Hindawi
Complexity
Volume 2024, Article ID 2005801, 15 pages
https://doi.org/10.1155/2024/2005801

Research Article

Dynamical Analysis of a Quadratic Megastable Chaotic Oscillator and Its Application in Biometric Fingerprint Image Encryption

Rajeskannan Subramanian,[1] Serdar Çiçek ,[2] Akif Akgul ,[3] Girma Adam ,[4] Anitha Karthikeyan,[5] and Karthikeyan Rajagopal [6]

[1] *Computer Science and Engineering, Chennai Institute of Technology, Chennai, Tamilnadu, India*
[2] *Department of Electrical and Electronics Engineering, Faculty of Engineering, Tarsus University, Mersin, Türkiye*
[3] *Department of Computer Engineering, Faculty of Engineering, Hitit University, Çorum, Türkiye*
[4] *Centre for Nonlinear Dynamics, Defence University, Bishoftu, Ethiopia*
[5] *Department of Electronics and Communication Engineering, Vemu Institute of Technology, Chittoor, Andhra Pradesh, India*
[6] *Centre for Nonlinear Systems, Chennai Institute of Technology, Chennai, Tamilnadu, India*

Correspondence should be addressed to Karthikeyan Rajagopal; rkarthiekeyan@gmail.com

Received 21 March 2023; Revised 5 February 2024; Accepted 12 March 2024; Published 26 March 2024

Academic Editor: Giacomo Innocenti

This investigation centers on megastable systems, distinguished by their countable infinite attractors, with a particular emphasis on the Quadratic Megastable Oscillator (QMO). Unlike traditional megastable oscillators reliant on external excitation, our proposed QMO operates autonomously, contributing to its distinctiveness. Through a comprehensive exploration of the QMO, we elucidate various dynamical behaviors, enriching the understanding of its complex system dynamics. In contrast to conventional megastable oscillators, the QMO yields nested types of multiple attractors for diverse initial conditions, elegantly depicted in phase portraits. To gauge the sustainability of chaotic oscillation, we employ influential parameter bifurcation plots, providing a nuanced insight into the system's dynamical evolution. The complexity of the proposed system is further underscored by its intricate basins of attraction, accommodating an infinite number of coexisting attractors. Exploring trajectory dynamics, we observe that certain initial conditions lead trajectories to distant destinations, evading the influence of local attractors. This behavior underscores the uniqueness of the QMO and highlights its potential applications in scenarios requiring nonlocalized attractor behaviors. Taking a practical turn, the QMO is applied to biometric fingerprint image encryption, demonstrating its efficacy in real-world applications. Rigorous statistical analyses and vulnerability assessments confirm the success of the QMO in providing secure encryption within chaotic system-based frameworks. This research contributes not only to the theoretical understanding of megastable systems but also establishes the QMO as a valuable tool in encryption applications, emphasizing its robustness and versatility in complex dynamical scenarios.

1. Introduction

Multistability is a very important phenomenon in dynamical systems [1, 2]. In addition to the standard sensitive dependence on initial conditions that distinguish a chaotic system and prevent long-term prediction, multistable systems have an attractive state that depends on the original conditions. Multistability is not practical when designing commercial products where it is necessary to maintain the desired state in a noisy environment. Furthermore, multistability can be used with appropriate control strategies to switch between coexisting states without compromising system performance [2]. In this regard, many researchers have investigated the property multistability in many literature. New dynamical systems were proposed recently with an infinite number of coexisting attractors, and these are known as megastable systems [3–5]. Multistability can be identified in two forms named extreme multistability and megastability, which deals with infinite number of oscillators. Applications that demand more complex systems such as cryptography and secure communications, chaotic systems with special properties are more suitable. The countable number of infinite attractors which can generate for different initial conditions supports well for infinite number of key generations. Many works of literature recommended megastable oscillators for designing encryption algorithms, but to the best of our knowledge, most of them have an external excitation [6, 7]. It motivates us towards developing a megastable oscillator without external excitation. In order to investigate the dynamics of the proposed system, we adopted stability analysis [8] and bifurcation plots. The significance of the initial condition and its effect on the dynamics can be revealed using a basin of attractors. In this work, we used a fully automated method for identifying attractor basins without approximations of dynamics [9, 10].

In recent years, the use of the Internet in daily and business life, the use of social media, and in addition to this, smart production systems, smart home systems, and Internet of things applications that came with the industry 4.0 revolutions have increased considerably. In all of these uses, there is a continuous flow of data [11, 12]. The advancements in information and communication technology have not only transformed various aspects of our daily lives but have also significantly broadened the scope of telemedicine. This evolution encompasses the delivery of health services, including remote diagnosis, treatment, and even surgical operations conducted from a distance [13]. In addition, physiological data such as fingerprint image, palm, eye iris and retina, face, hand geometry, finger geometry, vein image, and behavioral biometric data such as voice, handwriting, and walking are widely used today to safely recognize user identity [13–15]. Also, biometric identification has become more popular than traditional identification techniques, especially in identity cards, passwords, and personal identification numbers (PIN) applications.

Having an infinite number of attractors in a chaotic system can potentially provide some advantages for key generation applications. However, it is important to note that the actual usefulness of these advantages will depend on the specific requirements and limitations of the application. Here, we highlight a few potential advantages:

(i) Increased security: With a larger number of attractors, it can be more difficult for an attacker to determine which attractor corresponds to the correct key. This can increase the security of the system by making it more difficult to guess or brute-force the correct key.

(ii) Increased flexibility: Having more attractors to choose from can provide more flexibility in selecting the initial conditions for key generation. This can allow for a wider range of potential keys and make it easier to generate keys that meet specific requirements (e.g., length, complexity, etc.).

(iii) Robustness: In some cases, having multiple attractors can provide a certain level of robustness against perturbations or noise in the system. Even if the initial conditions are slightly perturbed, the system may still converge to a valid attractor and generate a valid key.

With the increase in digital data in these mentioned areas, illegal attacks during the transmission of these data have increased [16, 17]. As a result, researchers have worked on encryption methods to increase data security. Traditional encryption methods such as SHA-1, MD5, AES, IDEA, RSA, and DES are not ideal for encrypting biometric images due to large data capacity, computationally intensive, high time consumption, and high correlation between pixels. Instead, chaotic system-based encryption schemes have become more popular due to the good cryptological qualities of chaotic systems, such as their sensitivity to system parameters and initial conditions, nonperiodicity, mixing, and topological transitivity [16–19]. For this purpose, in the literature, there are various encryption studies based on chaotic systems [12, 14, 20, 21], hyperchaotic systems [22–25], and chaotic maps [26–28]. Due to the abovementioned advantages, chaotic systems have been highly preferred and studied in the encryption of physiological biometric images [14–17, 19, 24, 29, 30]. Therefore, biometric fingerprint image encryption is designed using the proposed Quadratic Megastable Oscillator (QMO) in this study.

The impetus behind this research stems from the pressing need for advanced encryption methodologies in safeguarding sensitive information. In an era characterized by the ubiquity of digital data and evolving cyber threats, there is an increasing demand for encryption systems that not only ensure confidentiality but also exhibit resilience against sophisticated attacks. The motivation to explore the Quadratic Megastable Oscillator (QMO) for biometric fingerprint image encryption arises from the unique dynamical properties it exhibits. Leveraging these properties, we aim to develop an encryption system that not only meets stringent security requirements but also demonstrates versatility and robustness in the face of diverse cryptographic challenges.

This research makes significant contributions to both the theoretical understanding of three-dimensional autonomous quadratic megastable oscillators and their practical application in secure communication systems. The comprehensive analysis of attractors, phase portraits, parameter bifurcation plots, and the sustainability of chaotic oscillation provides a nuanced insight into the complex dynamics of the QMO. Specifically, the exploration of attractors and basin of attraction concepts contributes to a deeper understanding of the system's behavior. The extension of the QMO to biometric fingerprint image encryption represents a novel application, demonstrating its efficacy in real-world scenarios. Rigorous statistical analyses, including NIST 800-22 tests, histogram analysis, correlation analysis, entropy analysis, and key sensitivity analysis, collectively establish the robustness and security features of the proposed encryption scheme. This research not only advances the field of dynamical systems but also provides a practical solution to the pressing need for secure encryption methodologies in the realm of biometric data protection.

The paper is organized as follows: In Section 1, the introduction of QMO and its application are detailed. In Section 2, a novel 3D Quadratic Megastable Oscillator (QMO) is presented and its dynamics are investigated with the help of stability analysis, orbit diagram, Lyapunov spectrum, and the basins of attraction. A biometric fingerprint image encryption of cryptographic application is shown in Section 5. Finally, the highlights of the study and conclusion are presented.

