1r+1} &= x_{1r} + \frac{T}{6}(z_0+2z_2+2z_3+z_4) \\ x_{2r+1} &= x_{2r} + \frac{T}{6}(h_0+2h_2+2h_3+h_4) \\ x_{3r+1} &= x_{3r} + \frac{T}{6}(o_0+2o_2+2o_3+o_4) \\ x_{4r+1} &= x_{4r} + \frac{T}{6}(u_0+2u_2+2u_3+u_4) \end{aligned}\right\} \qquad (2)$$

Where z, h, o,and u are initial slop f RK (4), i=1,2,3,4 and T is time step

If i=1 then

$$\boxed{\begin{aligned} &zi= a\,(X_{2r}- X_{1r})+ X_{4r} \\ &h_i = c\,X_{2r} - X_{1r}\,X_{3r} \\ &o_i= -b\,X_{3r} + X_{1r}\,X_{2r} \\ &u_i= d\,X_{1r}+0.5\,X_{2r}\,X_{3r} \end{aligned}}$$

If i=2, 3

$$\boxed{\begin{aligned} &zi =a[\,(X_{2r} + (t^*h_{i--1}/2)) - (X_{1r} + (t^*z_{i--1}/2))\,] + (X_{4r} +(t^*u_{i--1}/2\,)\,) \\ &h_i =c(X_{2r} + (t^*h_{i--1}/2))-(\,(X_{1r} + (t^*z_{i--1}/2))+(\,X_{3r} + (t^*o_{i--1}/2)\,) \\ &o_i = -b(X_{3r} + (t^*o_{i--1}/2)) + (\,(X_{1r}+ (t^*z_{i--1}/2))^*(X_{2r}+ (t^*h_{i--1}/2)) \\ &u_i = d(X_{1r} + (t^*z_{i--1}/2)/2)+0.5((X_{2r}+ (t^*h_{i--1}/2))^*(X_{3r}+ (t^*o_{i--1}/2)) \end{aligned}}$$

then

https://doi.org/10.30526/31.1.1833

If i=4 then

$$\begin{aligned}
&zi =a[ (X_{2r} + (t*h_{i-1})) - (X_{1r} + (t*z_{i-1})) ] + (X_{4r} +(t*u_{i-1} ) )\\
&h_i =c(X_{2r} + (t*h_{i-1}))-( (X_{1r} + (t*z_{i-1}))+( X_{3r} + (t*o_{i-1}) )\\
&o_i = -b(X_{3r} + (t*o_{i-1})) + ( (X_{1r}+ (t*z_{i-1}))*(X_{2r}+ (t*h_{i-1}))\\
&u_i = d(X_{1r} + (t*z_{i-1}))+0.5((X_{2r}+ (t*h_{i-1}))*(X_{3r}+ (t*o_{i-1}))
\end{aligned}$$

***Step2:***

Beyond hyper-chaotic Zhou system is rounded in continuous mode where the outcomes of four decimal fractions x1; x2; x3; x4 will be created. Decimal values are preprocessed initially in order to get the chaotic key sequence using the following equation (3):

$$X_{I; r}= (mod ((abs (X_{i; r})–ceil (abs (X_{i; r}))) \times 10^{14}; L)) \qquad (3)$$

*Where i= {1,2,3,4}*, ***r*** (rounds number) of the hyper-chaotic based system; abs ($X_{i}$,*r*) returns the absolute value of ($X_{i}$, *r*). Ceil ($X_{i, r}$) returns the value of x to the nearest integers higher than or equal to x, mod ($X_{i}$,*r*, L) returns the remainder after division, and *L* is the color level (*L*=256 where 256 grey-scale image). Equation outcomes are representing four chaotic keys for each round (r) that used to encryption.

## Encryption Algorithm based on chaotic key based (HZS)

At this stage, presuming the size of patient ordinary-image P is M×N. Considering the image P can be converted into its three components: Rp, Gp and Bp in which, the size of each color's matrix (Rp, Gp and Bp) is M ×N too. Pixel's value is an integer within the range of {0, 1… 255}. The image P encryption scheme using chaotic keys in each round of hyper-chaotic Zhou map, four keys will be maintained as illustrated in previous subsection (3.1) where those keys will be used to encrypt image P in terms of choosing three random keys from the resulted four keys based on first key as shown in the following formula:

$$Cx_{1, r} = mod (x_{1, r}, 4). \qquad (4)$$

Where $X_{1}$,*r* represents first sub key of the hyper-chaotic system, r is the number of rounds .Consecutive number used to choose keys and , $Cx_{1, r} \in [0, 3]$. From equation (3) generates the following data list:

| |
|---|
| *If $Cx_{1, r}$ =0 then choosing key {x1r, x2r, x3r}* |
| *If $Cx_{1, r}$ =1 then choosing key {x1r, x2r, x4r}* |
| *If $Cx_{1, r}$ =2 then choosing key {x1r, x3r, x4r}* |
| *If $Cx_{1, r}$ =3 then choosing key {x2r, x3r, x4r}* |

