Entropy **2015**, *17*, 1387-1410; doi:10.3390/e17031387

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Review

Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing

Piyush Kumar Shukla [1,*], Ankur Khare [2], Murtaza Abbas Rizvi [3], Shalini Stalin [4] and Sanjay Kumar [5]

[1] Computer Science & Engineering, University Institute of Technology, RGPV, Bhopal, Airport Bypass Road, Gandhi Nagar, Bhopal 462033, India

[2] Computer Science, Government Women's Polytechnic College, Sehore 462033, India; E-Mail: khareankur94@gmail.com

[3] National Institute of Technical Teachers' Training and research, Shamla Hills, Bhopal 462001, India; E-Mail: marizvi@nitttrbpl.ac.in

[4] AISECT, Scope Campus, Nh-12, Near Misrod,Hoshangabad Road, Bhopal 462047, India; E-Mail: shalini.stalin@yahoo.com

[5] Department of Information Technology, National Institutes of Technology, Raipur 492010, India; E-Mail: skumar.it@nitrr.ac.in

* Author to whom correspondence should be addressed; E-Mail: pphdwss@gmail.com; Tel.: +91-9425378576.

Academic Editor: Kevin H. Knuth

Received: 24 July 2014 / Accepted: 22 December 2014 / Published: 19 March 2015

Abstract: Recently, chaotic dynamics-based data encryption techniques for wired and wireless networks have become a topic of active research in computer science and network security such as robotic systems, encryption, and communication. The main aim of deploying a chaos-based cryptosystem is to provide encryption with several advantages over traditional encryption algorithms such as high security, speed, and reasonable computational overheads and computational power requirements. These challenges have motivated researchers to explore novel chaos-based data encryption techniques with digital logics dealing with hiding information for fast secure communication networks. This work provides an overview of how traditional data encryption techniques are revised and improved to achieve good performance in a secure communication network environment. A comprehensive survey of existing chaos-based data encryption techniques and their application areas are presented. The comparative tables can be used as a guideline to select an encryption technique suitable for the application at hand. Based on the limitations of the existing techniques, an adaptive chaos based data encryption framework of secure communication for future research is proposed.

Keywords: cryptography; ubiquitous computing; randomness; chaos function; digital logic based system; security

1. Introduction

Advances in secure wired and wireless communication devices have led to the development of highly secure and fast data encryption techniques, so pervasive surveillance, chaotic-based encryption systems have attracted significant attention in many application domains such as the military, mobile communication, and private data encryption, as well as the intelligent and reliable applications. In these applications real time, fast, secure and reliable monitoring are essential requirements. These applications yield a huge volume of dynamic and heterogeneous text, image, audio and video data for transmission. These raw data can be transmitted in encrypted form (cipher text). For this purpose many traditional encryption algorithms can be used, but some of these algorithms are hard to understand, complex to implement, slow for encryption, and not suitable for real time applications, so a new concept of a chaotic system has arisen for highly secure, fast and easy implemented encryption systems for secure transmission networks.

2. Cryptology

It is the mathematical study of cryptography and cryptanalysis. It is used to provide protection for private information against theft. There are several contributing areas of cryptology [1]. (Figure 1).