2. Quadratic Megastable Oscillator (QMO)

In his book "Elegant Chaos" [31], Sprott has proposed several classes and types of chaotic systems. One such classification is a quadratic oscillator defined generally as

$$\ddot{x} + f(\dot{x}, x) = A\sin(\omega t), \tag{1}$$

where the function $f(\dot{x}, x)$ should contain at least one sinusoidal term or cubic nonlinear term. But such systems are normally forced to exhibit chaos.

Inspired by (1), we propose a simple third-order quadratic oscillator which exhibit chaos without external excitation. Quadratic Megastable Oscillator (QMO) shows megastability without an external excitation whereas megastable oscillators [32] discussed in the most of literature show chaotic oscillations only under external excitation [33–38].

The mathematical model of QMO is

$$\begin{aligned} \dot{x} &= y, \\ \dot{y} &= -b\,\mathrm{sgn}(x) + a\sin(z). \\ \dot{z} &= -x. \end{aligned} \tag{2}$$

We considered the parameter values $a = 0.1$, $b = 0.4$ and performed the numerical simulation for $x = -20$ to $x = +20$ all other states are kept as $y = z = 0$, the 2D phase portrait is presented in Figure 1. We could clearly observe the growing kind of attractors. We used MATLAB ODE solver with a runtime of 500.

In order to find the equilibrium points, the state space equations are equated to zero.

$$\begin{aligned} \dot{x} &= \dot{y} = \dot{z} = 0, \\ y &= x = 0, \\ a\sin(z) &= 0. \\ z &= \sin^{-}(\theta) \Longrightarrow n\pi, \\ &(\text{or})\ \pi + 2n\pi \text{ This can also be written as } n\pi. \end{aligned} \tag{3}$$

The equilibrium points of QMO system can be written as (0, 0, $n\pi$), where n is an arbitrary integer.

3. Stability Analysis of QMO System

The stability analysis [8] can be found using the Jacobian matrix and eigenvalues as given in equations (4) and (6).

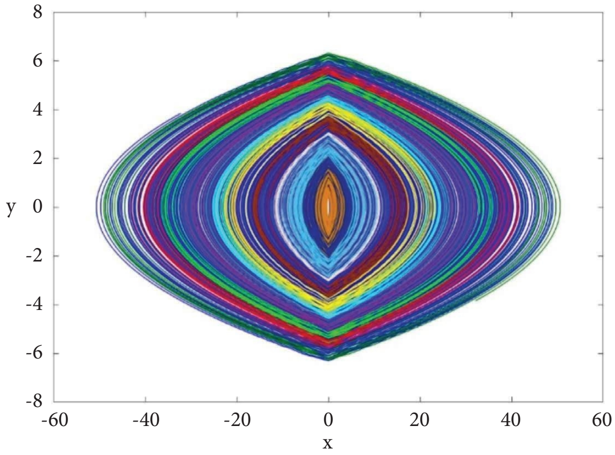


FIGURE 1: 2D Phase portrait of QMO system for 21 initial conditions (from $x = -20$ to $x = +20$ with steps equal to 2) and the initial conditions for the other states is kept at 0.

The Jacobian matrix of the QMO system at equilibrium drives to infinity because of the term dirac(0). Hence, we replaced the term sign(x) as tanh(Ax) and for $A = 250$ it have been shown that the hyperbolic tan function matches the signum function. The modified Jacobian matrix is

$$\begin{bmatrix} 0 & 1 & 0 \\ b\left(A\tanh(\mathrm{Ax})^2 - A\right) & 0 & a\cos(z) \\ -1 & 0 & 0 \end{bmatrix}. \tag{4}$$

The characteristic polynomial can be derived as

$$\lambda^3 + \mathrm{Ab}\lambda + a\cos(n \times \pi), \tag{5}$$

where the eigenvalues for different cases is presented in Table 1.

We plotted the real parts of the eigenvalues ($\lambda_1, \lambda_2\ \&\ \lambda_3$) for $n = 1$ to 10 in Figure 2. For even values of n produces one negative and two complex conjugate eigenvalues which show the equilibrium point should be an attracting spiral saddle. For odd values of n produce one positive and two complex conjugate (with negative real part) eigenvalue, hence the stability can be classified as an extruding spiral saddle.

4. Dynamical Behavior of QMO for Parameter Variation

A bifurcation plot is a graphical representation that showcases the behavior of a dynamic system as a key parameter is varied. It provides valuable insights into the system's transitions, stability, and the emergence of complex behaviors such as chaos. In the case of chaotic systems, bifurcation plots are particularly useful as they unveil the intricate relationship between system parameters and the resulting dynamics. A bifurcation plot typically consists of a parameter axis and a state variable axis. As the parameter value is gradually changed, the corresponding values of the state variable are plotted on the graph. The resulting plot

Table 1: Stability of the QMO system for different cases.

Cases	Eigen values	Stability
Case 1: for n is even	$2n\pi + \pi \Longrightarrow$ at $a = 0.1$ $\lambda_1 = -0.464159$ $\lambda_{2,3} = 0.232099 \pm 0.40197$	Attracting spiral saddle
Case 2: for n is odd	$2n\pi \Longrightarrow$ at $a = 0.1$ $\lambda_1 = 0.464159$ $\lambda_{2,3} = -0.232079 \pm 0.40197$	Repelling spiral saddle

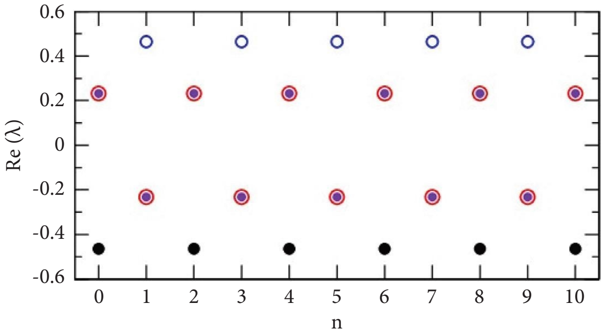


Figure 2: Eigenvalues (real part) of QMO system for "n" variation from 1 to 10. Considering the parameter values $a = 0.1$, $b = 0.4$.

reveals the system's behavior as the parameter sweeps through different ranges, indicating points of stability, periodicity, or chaotic behavior. Bifurcation plots often exhibit distinctive patterns such as period-doubling, intermittency, or strange attractors, which provide crucial insights into the system's behavior.

The Lyapunov exponent is a measure used to quantify the sensitivity to initial conditions in chaotic systems. It characterizes the exponential rate of divergence or convergence of nearby trajectories in phase space. A positive Lyapunov exponent indicates sensitive dependence on initial conditions and chaotic behavior, while a negative exponent suggests convergence towards stability or periodicity. The calculation of Lyapunov exponents involves analyzing the linearized dynamics of a system and determining the exponential growth or decay of perturbations. A positive Lyapunov exponent indicates chaotic behavior, while a negative exponent implies stability. Moreover, the magnitude of the Lyapunov exponent provides information about the system's sensitivity to initial conditions. A higher magnitude indicates stronger sensitivity and a more chaotic system.

The study of parameter variation in megastable chaotic systems holds significant importance in understanding their behavior and dynamics. Megastable chaotic systems are characterized by exhibiting both stability and chaotic behavior under different parameter values. Exploring the effect of parameter variation helps elucidate the range of behaviors these systems can exhibit and provides insights into their underlying mechanisms.

By systematically varying the system's parameters and observing the resulting dynamics, researchers can identify critical points at which the system undergoes bifurcations and transitions between stability and chaos. Bifurcation plots offer a visual representation of these transitions, highlighting the parameter values at which the system enters chaotic regimes or returns to stability. In addition, studying the Lyapunov exponents of a megastable chaotic system under different parameter values helps quantify its sensitivity to initial conditions. The Lyapunov exponents provide a measure of the system's predictability and offer insights into the overall stability or chaotic nature of system. A comprehensive analysis of Lyapunov exponents for various parameter values allows researchers to identify regions of parameter space where the system exhibits stable behavior or transitions into chaotic regimes.

The influence of parameter variation is a crucial factor in understanding the dynamics of chaotic systems. In Section 3 of the study, it becomes evident that the dynamics of the QMO system are significantly affected by parameter a changes. To gain insights into the system's behavior with varying parameters, we explored a specific range of parameters. We focused on plotting the local maxima of the state variable y against the parameter values $0 \leq a \leq 0.5$. The resulting orbit diagram, depicted in Figure 3(a), vividly illustrates the chaotic nature of the QMO system within the considered parameter range.

Additionally, we employed Wolf's algorithm [39] to calculate the Lyapunov Exponents for system. A finite time interval of 25000 s was chosen for this analysis. The Lyapunov Exponents were then plotted in Figure 3(b). It is worth noting that the summation of Lyapunov exponents for any particular value of parameter becomes zero, which provides strong evidence for the conservative nature of the system. This observation further reinforces the understanding of the QMO system's behavior and its sensitivity to parameter variations.