The selection done according to data list as the following example: If *$Cx_{1, r}$ =0 then* (*{x1r, x2r, x3r*) is applied to do encryption. According to the following formula:

$$\begin{aligned}
CRp (I; j) &=Rp (I; j) \oplus x1r,\\
C\ Gp (I; j) &=Gp (I; j) \oplus x2r \qquad (5)\\
C\ Bp (I; j) &=Bp (I; j) \oplus x3r,
\end{aligned}$$

Where i= {1……, M}; j= {1……, N}; ⊕ represents the exclusive OR; C Rp (I; j); C Gp (I; j); C Bp (I; j) cipher components image, and Rp (I; j);Gp (I; j);Bp (I; j) original components of image and then ciphered image C will be sent to the receiver side. Receiver side will decipher the image C where the encryption and decryption algorithm are likely similar.

## Empirical Results

Patients data image received from WBAN sensors are encrypted via the proposed encryption algorithm based on (HZS). It was performed where the empirical analysis of the proposed

https://doi.org/10.30526/31.1.1833

algorithm approaching in this paper has been processed with ‘Lenna.jpg’ as the test image. The results can be illustrated as follow:

## Key Sensitivity Analysis

The sensitivity of the key is a major feature of the proposed encryption algorithm, sensitivity evaluation of the chaotic key, figure (3a) expressing the sampled image "Leena.bmp", Figure (3b) is encrypted using a chaotic key with (initial control parameter ($a = 35$; $b = 3$; $c = 12$; $d=1$) and initial key ($x_0 = 10$; $y_0 = 20$; $z_0 = 3$; $w_0 = 40$), round R=20). Figure (3c), decrypted image using the identical chaotic key, however, slight change in initial key will create an unforeseen result. An example in figure (3d) illustrating the decrypting of the image by changing the initial key, initial control parameter ($a = 35$; $b = 3$; $c = 12$; $d=1$) and initial key ($x_0 = 10.00001$; $y_0 = 20.00001$; $z_0 = 30.00001$; $w_0 = 40.00001$). From the above results, it has proven that, a slight change occur in the key will create unlikely decrypted image resulted and original image cannot be obtained.

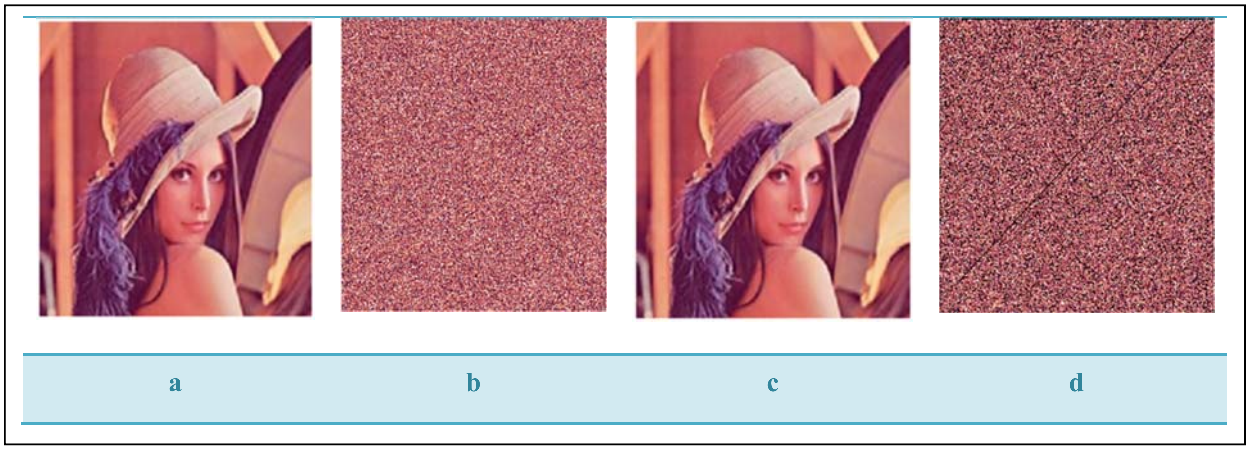

**Figure (3): Proposal Results**

## Key Space Analysis

The proposed algorithm architecture ability has been designed to withstand against any attacks due to algorithm's key space is ($10^{70}$) in which it works based on five initial values for the hyper-chaotic *(x0; y0; z0; w0;r)* as the authentic key. Each digit has fourteen digital numbers that’s why a great ability to resist attacks.

## Test Criteria

A set of test criteria are used to prove the proposed algorithm ability in terms of hiding the pure image meanwhile, when reconstruct original image from deciphered source where results obtained are shown on table (1). Criteria considered to test are MSE (Mean Square Error); SNR (Signal to Noise Ratio) and finally PSNR (Peak Signal to Noise Ratio) between main and ciphered image. From table (1); large MSE values are caused large error between original image and cipher image while smaller values of SNR and PSNR able to hide pure image information resulted in high image suppression of the original image information.