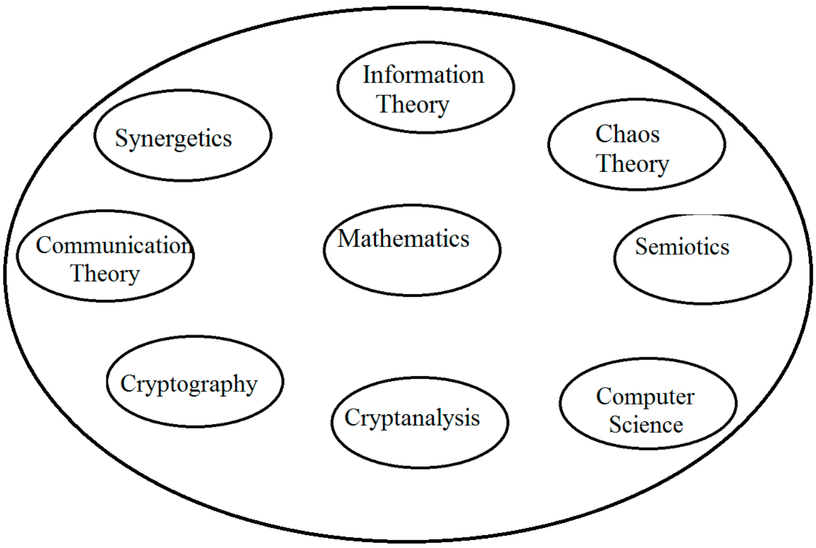

Figure 1. Contributing subject areas of cryptology.

3. Cryptography

A cryptographic system is a program or collection of programs which has transformed the information in unreadable format (cipher text) in a key dependent and unpredictable manner (Figure 2) [1].

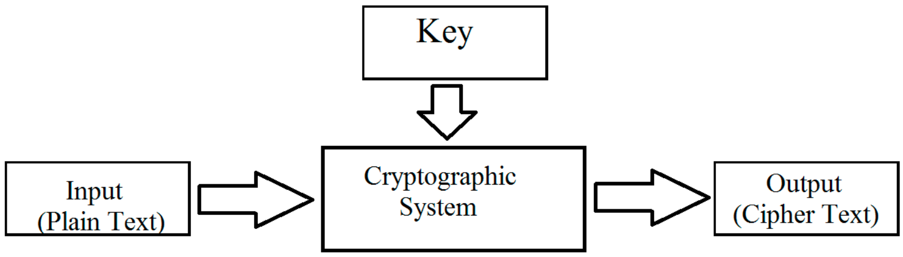

Figure 2. Cryptosystem.

4. Cryptanalysis [2]

Cryptanalysis is used to break the code and deduce a specific plain text or the key being used. All future and past information encrypted with that key are compromised. Table 1 summarizes the several types of cryptanalysis attacks, based on the amount of information identified by the cryptanalyst.

Table 1. Cryptanalysis Attacks.

Type of Attack	Known to Cryptanalyst
Cipher text only	• Encryption algorithm • Cipher text to be decoded
Known plain text	• Encryption algorithm • Cipher text to be decoded • One or more plain text-cipher text pairs formed with the secret key
Chosen plain text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key
Chosen cipher text	• Encryption algorithm • Cipher text to be decoded • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key
Chosen text	• Encryption algorithm • Cipher text to be decoded • Plain text message chosen by cryptanalyst, together with its corresponding cipher text generated with the secret key • The purported cipher text chosen by cryptanalyst, together with its corresponding decrypted plain text generated with the secret key

5. Chaos Theory

Chaos or chaotic system for short is an intervention between rigid regularity and unpredictability based on probability (Figure 3) [3].

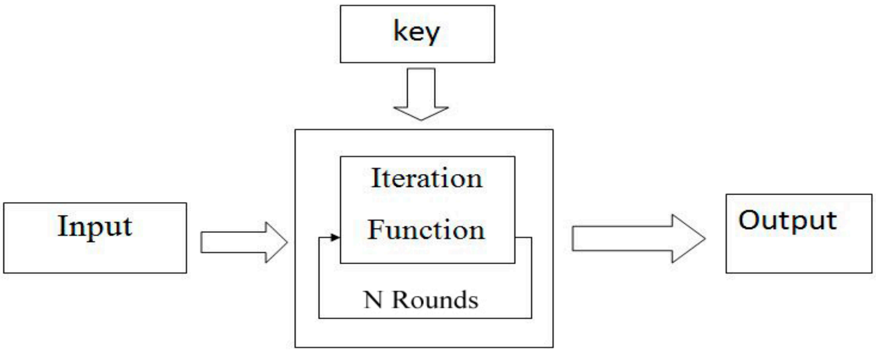

Figure 3. Chaos iterative function.

Chaos can be defined by some special characteristics [4].