The study emphasizes the vital role that parameter variation plays in the dynamics of chaotic systems, as exemplified by the QMO system. By exploring a specific parameter range and examining the local maxima of the state variable y, the researchers demonstrated the chaotic nature of the system. Furthermore, the calculation of Lyapunov Exponents using Wolf's algorithm validated the conservative behavior of the system, as indicated by the summation of the exponents being consistently zero for different parameter values. These findings contribute to a deeper understanding of the QMO system's dynamics and provide valuable insights for further research in the field of chaotic systems.

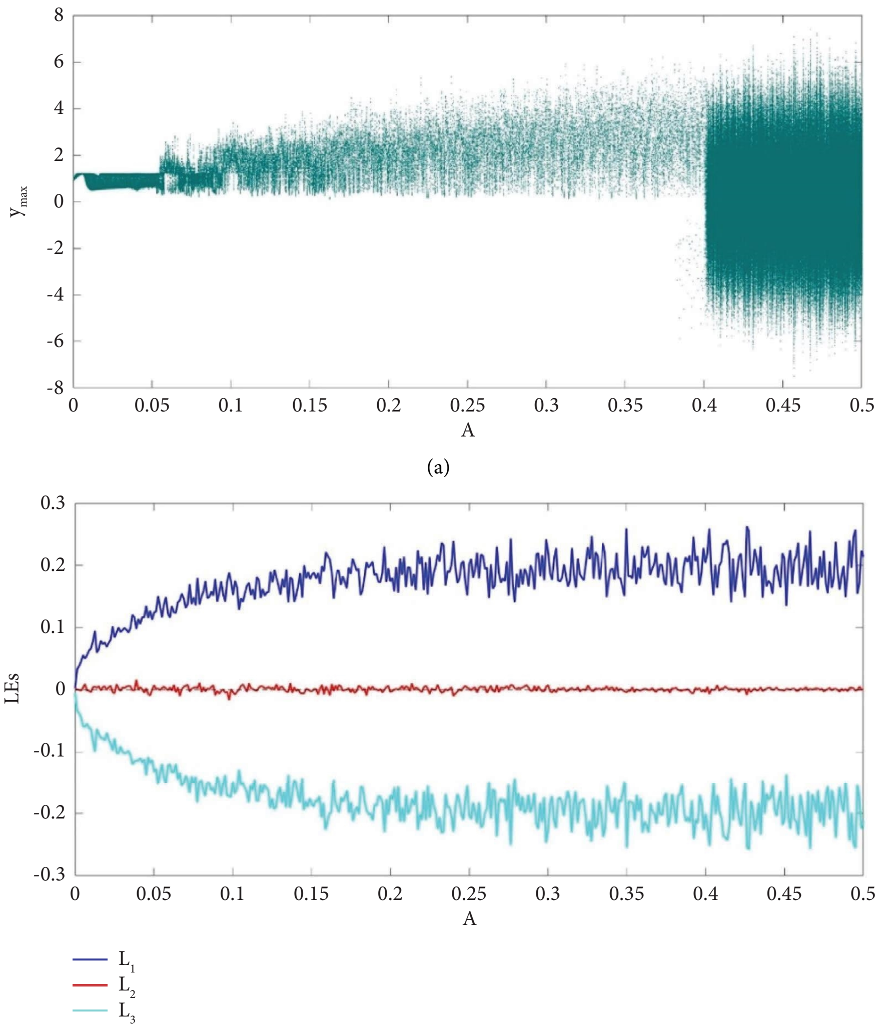


Figure 3: (a) Bifurcation of the QMO system with A; (b) corresponding Lyapunov exponents (LEs).

4.1. Basin of Attraction. The concept of basins of attraction is a central part of the body of knowledge about multistable dynamical systems. Since most of the nonlinear systems are impossible to study with analytical methods, numerical simulations are the only choice for inquiry into their behavior. In order to construct the basins [9], the trajectory of each chosen initial condition is compared to the trajectory of a collection of known attractors. In addition to knowing the long-term behavior of each initial condition, estimating the basins has many other benefits. As an example, during chaotic transients, they can reveal chaotic dynamics before settling into a nonchaotic attractor. We used the algorithm [10] for identifying the basin of attraction plot for the limit cycle attractors shown in Figure 1. Figure 4 shows the basin of attraction of the proposed QMO system. For the given parameter value the system has 5 attractors in the x-y region.

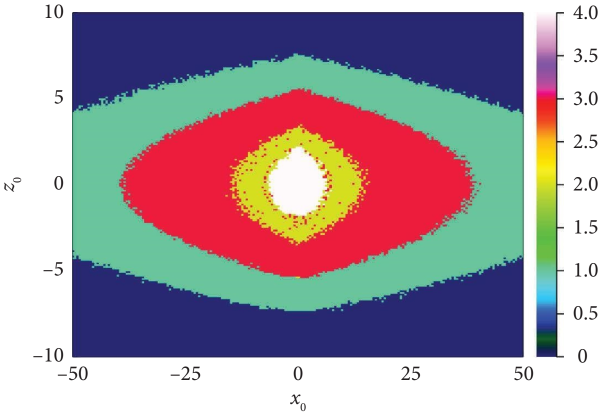


Figure 4: Basin of attraction plot to show the presence of different attractors.

5. Application of Fingerprint Image Encryption Using the QMO System

In this section, the fingerprint image encryption application is designed and analyzed using the QMO system. The encryption and decryption processes of the designed fingerprint image encryption system are given in Figure 5 as a diagram. Three initial values (x_0, y_0, z_0) and two parameters $(a,\ b)$ values of the QMO system are used as the key in the encryption design. In each encryption process, the initial conditions and parameter values are taken differently within the specified limits. For each image encryption processing, key information is obtained from a randomly determined list of initial conditions and parameter values in the specified order. A new key from this list is used in each encryption operation. Thus, even if the same image is encrypted, the encrypted image is different. In the encryption process, the x, y, and z state variables of the QMO system are first calculated with the key information. Next, 32 bit single floating-point IEEE-754 binary numbers are created from the retrieved state variables. From these 32 bit binary values, the 6 bit LSB of the x state variable, the 2 bit LSB of the y state variable, and the 6 bit LSB of the z state variable are taken. The LSB bits from the x and y state variables are combined to obtain an 8 bit value in the combining part. Likewise, the LSB bits from the y and z state variables are combined to obtain an 8 bit value. These two combined 8 bit values are sent sequentially to the XOR part in each period by the "Multiplexer." The Up-Counter unit is used as the input selector of the Multiplexer unit. The Multiplexer sends the 8 bit values (x-y and y-z) obtained from the x, y, and z state variables to the output, according to the 0 and 1 information sequentially from the up-counter unit that counts up to one. Thus, the complexity is increased by sending the combination value obtained from the chaotic system state variables. In the XOR part, the 8 bit data from the Multiplexer part and the 8 bit data coming from the fingerprint image are processed by XOR.

In the decryption process, 8 bit combined data is obtained from the QMO system in the same way as in the encryption process. The incoming encrypted fingerprint image data and the 8 bit combined data are processed by XOR operation to decrypt the fingerprint image. Thus, the decrypted fingerprint image is obtained. Encryption and decryption processes were performed in MATLAB- Simulink program with the block diagrams given in Figures 6 and 7, respectively. The step size in the designed encryption and decryption process is $1e-8$ seconds. The processing bit rate of the system is 800 Mbps.

For the analysis of the designed encryption system, a real grayscale fingerprint image with a height value of 390 pixels, a width value of 355 pixels, and a bit depth value of 8, taken from the fingerprint database given in reference [40], was used. The gray fingerprint image used in the design may vary in size. The design can be used exactly for fingerprint images of different sizes. Color fingerprint images can be implemented using the encryption design provided separately for red, green, and blue pixel values.

The encrypted and decrypted fingerprint images obtained from the encryption and decryption processes (in Figure 5) are given in Figure 8. As can be seen in Figure 8, the design (Figures 6 and 7) can successfully perform encryption and decryption operations.

5.1. Security Analysis. The encryption process should be able to perform well against various statistical and security attacks. To determine the performance of encryption, it is necessary to examine it with various security tests. In this section, randomness performance, statistical and attack analyses which are histogram, correlation, correlation maps, entropy, key sensitivity, key space, and known/chosen were applied for the performance analysis of encryption.

5.1.1. The Randomness Performance of the QMO System. Since the chaotic QMO system is used in the encryption design, the randomness level of the outputs obtained from this system must be suitable for encryption. The widely accepted NIST 800-22 test is used for randomness performance analysis. The NIST 800-22 test consists of 15 separate tests. For each test result to be successful, the p value indicating randomness must be greater than the α value chosen between 0.001 and 0.01 [41]. The NIST 800-22 test performance results of the x, y, and z state variables of the chaotic QMO system are given in Table 2. The p value was taken as 0.01 in the tests. As can be seen from Table 2, the values obtained from the outputs of the x, y, and z state variables of the QMO system were successful in the randomness tests.