**Table (1): Results obtained from the proposed algorithm**

| *CriteriaName* | *MSE*<br>*averagesof (red; green; blue)* | *SNR*<br>*averages of (red; green; blue)* | *PSNR*<br>*averages of (red; green; blue)* |
|---|---|---|---|
| *Leena.jpg* | 3981.175 | 8.1 | 12.23 |

As stated in table (1), the results acquired in respect of MSE, SNR and PSNR are acceptable. These results prove the efficiency of the proposed algorithm.

## Conclusion

Security and privacy protection is a sensible issue in WBAN systems. This paper proposes an encryption algorithm based on hyper-chaotic Zhou system to support the privacy protection of WBAN systems. The proposed algorithm is balancing inconsistency between the operation's accuracy and algorithm's security in encryption scope. The proposed algorithm, hyper-chaotic Zhao system is optimized in order to produce chaotic key that used by encryption algorithm. Empirical results acquired are proven such potential ability of acquiring good influence in both encrypting and decrypting modes used in WBAN systems. Large key scheme provided by the proposed algorithm is highly sensitive to any small change could be happen. Based on MSE, large values give a successful indication by the proposed key in terms of concealing pure image information; meanwhile results obtained from SNR and PSNR shows large noise caused by the proposed key. Future wok can be applied into several aspects where security is a main player in all computing technologies. It can be used in securing cloud computing frameworks that serve and participate in medical and non-medical applications.

## References

[1] R. Negra ; I. Jemili and A. Belghith. Wireless Body Area Networks: Applications and Technologies. Procedia Computer Science, *83*,.1274–1281, 2016.

[2] N. D. Han; L. Han; D. M. Tuan; H. P. In and M. Jo. A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks. Information Sciences, *284*,.157–166, 2014.

[3] G. H. Zhang; C. Chung; Y. Poon; Y. T. Zhang; H. Abdel-Wahab; R. Montemanni, and H. M. Sun. A Review on Body Area Networks Security for Healthcare. International Scholarly Research Network ISRN Communications and Networking, 8(1), 2011.

[4] J. Undercoffer; S. Avancha; A. Joshi and J. Pinkston. Security for Sensor Networks. Kluwer Academic Publishers Norwell,.253–275, 2004.

[5] M. Masdari;S. Ahmadzadeh, andM. Bidaki. Key management in wireless Body Area Network: Challenges and issues. Journal of Network and Computer Applications, 91May 2016,.36–51, 2017.

[6] W. Wei; S. Miaomiao; P. Yu; R. Peng andW. Huiqiana. An encryption algorithm based on combined chaos in body area networks. Computers & Electrical Engineering, 0,.1–10, 2017.

[7] G. Gao; X. Peng; Y. Tian,and Z. Qin. A Chaotic Maps-Based Authentication Scheme for Wireless Body Area Networks,.1–18, 2016.

https://doi.org/10.30526/31.1.1833

[8] X. Li; J. Peng; S. Kumari;F. Wu; M. Karuppiahand Raymond K. K. Choo. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Computers and Electrical Engineering, 61.238–249, 2017.

[9] T. Gao and Z. Chen. A new image encryption algorithm based on hyper-chaos. *Physics Letters* A, *372*(4),.394–400, 2008

[10] X. Deng; C. Liao; C. Zhu, andZ. Chen. A Novel Image Encryption Algorithm Based on Hyperchaotic System and Shuffling Scheme. 2013 IEEE 10th International Conference on High Performance Computing and Communications *and* 2013 IEEE International Conference on Embedded and Ubiquitous Computing,.109–116, 2013.

[11] N. Khalifa; R. L. Filali, and M. Benrejeb. On secure image transmission combining chaotic encryption and watermarking using dead beat synchronization of 4D Henon maps. *3rd* International Conference on Control, Engineering and Information Technology, CEIT 2015, 4–7, 2015.

[12] M. Junming, &Y. Ruisong. An Image Encryption Scheme Based on Hybrid Orbit of Hyper-chaotic Systems. International Journal of Computer Network and Information Security, *7*(5), 25–33, 2015.

[13] S. Sadoudi; C. Tanougast; M. Azzaz, and A. Dandache. "Design and FPGA implementation of a wireless hyperchaotic communication system for secure real-time image transmission," EURASIP Journal on Image and Video Processing, 43.1, 2013

[14] D. Tan and Z. Chen, "On A General Formula of Fourth Order Runge Kutta Method," Journal of Mathematical Sciences & Mathematics Education, 7, 2, 1–10, 2015.

[15] Y. Toopchi, & J. Wang. Chaos control and synchronization of a hyperchaotic Zhou system by integral sliding mode control. Entropy, 16, 12,.6539–6552, 2014.

[16] A. K.A. Hassan. Proposed hyperchaotic system for image encryption. International Journal of Advanced Computer Science and Applications, 7(1),.37–40, 2016.

https://doi.org/10.30526/31.1.1833