- *Nonlinearity*: nonlinearity means that the change in an element at an initial time can escort to a change in the same or a different element at a later time, that is not depend to the change at the initial time.
- *Determinism*: it has not probabilistic (deterministic) which is governed by exact and correct rules with none of the element of chance.
- *Sensitivity to initial condition*: negligible changes in its initial state can generate fully different final state.
- *Irregularity*: it means "order in disorder".
- *Long term prediction*: chaos gives uncontrolled long term prediction due to sensitivity to initial conditions.
- *The logistic map*: the chaotic function uses logistic map. The map is one dimensional so it gives scalars for the encryption process.

$$Xn + 1 = A\ Xn\ (Xn - 1)$$

6. Application Areas of Chaos [4]

Historically, the chaos is used in mathematics and physics in starting. It prolonged into engineering and more recently into information and social science. A few years ago there has been rising interest in commercial and industrial applications of chaotic systems. There are several types of latent commercial and industrial applications based on different aspects of chaos based system which are shown in Table 2 [4].

Table 2. Chaos based Applications.

Category	Applications
Control	Control of irregular behavior in devices and systems.
Synthesis	Potential control of epilepsy, improved hesitant of systems, such as ring laser gyroscopes. Switching of packets in computer networks.
Synchronization	Secure communications, chaotic broad band radio, and encryption.
Information Processing	Encoding, decoding, and storage of information in chaotic systems, such as memory elements and circuits. Better performance of neural networks. Pattern recognition.
Short Term Prediction	Contagious diseases, weather, economy.

Table 2. *Cont.*

Category	Applications
Engineering	Vibration control, stabilization of circuits, chemical reactions, turbines, power grids, lasers, fluidized beds, combustion, and many more.
Computers	Switching of packets in computer networks. Encryption. Control of chaos in robotic systems.
Communications	Information compression and storage. Computer network design and management.
Medicine and Biology	Cardiology, heart rhythm (EEG) analysis,Prediction and control of irregular heart activity (chaos-aware defibrillator).
Management and Finance	Economic forecasting, restructuring, financial analysis, and market prediction and intervention.
Consumer Electronics	Washing machines, dishwashers, air conditioners, heaters, mixers.

7. Chaos and Cryptography [1]

Chaos and cryptography share some similar characteristics shown in Figure 4:

(1) Both chaotic map and encryption system are deterministic (not probable).
(2) Both are unpredictable and not simple. It any external observer which has not any knowledge of the algorithm and initial condition as key, cannot understand the random behavior of the system.
(3) A chaotic system is sensitive to initial condition means Small changes of any element can be fully changed the output. Cryptography is depending key based confusion and diffusion, *means* modification of one bit of plain text or key could change all bits of the cipher text with 50% probability.
(4) The iterative chaotic system is topological transitive and cryptography is multi round transformation means Single chaotic map with iterative transformation.

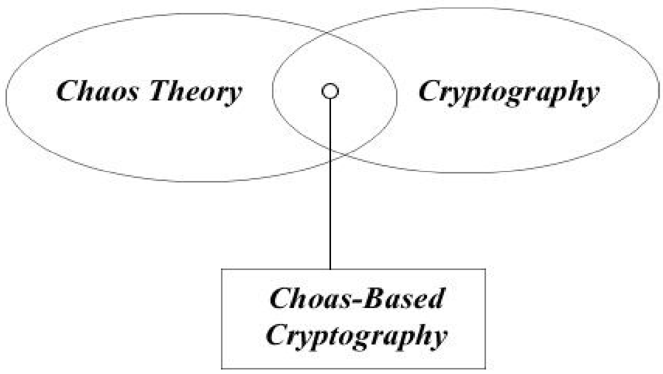

Figure 4. Relation between chaos and cryptography.

8. Traditional Encryption and Chaos Based Encryption [1]

Chaos is also different from cryptography in some other features [1].

(1) Chaotic systems are based on real/complex number spaces (bounded continuous space) whereas cryptography defined binary sequences (finite discrete space).

(2) Chaos theory is providing the idea to understand the asymptotic behavior of iterative processes whereas cryptography defined the characteristics of first a few iterations.