5.1.2. Histogram Analysis. The distribution of pixel values in the encrypted image can be examined by using histogram analysis. The ideal histogram distribution should be uniform. In this way, the distribution of encrypted information is almost the same, indicating that the original information is difficult to predict with statistical analysis [28, 42]. Figure 9 shows the histogram diagrams of the original fingerprint and the encrypted image. As may be seen, the histogram diagram of the encrypted fingerprint image is uniform and therefore difficult to predict by statistical analysis.

5.1.3. Correlation Analysis. The correlation coefficient value between two neighboring pixels in the original image and the encrypted image is another crucial factor in determining encryption performance. The correlation between the vertical, horizontal and diagonal pixel values of the image should be near to zero to avoid statistical attacks. A correlation value near 0 denotes a negligibly weak correlation, whereas a correlation value near 1 denotes a significant relationship [28, 43]. The correlation coefficient is given in equation (6) [18, 43]:

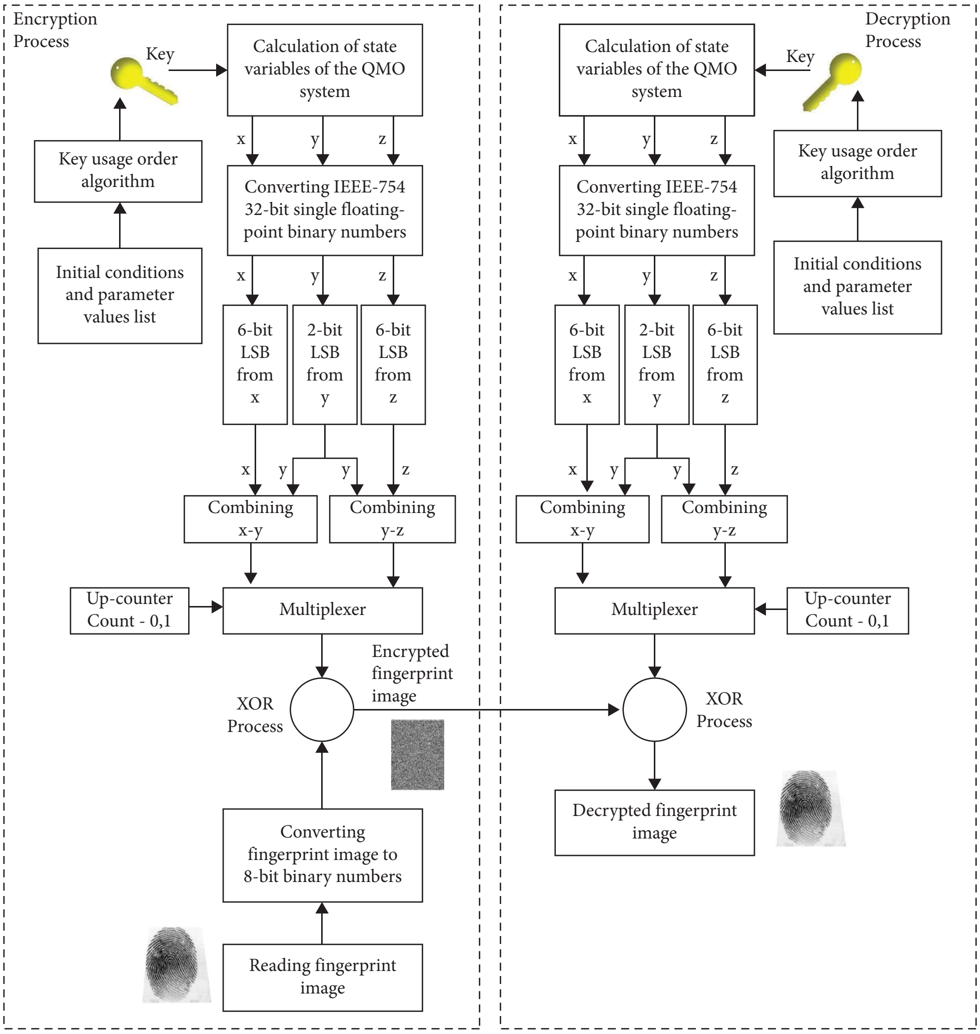

Encryption Process
Key
Calculation of state variables of the QMO system
x
y
z
Key usage order algorithm
Initial conditions and parameter values list
Converting IEEE-754 32-bit single floating-point binary numbers
6-bit LSB from x
2-bit LSB from y
6-bit LSB from z
Combining x-y
Combining y-z
Up-counter Count - 0,1
Multiplexer
Encrypted fingerprint image
XOR Process
Converting fingerprint image to 8-bit binary numbers
Reading fingerprint image
Decryption Process
Decrypted fingerprint image

Figure 5: The encryption and decryption processes diagram.

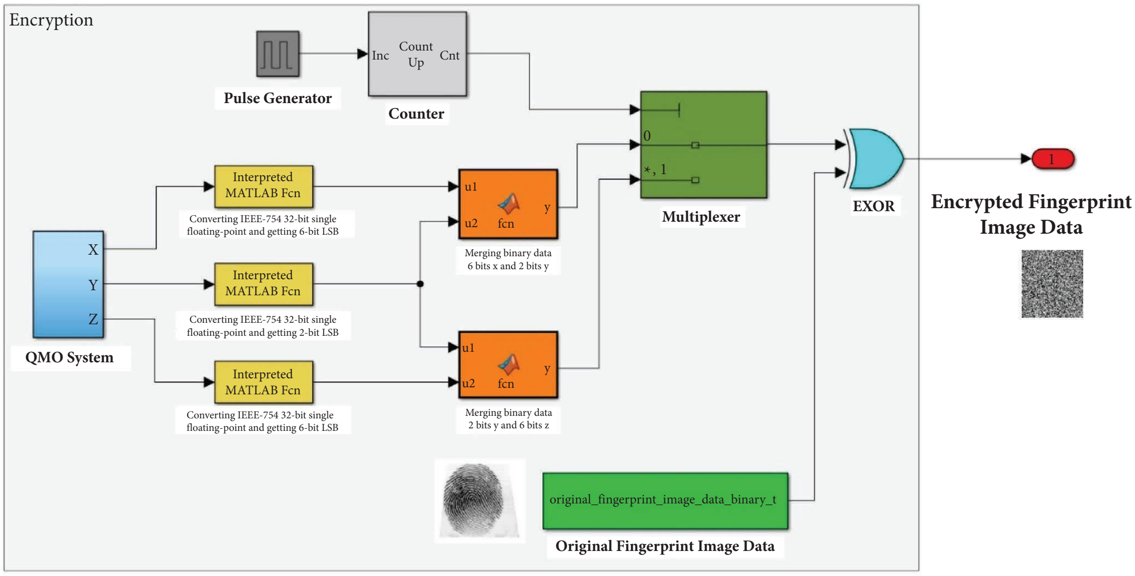

Encryption
Pulse Generator
Inc
Count Up
Cnt
Counter
Multiplexer
0
*, 1
EXOR
1
Encrypted Fingerprint Image Data
Interpreted MATLAB Fcn
Converting IEEE-754 32-bit single floating-point and getting 6-bit LSB
Converting IEEE-754 32-bit single floating-point and getting 2-bit LSB
Converting IEEE-754 32-bit single floating-point and getting 6-bit LSB
u1
u2
fcn
y
Merging binary data 6 bits x and 2 bits y
Merging binary data 2 bits y and 6 bits z
X
Y
Z
QMO System
original_fingerprint_image_data_binary_t
Original Fingerprint Image Data

Figure 6: Simulink diagram of the encryption process.

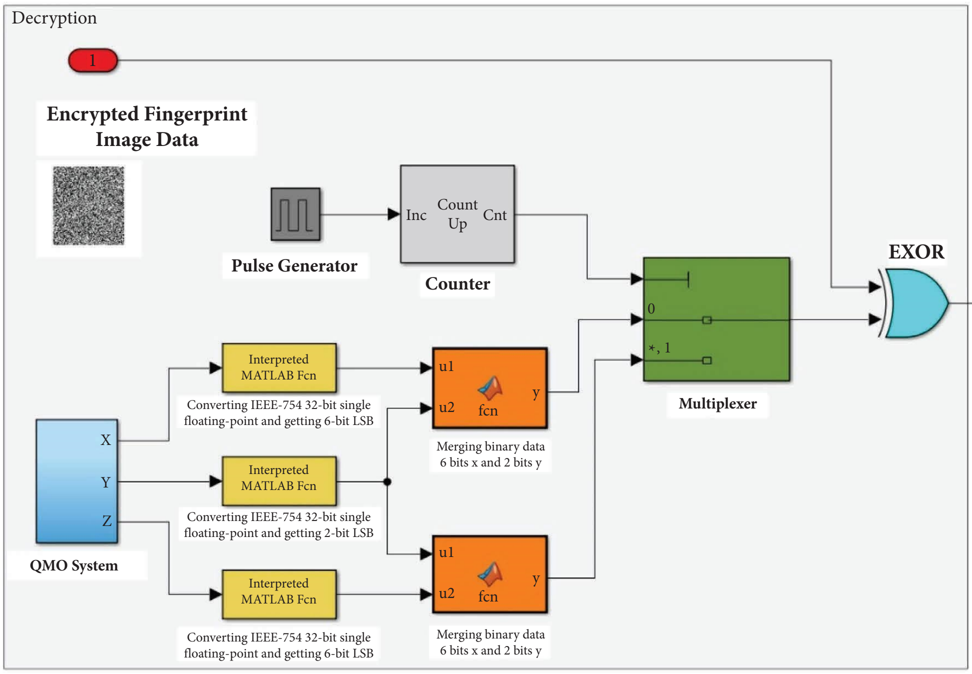

Decryption
1
Encrypted Fingerprint Image Data
Pulse Generator
Inc
Count Up
Cnt
Counter
Interpreted MATLAB Fcn
Converting IEEE-754 32-bit single floating-point and getting 6-bit LSB
Interpreted MATLAB Fcn
Converting IEEE-754 32-bit single floating-point and getting 2-bit LSB
Interpreted MATLAB Fcn
Converting IEEE-754 32-bit single floating-point and getting 6-bit LSB
X
Y
Z
QMO System
u1
u2
fcn
y
Merging binary data 6 bits x and 2 bits y
u1
u2
fcn
y
Merging binary data 6 bits x and 2 bits y
0
*, 1
Multiplexer
EXOR
1
Decrypted Fingerprint Image Data

Figure 7: Simulink diagram of the decryption process.

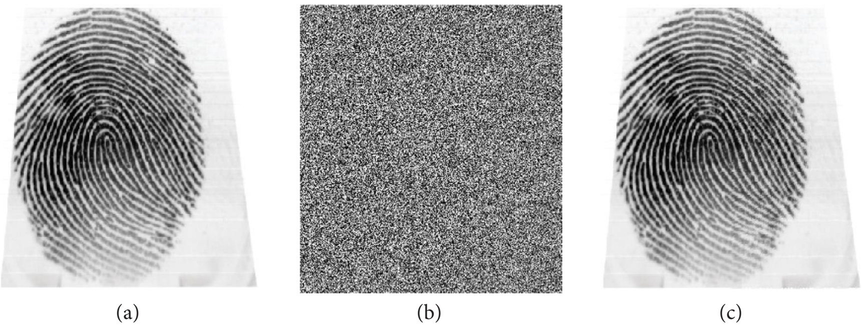


Figure 8: The encryption and decryption processes (a) original fingerprint image and (b) encrypted fingerprint image (c) decrypted fingerprint image.

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}}, \tag{6}$$

$$\begin{aligned}\operatorname{cov}(x, y) &= E([x - E(x)][y - E(y)]) \\ &= \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)],\end{aligned} \tag{7}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2, \tag{9}$$

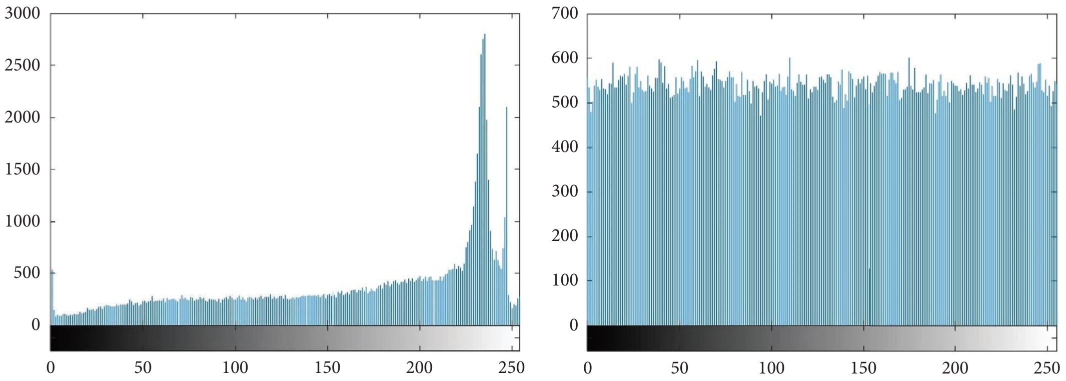
Analyzing the correlation distribution provides insights into the degree of correlation between the original and encrypted images. A deviation from the expected correlation values for a secure encryption scheme indicates the effectiveness of the encryption in breaking the correlation patterns present in the original image, contributing to enhanced security.

Here, x and y are adjacent pixels from the encrypted or original images that will be examined. Cov (x, y) is the covariance of x and y, equation (7), D (x) and D (y) is the variance of x, equation (9) and y. E (x) and E (y) represent the average of x pixels, equation (8), and y pixels. N in the formulas refers to the total number of pixels in the image [18, 43]. The correlation coefficient values of the actual image and encrypted image used in the study are given in Table 3. As shown in Table 3, the correlation coefficient of the vertical, horizontal and diagonal pixel values of the actual image is near to 1, even though the fingerprint image's correlation coefficients are almost zero. Also, Figure 10 presents the correlation distribution maps of the actual and encrypted image in horizontal, vertical and diagonal forms. According to the correlation distribution maps, while the correlation distribution in the actual image is concentrated

Table 2: The NIST 800-22 test performance results of the x, y, and z state variables of the chaotic QMO system.

Test type	p value x	p value y	p value z	Result
Frequency (monobit) test	0.9378	0.7025	0.2627	Success
Frequency test within a block	0.2204	0.9218	0.1046	Success
Runs test	0.9076	0.7489	0.5165	Success
Test for the longest run of ones in a block	0.1097	0.8477	0.1085	Success
Binary matrix rank test	0.1308	0.4985	0.6488	Success
Discrete Fourier transform test	0.9780	0.0283	0.0651	Success
Nonoverlapping template matching test	0.9294	0.8947	0.4218	Success
Overlapping template matching test	0.6813	0.2080	0.1662	Success
Maurer's universal statistical test	0.2050	0.8413	0.3269	Success
Linear complexity test	0.0758	0.9445	0.9277	Success
Serial test	0.9903	0.8832	0.4318	Success
	0.9077	0.7490	0.5144	Success
Approximate entropy test	0.2163	0.2737	0.4486	Success
Cumulative sums test	0.8883	0.7848		Success
Random excursions test			*	
($x = -4$)	0.0707	0.3537		Success
($x = -3$)	0.9046	0.3775		Success
($x = -2$)	0.7340	0.3514		Success
($x = -1$)	0.7972	0.2836		Success
($x = 1$)	0.7192	0.4131		Success
($x = 2$)	0.2173	0.7693		Success
($x = 3$)	0.1456	0.7260		Success
($x = 4$)	0.3911	0.0434		Success
Random excursions variant test			*	
($x = -9$)	0.3383	0.9068		Success
($x = -8$)	0.2474	0.9917		Success
($x = -7$)	0.1845	0.7380		Success
($x = -6$)	0.2828	0.8225		Success
($x = -5$)	0.4540	0.8617		Success
($x = -4$)	0.9120	0.9213		Success
($x = -3$)	0.4611	0.7462		Success
($x = -2$)	0.2658	0.2229		Success
($x = -1$)	0.6513	0.0423		Success
($x = 1$)	0.1588	0.1845		Success
($x = 2$)	0.1248	0.3968		Success
($x = 3$)	0.2663	0.9641		Success
($x = 4$)	0.2626	0.6375		Success
($x = 5$)	0.0749	0.9040		Success
($x = 6$)	0.0451	0.9758		Success
($x = 7$)	0.0768	0.7254		Success
($x = 8$)	0.0748	0.6256		Success
($x = 9$)	0.0367	0.6714		Success

*Test not applicable. There are an insufficient number of cycles.



(a)

(b)

Figure 9: Histogram diagrams (a) original fingerprint image and (b) encrypted fingerprint image.

Table 3: The correlation coefficient and entropy values of the actual image and the encrypted image.