Table 3. Comparison between chaos based and traditional cryptosystem

Chaos Based Cryptosystem	Traditional Cryptosystem
Floating point arithmetic	Integer arithmetic
Slow computation	Fast computation
Based on any nonlinear function	Usually based on the mod function
Does not necessitate prime numbers	Usually based on prime numbers
Low cycle length	High cycle length
Statistical bias	No statistical bias
Data superfluous	Data companionable
Chaos Theory	**Cryptography**
Chaos based system	Pseudo-chaos based system
Indiscriminate transformation	Indiscriminate transformation
Infinite number of stages	Finite number of stages
Infinite number of repetitions	Finite number of repetitions
Initial stage	Plain text
Final stage	Cipher text
Initial situation and/or parameters	Keys
Asymptotic autonomy of initial and final stages	Confusion

9. Literature Survey

A new scheme is proposed performing lossless compression is based on the arithmetic coding (AC) and also encryption of data is based on a pseudo random bit generator (PRBG). The PRBG based on the standard logistic map and the Engel Continued Fraction (ECF) map to generate a key stream with both chaotic and algebraic features. The effectiveness and high performance of the BAC in lossless data compression and chaotic theory-based data encryption provide a technique used in many applications such as multimedia applications and medical Imaging [3]. Zhang, B. *et al.* proposed an improved chaos-based stream cipher in which a secret key with two158 key space sizes is composed of three independent chaos initial states. One chaos initial state gives two sampling quantified sequences which are generated by other two chaos initial states based on the pre-image compressibility of the logistic map. The probability of success of the algorithm is 1 and the computational complexity is 260.7 and negligible memory complexity and data complexity. The secret key entropy of the technique reduces from 158 to 60.7 [5]. A Modified Logistic Map (MLM) is used to get better logistic map performance based on the higher Lyapunov exponent and uniformity of bifurcation map. The proposed cipher provides 16 bits of encrypted data per clock cycle and hardware implementation results on aXilinx Virtex-6 FPGA provides a synthesis clock frequency of 93 MHz and a throughput of 1.5 Gbps using 16 hardware multipliers, so the cipher is appropriate for embedded strategies which have fixed constraints on power consumption, hardware resources and real-time parameters [6,7]. A chaos-based Short Message Service (SMS) encryption scheme is developed which combines with the improved A5/1 algorithm for mobile phones on FPGA. The security of chaos-based SMS encryption scheme can be analyzed on mobile phones [8].The new high speed chaotic cryptographic scheme requires a little memory capacity, but provides higher security. The proposed method generates better results than the

AESCTR based on correlation, UACI, NPCR, and NIST statistical tests. Encryption speed and security of the method is very high and its realization is easy with large key size and low memory capacity, so it fulfills the requirements of industrial control used in Wi-Fi and ZigBee networks [9,10].

Electrocardiogram (ECG) signals could be applied as a new tool for biometric recognition which isused for information security. The encryption system collects ECG signals from the person performing the encryption using a portable instrument. The chaos theory-based algorithm is used to generate initial keys for the logistic map for encryption. Simulation results show the efficiency, security and feasibility of the system. The encryption time is also acceptable with same sizes of cipher text and plaintext [11]. The chaotic system at the transmitter and receiver has a secret key and a chaotic system is used for mixing the plaintext with the chaotic output known as pseudo noise. This methodology demonstrated that chaotic maps enhanced the strength of the algorithms as compared to the cases when no chaos is used [12]. A chaotic pseudo cryptosystem is implemented on a finite precision machine to show both analog and digital implementation with the limitations using a pseudo-chaotic cryptosystem [13].

The weaknesses of synchronized chaotic-based cryptosystem are also investigated against known plaintext and chosen plaintext attacks to recover the system parameters. It is shown that the computational complexity of the chosen plaintext attack can be reduced to yield a simple set of linear equations [14]. Chaotic dynamical systems in cryptography are also represented some mathematical properties which determine the security and performance of different algorithms and systems [15]. Periodic switching of cryptographic keys is normally used as a method to boost the security of cryptographic systems, so a new encryption approach is proposed that combines chaotic behavior with the periodic switching of keys. A drawback of the cycling chaos results from the fact that the switching of attractors can potentially enhance the encryption time of each character which is not quantified [16]. The two-dimensional discretized chaotic map-based encryption algorithm was proposed for analyzing the security weaknesses against chosen cipher text attacks. A dependence among secret parameters give a smaller key space that can be revealed using a chosen cipher text attack and also shows the feasibility of attacks [17]. The discrete-time hyper chaotic system is applied for the synchronization of a two-channel secure communication system. Numerical simulations demonstrate the efficiency of the two channel-secure communications approach using the synchronization of 3D indiscriminate hyper chaotic H'enon maps as transmitter and receiver key [18].