Image	Horizontal correlation	Vertical correlation	Diagonal correlation	Entropy
Original image	0.9558	0.9684	0.9432	6.1343
Encrypted image	−0.0025	−0.0032	−0.0025	7.9987

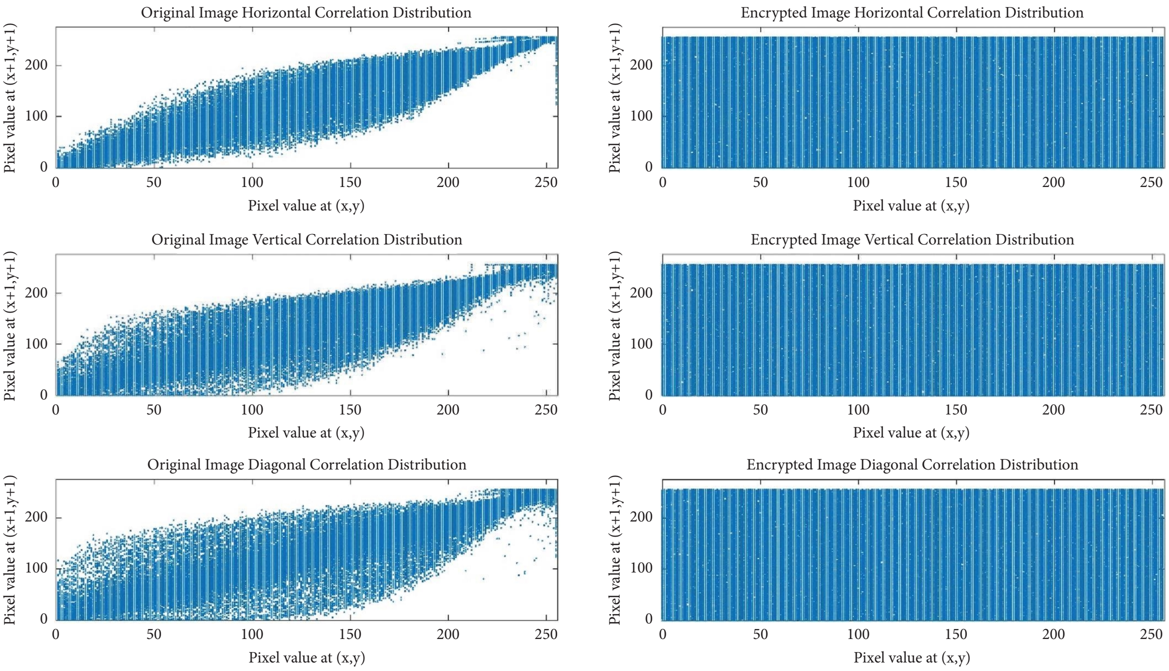


Figure 10: Correlation distributions for original and encrypted images.

in a certain region, it is homogeneous in the encrypted image. This outcome demonstrates that statistical assaults are unable to decrypt the image.

5.1.4. Entropy Analysis. The entropy value of a data stack gives information about the distribution and randomness of the data. The entropy of the actual and encrypted fingerprint image used in the study shows the distribution of each gray value. Entropy is generally calculated with equation (10). In equation (10), N represents the number of symbols, x_i is the pixel value and $p(x_i)$ represents the probability that x_i will appear in the data stack. The N value for the 8 bit depth of the grayscale fingerprint image used in the study is 8 [16, 20, 26, 27, 30].

$$H(x) = -\sum_{i=0}^{2^N} -1p(x_i)\log_2 p(x_i). \tag{10}$$

If the entropy value is near 8 indicates that the ideal information entropy is reached [23, 42, 43]. A high entropy number denotes a uniform distribution of the image's gray values. This makes it difficult for attackers to obtain the actual image through information analysis [28]. The entropy results of the original fingerprint image and the encrypted fingerprint image are given in Table 3. While the entropy value of the original image is 6.1343, the entropy value of the encrypted image is 7.9987, which is very near to 8. This indicates that the encryption design has good performance against statistical attacks.

5.1.5. Key Sensitivity Analysis. The effectiveness of the key sensitivity analysis of the encryption design can be assessed using UACI and NPCR values. NPCR describes the ratio of the encrypted image's changed pixel values to the original image's altered pixel values. The intensity of the difference between a specific pixel's value in the original image and the encrypted image's pixel values is specified by UACI. NPCR is calculated as in equations (11) and (12) and UACI is calculated as in equation (13). Where H is the pixel number of the image's height, W is the pixel number of the image's width, i and j represent the pixel position, and C_1 and C_2 represent the two encrypted images. NPCR and UACI have optimum values of 99 and 33 percent, respectively [18, 23, 28, 42, 43].

$$\mathrm{NPCR} = \frac{1}{H \times W} \sum_{i,j} D(i,j) \times 100\%, \tag{11}$$

$$D(i,j) = \begin{cases} 1, & \text{if } C_1(i,j) \neq C_2(i,j), \\ 0, & \text{if } C_1(i,j) = C_2(i,j), \end{cases} \tag{12}$$

$$\mathrm{UACI}=\frac{1}{H\times W}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times 100\%. \qquad (13)$$

For the key sensitivity analysis, the initial conditions and parameter values of the QMO system were increased by 10^{-6}. For instance, instead of using 10 as the initial value for the x state variable, 10.000001 is used. In this way, UACI and NPCR values of the normally encrypted fingerprint image and the encrypted fingerprint image with parameter values increased by 10^{-6} were calculated. According to the calculation result [44] as shown in Table 4 the NPCR value was 99.426% and the UACI value was 33.398%. Therefore, the proposed encryption design has high key sensitivity.

5.1.6. Key Space Analysis. One parameter that determines the security of encryption is the key space size. The larger the key space, the better the encryption performance and the greater the resistance to key analysis. The key space size should be bigger than 2^{100} [23, 43] or 2^{128} [28, 42] for good security. The system used in this study has three initial values (x_0, y_0, z_0) and two parameters (a, b) as key. Assuming that the key precision in the design is 10^{-15}, the overall key size is 10^{75}. Consequently, since the value of 10^{75} is much greater than the value of 2^{128}, the key space is sufficient to resist the extensive attack.

5.1.7. Known/Chosen Image Analysis. The encryption design should resist against some known/selected image attacks. These attacks are used to decrypt the encryption mask [23, 43]. Three initial values (x_0, y_0, z_0) and two parameters (a, b) values of the QMO system are used as the key in the encryption design. The result of these values is mixed through various processes and used in the encryption process. As stated in the analysis of the QMO system, the initial condition of the state variable x, in particular, can vary in a wide range between −20 and 20. As stated in the key sensitivity analysis section, it is seen that even a very small change in the initial condition creates a sufficient difference in encryption. Thus, with each change in the initial conditions and the system's parameter values, the encryption key also changes.

In this way, the initial conditions of the system and the values of the system parameters constitute the key to the encryption system. This key changes with each new encryption. The receiving system also knows the keys list and the order of use algorithm within the specified limits. In practical uses, these key sequences are constantly updated. For the attacker to succeed, the attacker must know the list of these keys updated periodically and the usage order algorithm. Without this information, it cannot be decrypted by repeatedly sending the same image or one image with only minor changes.

In the known/selected image analysis (Figure 11), firstly, the complete white image (Figure 11(a)) was encrypted (Figure 11(b)) in the designed encryption system. Then, the image with only one black pixel and all the remaining pixels white (Figure 11(c)) is encrypted (Figure 11(d)). The NPCR and UACI values were analyzed for the difference between the encrypted versions of the two images, and the results are given in Table 4. Since the NPCR value is 99.609% and the UACI value is 33.464%, the designed encryption system is resistant to known/selected image attacks.

Table 4: Key sensitivity analysis calculation results for NPCR and UACI.

Test	Key sensitivity analysis result (%)	Known/chosen image analysis result (%)
NPCR	99.426	99.609
UACI	33.398	33.464

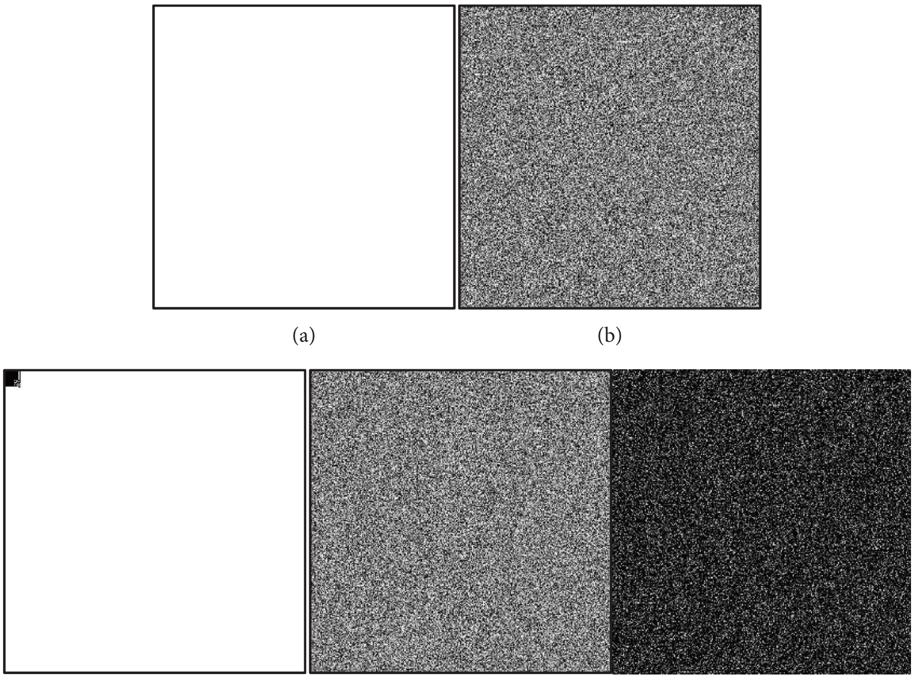
6. Discussion

The findings presented in this study contribute significantly to the understanding of countable infinite attractors in megastable systems, particularly in the context of the Quadratic Megastable Oscillator (QMO). The observed dynamical behaviors of the QMO, such as the generation of nested types of multiple attractors for various initial conditions, enrich our comprehension of complex system dynamics. This intricate behavior is elegantly portrayed through phase portraits, providing a visual representation of the system's evolving states.