Chaos-based techniques are also useful for block encryption ciphers based on two well-known chaotic maps—exponential and logistic—used to produce ciphers with differential and linear approximation probabilities. Cryptanalysis shows that there exists no more efficient attack to ciphers than brute force in a Feistel network. The Feistel network generates secure S-boxes: table-driven nonlinear substitution operations with the help of chaos theory[19,20].The theoretical and simulation results show the high speed and easy implementation and high security of the algorithm with chaotic properties such as ergodicity and sensitive dependence on initial conditions, so it is used practically in secure communication [21,22].Chaos-based encryption techniques have high unpredictability and simplicity of implementation over conventional secure communications systems. The four chaotic modulation techniques Chaotic Masking (CM), Chaos Shift Keying (CSK), Chaos On-Off Keying (COOK), and Differential Chaos Shift Keying (DCSK) are implemented for the Lorenz system as a chaos generator using Simulink in a Matlab environment [23,24]. The AES algorithm has been used for various wireless sensor network standards such as Zig Bee, Wireless HART and ISA100.11a. Both algorithms are evaluated on TelosB motes and it was demonstrated that the chaos-based algorithm is much faster than the AES-based algorithm with the same cryptography quality [25].

A differential analysis method is introduced to evaluate the feasibility and the security of chaos used in cryptographic algorithm design and conventional cryptosystem for commercial fields [26,27]. The Wei scheme is perfectly used against Unicity distance (The length of an original cipher text needed to break the cipher by reducing the number of possible spurious keys to zero in a brute force attack) mathematically or logically which makes the Wei scheme suitable for practical applications [28]. Chaos cryptogram shave a significant advantage in the encryption of multimedia information which is transmitted in the form of streams from the initial crunode to other crunodes [29].The public-key cipher based on the finite-state Chebyshev map is slower than RSA and the best conventional algorithms, such as AES. Since this result is by nature asymptotic it is believed that it has no practical consequences, but it does put limits (if theoretical) onchaos-based cryptography with the same standards of security and speed as in conventional cryptography [30,31]. The Chebyshev polynomials-based public key encryption algorithm for textual data provides security against cryptanalysis attacks using a simple hashing algorithm and digital signature [32].

A novel authentication scheme combining chaotic cryptographics and a hashing scheme to produce the hash value for a given message for collision free encryption is used in practical secure communication [33]. The Baptista-type chaotic cryptosystem for embedding compression and encryption using a lookup table is determined adaptively by the probability of occurrence of plaintext symbols. The key space of the cryptosystem is equivalent to 130 bits, which guarantees that the cipher text is no longer than the plaintext [34,35]. A symmetric cryptographic technique based on chaos properties (sensitivity to initial conditions and ergodicity) which are exploited to produce an avalanches effect by which two different keys produce different cipher text for the same message is proposed in [36].

Digital chaotic generators are capable of building robust and fast chaos-based cryptosystems and chaos-based steganography and watermarking systems whose performances are measured in terms of the tradeoff between security and speed [37]. A novel digital anticounterfeiting scheme is developed based on chaotic cryptography which supports multiple and repeated queries for authentication and intelligent identification and provided security against batch copy and database attack fraud [38]. A quantum key establishment process-based cryptography, an extension to the BB84 protocol, K05, using chaos functions with shortest key is developed for faster encryption [39]. Several one-dimensional chaotic maps generate independent and approximately uniform pseudo dynamic sequences for the block encryption algorithm [40]. Deng developed improved clock synchronized and unsynchronized schemes using a chaotic maps-based key agreement protocol. It is described that the asynchronous key agreement protocol can’t resist replaying attacks so it is not used for security applications [2]. Every single character is encrypted by the Baptista method using a regular changing key for controlling the chaos attractor to improve the encryption security [41]. A new kind of chaotic encryption algorithm, duality chaos, is also proposed to overcome the limitations of chaotic systems for practical applications [42].