The sustainability of chaotic oscillation in the QMO is thoroughly examined using influential parameter bifurcation plots, shedding light on the nuanced interplay of system parameters in shaping its dynamics. The system's complexity is further underscored by the existence of intricate basins of attraction, accommodating an infinite array of coexisting attractors. This feature introduces a level of richness and versatility in the dynamics of the QMO, suggesting potential applications in scenarios requiring diverse attractor landscapes.

A notable observation is the nonlocalized trajectory behavior under specific initial conditions, where trajectories lead to distant destinations, evading the influence of local attractors. This phenomenon adds a layer of unpredictability to the system's behavior and highlights the unique characteristics of the QMO compared to conventional megastable oscillators. The practical application of the QMO in biometric fingerprint image encryption showcases its real-world efficacy. The statistical and attack analyses conducted on the encryption design affirm the QMO's success in providing secure encryption within chaotic system-based frameworks. This practical validation further emphasizes the relevance and applicability of the QMO in encryption applications.

NPCR, UACI, correlation coefficient, and entropy values of the proposed method are compared with previous studies in Table 5. The proposed system is similar to [30, 46] and gave better results than [48] for NPCR and UACI values. According to the average correlation coefficient values, the proposed system is slightly behind [45, 46], but gives better results than [48]. According to the entropy value, the proposed system achieved the best results in [30, 46, 48–50]. In totality, the quadratic megastable system-based


(a) (b)

(c) (d) (e)

Figure 11: Known/chosen image analysis result (a) completely white image and (b) its encrypted image (c) completely white image with only one black pixel and (d) its encrypted image (e) difference image between (b and d).

Table 5: The comparison of the proposed encryption design with similar research.

Encryption designs	NPCR	UACI	Correlation coefficients	Entropy
Yoosefian Dezfuli Nezhad et al. [30]	99.60%	33.46%	Horizontal: — Vertical: — Diagonal: —	7.9882
Su et al. [45]	—	—	0.0019 (average)	—
Li [46]	99.61% (average)	33.44% (average)	Horizontal: −0.0023 Vertical: −0.0044 Diagonal: −0.0007	7.5310 (average)
Su et al. [47]	—	—	Horizontal: 0.0020 Vertical: 0.0091 Diagonal: 0.0038	—
Umoh and Iloanusi [48]	99.59% (average)	99.41% (average)	Horizontal: — Vertical: — Diagonal: —	7.5945 (average)
Proposed encryption design	99.609%	33.464%	Horizontal: −0.0025 Vertical: −0.0032 Diagonal: −0.0025	7.9987

encryption emerges as a robust and effective method for securing fingerprint images.

While the study on the Quadratic Megastable Oscillator (QMO) and its application in biometric fingerprint image encryption offers valuable insights, it is essential to acknowledge certain limitations that could impact the generalization and applicability of the findings:

(1) Theoretical Assumptions: The study relies on certain theoretical assumptions related to the behavior of the QMO, and these assumptions may not perfectly align with real-world conditions. Practical implementations could be affected by factors not considered in the theoretical model.

(2) Sensitivity to Initial Conditions: Chaotic systems, such as the QMO, are known to be highly sensitive to initial conditions. Small variations in the initial conditions can lead to significantly different outcomes. This sensitivity might pose challenges in real-world applications where precise control over initial conditions may be difficult.

(3) Computational Complexity: The comprehensive analysis involving attractors, phase portraits, and

parameter bifurcation plots necessitates computational resources. The computational complexity of the proposed encryption scheme might be a limitation in scenarios with resource-constrained environments.

(4) Robustness under Varying Image Characteristics: The effectiveness of the encryption scheme is demonstrated through various analyses, but its robustness may vary depending on the characteristics of different fingerprint images. It is crucial to assess performance across a diverse range of biometric data.

7. Conclusion

In conclusion, this study offers a comprehensive exploration of the behavior of three-dimensional autonomous quadratic megastable oscillators, shedding light on their characteristics and dynamics in the absence of external stimulation. The analysis encompasses a thorough investigation of attractors, phase portraits, parameter bifurcation plots, and the sustainability of chaotic oscillation.

A key focus of this analysis is the examination of the oscillators' attractors, distinctive patterns that emerge over time. Our findings suggest that initializing the oscillators with different initial conditions leads to the generation of multiple attractors. Visual representation through phase portraits facilitates a clearer understanding of the oscillators' trajectories in their three-dimensional phase space. Additionally, parameter bifurcation plots are employed to visualize the impact of specific parameter changes on the system's behavior, assessing the sustainability of chaotic oscillations under varied parameter values.

Stability analysis and the concept of basins of attraction are crucial aspects discussed in this study. Stability analysis evaluates the system's response to perturbations and its convergence to specific states over time, while the basin of attraction identifies regions in phase space where specific attractors are achieved. These analyses collectively contribute to a comprehensive understanding of the system's overall behavior.

Furthermore, the study extends the application of the quadratic megastable oscillator system to biometric fingerprint image encryption. Rigorous parameter analyses, including NIST 800-22 tests, highlight the robust security features of the quadratic megastable system. Histogram analysis reveals a uniform distribution of encrypted pixel values, resistant to statistical scrutiny. Correlation analysis reinforces security, indicating a substantial deviation from the original image's correlation coefficients. Correlation distribution maps illustrate the encrypted image's resilience against region-based attacks. Entropy analysis underscores effective protection against statistical assaults, supported by entropy values. Key sensitivity analysis emphasizes the encryption's strength, evidenced by high NPCR and UACI values, along with a substantial key space size surpassing established security thresholds, ensuring resistance to extensive attacks. These results collectively affirm the quadratic megastable system's effectiveness in biometric image encryption, showcasing its potential in secure communication systems.

Data Availability

The data used to support the findings of this paper are included within the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

It is with great gratitude that we acknowledge that funding for this project was provided by the Center for Nonlinear Systems at the Chennai Institute of Technology (CIT), India, under Grant number CIT/CNS/2022/RP-016.

References

[1] A. Chudzik, P. Perlikowski, A. Stefanski, and T. Kapitaniak, "Multistability and rare attractors in van der Pol- Duffing oscillator," *International Journal of Bifurcation and Chaos*, vol. 21, no. 07, pp. 1907–1912, 2011.

[2] A. N. Pisarchik and U. Feudel, "Control of multistability," *Physics Reports*, vol. 540, no. 4, pp. 167–218, 2014.

[3] S. Jafari, K. Rajagopal, T. Hayat, A. Alsaedi, and V.-T. Pham, "Simplest megastable chaotic oscillator," *International Journal of Bifurcation and Chaos*, vol. 29, no. 13, Article ID 1950187, 2019.

[4] Z. Wei, V.-T. Pham, A. J. M. Khalaf, J. Kengne, and S. Jafari, "A modified multistable chaotic oscillator," *International Journal of Bifurcation and Chaos*, vol. 28, no. 07, Article ID 1850085, 2018.

[5] B. Chen, K. Rajagopal, I. I. Hamarash, A. Karthikeyan, and I. Hussain, "Simple megastable oscillators with different types of attractors; tori, chaotic and hyperchaotic ones," *European Physical Journal: Special Topics*, vol. 229, no. 6-7, pp. 1155–1161, 2020.

[6] K. Zhang, M. D. Vijayakumar, S. S. Jamal et al., "A novel megastable oscillator with a strange structure of coexisting attractors: design, analysis, and FPGA implementation," *Complexity*, vol. 2021, Article ID 2594965, 11 pages, 2021.

[7] D. Veeman, H. Natiq, N. M. G. Al-Saidi, K. Rajagopal, S. Jafari, and I. Hussain, "A new megastable chaotic oscillator with blinking oscillation terms," *Complexity*, vol. 2021, Article ID 5518633, 12 pages, 2021.

[8] A. B. Akgul, O. F. Boyraz, K. Rajagopal, E. Guleryuz, M. Z. Yildiz, and M. Kutlu, "An unforced megastable chaotic oscillator and its application on protecting electrophysiological signals," *ZeitschriftfürNaturforschung A*, vol. 75, no. 12, pp. 1025–1037, 2020.

[9] A. L. I. Viet-Thanh Pham, A. L.-S. A. I. D. I. Dalia Sami, M. G. Nadia, K. Rajagopal, F. E. Alsaadi, and S. Jafari, "A novel mega-stable chaotic circuit," *Radioengineering*, vol. 29, no. Issue 1, pp. 140–146, 2020.

[10] G. Datseris and A. Wagemakers, "Effortless estimation of basins of attraction," *Chaos*, vol. 32, no. 2, Article ID 023104, 2022.

[11] M. Yousefi Valandar, P. Ayubi, M. Jafari Barani, and B. Yosefnezhad Irani, "A chaotic video steganography technique for carrying different types of secret messages," *Journal*

of Information Security and Applications, vol. 66, Article ID 103160, 2022.

[12] A. Akgul, B. Gurevin, I. Pehlivan, M. Yildiz, M. C. Kutlu, and E. Guleryuz, "Development of microcomputer based mobile random number generator with an encryption application," *Integration*, vol. 81, pp. 1–16, 2021.

[13] C. Z. Liew, R. Shaw, L. Li, and Y. Yang, "Survey on biometric data security and chaotic encryption strategy with Bernoulli mapping," in *Proceedings of the 2014 International Conference on Medical Biometrics*, pp. 174–180, Shenzhen, China, May 2014.

[14] A. Akgül, M. Z. Yıldız, ÖF. Boyraz, E. Güleryüz, S. Kaçar, and B. Gürevin, "Microcomputer-based encryption of vein images with a non-linear novel system," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 35, no. 3, pp. 1369–1385, 2020.

[15] M. A. Murillo-Escobar, C. Cruz-Hernàndez, F. Abundiz-Pèrez, and R. M. Lòpez-Gutièrrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8198–8211, 2015.

[16] F. Abundiz-Pérez, C. Cruz- Hernàndez, M. A. Murillo-Escobar, R. M. Lòpez-Gutièrrez, and A. Arellano-Delgado, "A fingerprint image encryption scheme based on hyperchaotic Rössler map," *Mathematical Problems in Engineering*, vol. 2016, Article ID 2670494, 15 pages, 2016.

[17] G. Mehta, M. K. Dutta, and P. S. Kim, "An efficient & secure encryption scheme for biometric data using holmes map & singular value decomposition," in *Proceedings of the 2014 International Conference on Medical Imaging, M-Health and Emerging Communication Systems (MedCom)*, pp. 211–215, Greater Noida, India, November 2014.

[18] G. Hanchinamani and L. Kulakarni, "Image encryption based on 2-D Zaslavskii chaotic map and Pseudo hadmard transform," *International Journal of Hospitality Information Technology*, vol. 7, no. 4, pp. 185–200, 2014.

[19] F. Han, J. Hu, X. Yu, and Y. Wang, "Fingerprint images encryption via multi-scroll chaotic attractors," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 931–939, 2007.

[20] B. Arıcıoğlu and S. Kaçar, "Circuit implementation and PRNG applications of time delayed Lorenz System," *Chaos Theory and Applications*, vol. 4, no. 1, pp. 4–9, 2022.

[21] S. Mobayen, C. Volos, Ü. Çavuşoğlu, and S S Kaçar, "A simple chaotic flow with hyperbolic sinusoidal function and its application to voice encryption," *Symmetry*, vol. 12, p. 2047, 2020.

[22] M. Varan, A. Akgul, F. Kurugollu, A. Sansli, and K. Smith, "A novel security methodology for smart grids: a case study of microcomputer-based encryption for PMU devices," *Complexity*, vol. 2021, Article ID 2798534, 15 pages, 2021.

[23] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, p. 577, 2019.

[24] Q. Lai, Z. Wan, A. Akgul, O. F. Boyraz, and M. Z. Yildiz, "Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption," *Chinese Journal of Physics*, vol. 67, pp. 615–630, 2020.

[25] G. Mehta, M. K. Dutta, and P. S. Kim, "Combinational domain-based encryption using FrWT and hyper-chaotic system for biometric data security," *Information Security Journal: A Global Perspective*, vol. 26, no. 4, pp. 198–211, 2017.

[26] M. Zhang and X. Tong, "A new chaotic map-based image encryption schemes for several image formats," *Journal of Systems and Software*, vol. 98, pp. 140–154, 2014.

[27] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocessors and Microsystems*, vol. 65, pp. 1–6, 2019.

[28] R. Li, Q. Liu, and L. Liu, "Novel image encryption algorithm based on improved logistic map," *Institution of Engineering and Technology Image Processing*, vol. 13, no. 1, pp. 125–134, 2019.

[29] Ö.F. Boyraz, M. E. Çimen, E. Güleryüz, and Z. Yıldız, "A chaos-based encryption application for wrist-vein images," *Chaos Theory and Applications*, vol. 3, no. 1, pp. 3–10, 2021.

[30] S. Yoosefian Dezfuli Nezhad, N. Safdarian, and S. A. Hoseini Zadeh, "New method for fingerprint images encryption using DNA sequence and chaotic tent map," *Optik*, vol. 224, Article ID 165661, 2020.

[31] J. C. Sprott, "Elegant chaos: algebraically simple chaotic flows," *World Scientific*, 2010.

[32] J. C. Sprott, S. Jafari, A. J. M. Khalaf, and T. Kapitaniak, "Megastability: coexistence of a countable infinity of nested attractors in a periodically-forced oscillator with spatially-periodic damping," *European Physical Journal: Special Topics*, vol. 226, no. 9, pp. 1979–1985, 2017.

[33] K. Rajagopal, J. P. Singh, B. K. Roy, and A. Karthikeyan, "Dissipative and conservative chaotic nature of a new quasi-periodically forced oscillator with megastability," *Chinese Journal of Physics*, vol. 58, pp. 263–272, 2019.

[34] P. Prakash, K. Rajagopal, J. P. Singh, and B. K. Roy, "Megastability, multistability in a periodically forced conservative and dissipative system with signum nonlinearity," *International Journal of Bifurcation and Chaos*, vol. 28, no. 09, Article ID 1830030, 2018.

[35] P. Prakash, K. Rajagopal, J. P. Singh, and B. K. Roy, "Megastability in a quasi-periodically forced system exhibiting multistability, quasi-periodic behaviour, and its analogue circuit simulation," *Adverse Event Unit- International Journal of Electronics and Communications*, vol. 92, pp. 111–115, 2018.

[36] H. Jahanshahi, K. Rajagopal, A. Akgul, N. N. Sari, H. Namazi, and S. Jafari, "Complete analysis and engineering applications of a megastable nonlinear oscillator," *International Journal of Non-linear Mechanics*, vol. 107, pp. 126–136, 2018.

[37] C. Li, J. C. Sprott, W. Hu, and Y. Xu, "Infinite multistability in a self-reproducing chaotic system," *International Journal of Bifurcation and Chaos*, vol. 27, no. 10, Article ID 1750160, 2017.

[38] C. Li, J. C. Sprott, and Y. Mei, "An infinite 2-D lattice of strange attractors," *Nonlinear Dynamics*, vol. 89, no. 4, pp. 2629–2639, 2017.

[39] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[40] F. Magalhães, H. P. Oliveira, and A. Campilho, "SPD2010-fingerprint singular points detection competition database," 2010, https://paginas.fe.up.pt/%7Espd2010/.

[41] S. Arslan Tuncer and T. Kaya, "True random number generation from bioelectrical and physical signals," *Computational and Mathematical Methods in Medicine*, vol. 2018, Article ID 3579275, 11 pages, 2018.

[42] F. Yu, Z. Zhang, H. Shen et al., "Design and FPGA implementation of a pseudo-random number generator based on a Hopfield neural network under electromagnetic radiation," *Frontiers in Physics*, vol. 9, Article ID 690651, 2021.

[43] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," *IET Image Processing*, vol. 14, no. 1, pp. 40–52, 2020.

[44] Y. Wu, *NPCR and UACI Measurements with Statistical Tests*, MATLAB Central File Exchange, Natick, MA, USA.

[45] Y. Su, W. Xu, and J. Zhao, "Optical image encryption based on chaotic fingerprint phase mask and pattern-illuminated Fourier ptychography," *Optics and Lasers in Engineering*, vol. 128, Article ID 106042, 2020.

[46] R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30583–30603, 2021.

[47] Y. Su, W. Xu, T. Li, J. Zhao, and S. Liu, "Optical color image encryption based on fingerprint key and phase-shifting digital holography," *Optics and Lasers in Engineering*, vol. 140, Article ID 106550, 2021.

[48] E. A. Umoh and O. N. Iloanusi, "A topology for fingerprint image encryption based on HDWT-SVD and hyperchaos," in *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, Lagos, Nigeria, April 2022.

[49] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Suggested integral analysis for chaos-based image cryptosystems," *Entropy*, vol. 21, no. 8, p. 815, 2019.

[50] R. Hosseinzadeh, M. Zarebnia, and R. Parvaz, "Hybrid image encryption algorithm based on 3D chaotic system and choquet fuzzy integral," *Optics*, vol. 120, Article ID 105698, 2019.