10. Comparison Table

The various research papers have been summarized based on some features in Table 4.

Table 4. Comparison table.

	Authors Name & Performance Comparison of Their Research Papers					
Features	**A.B. Orue *et al.* [43]**	**A. Masmoudi *et al.* [3]**	**A. Palacios *et al.* [16]**	**Ahmed M. Elshamy *et al.* [44]**	**Amit Pande *et al.* [6]**	**Bassem Bakhache *et al.* [9]**
Security	Moderately high	High	High	Secure enough	Comparatively high	High
Cryptanalysis Attack Prevention	All four	Chosen and Known Plain text	All four	-	Except Known plaintext	Linear and Differential
Cipher type	Stream	Stream	Stream	-	Stream	Stream
Application Area	Communication System	Medical Imaging	Communication System	Optical image Encryption	Real Time Embedded Systems	Industrial Control
Space Complexity	Medium	More space	High	Medium	High	Low
Implementation of algorithm	Complex	Hard	Hard	More Complex	Hard	Highly Complex
Used technique	Chaos Synchronization	BAC and PRBG	Periodic switching	Chaotic Baker Map and DRPE	MLM based PRNG	PWLCM
Efficiency/Reliability	Medium	High	High	Comparable High	Medium	High
Methodology/Environment	Matlab Environment	C++	-	Matlab	XilinxVirtex-6 FPGA	NIST Environment
Speed (Processing)	Slow	High	Slow	High	Enough	High
Prediction Possibility	Slightly	Probably	No	No	No	Slightly
Feasible	Yes	No	At some condition	Yes	No	No
Accuracy	Medium	Medium	High	High	Medium	Medium
Key length	Large enough	Large	Large	Large enough	High	Slightly Large
Cost	Medium	High	Medium	High	High	Low
Quality Assurance	Medium	Resemblance	High	High	Applicable	Resemblance

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers					
Features	**Bassem Bakhache *et al.* [10]**	**Bhavana Agrawal *et al.* [45]**	**Bin Zhang *et al.* [5]**	**Brad Aimone *et al.* [46]**	**Ching Kun Chen *et al.* [11]**	**C. Wang *et al.* [47]**
Security	High	Medium	Medium	Secure enough	Comparatively high	High
Cryptanalysis Attack Prevention	Linear and Differential	All Four	Inversion and compression	-	Brute Force Attack	-
Cipher type	Stream	Stream and Block	Stream	-	Stream and Block	Stream and Block
Application Area	Industrial Control	Communication Systems	Communication System	Electronics Circuit System	Real World Applications	Communication System
Space Complexity	Low	High	Negligible	High	Enough High	Medium
Implementation of algorithm	Highly Complex	Hard	Enough Complex	More Complex	Medium	Much Complex
Used technique	PWLCM	-	Fu's Chaotic System	Richert and Whitmer's Circuit	ECG Circuit	Backstepping with Tunning function
Efficiency/Reliability	High	Medium	Medium	Comparable High	Medium	Medium
Methodology/Environment	NIST Environment	-	-	Matlab	-	Rossler System
Speed (Processing)	High	Medium	Comparatively High	Low	Acceptable	High
Prediction Possibility	Slightly	Yes	No	No	At Some Condition	No
Feasible	No	No	At Some Condition	Yes	Reasonable	No
Accuracy	Medium	Reasonable	Medium	High	Reasonable	High
Key length	Slightly Large	Large	Large	Large	Enough Large	Large
Cost	Low	Medium	Medium	High	Slightly High	High
Quality Assurance	Resemblance	Applicable	Resemblance	Medium	Applicable	Resemblance

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers					
Features	**Dalia H. Elkamshoushy *et al.* [12]**	**Daniel Ioan Curiac *et al.* [13]**	**Ercan Solak [14]**	**Ercan Solak *et al.* [17]**	**Fei Peng *et al.* [48]**	**Filali Rania Linda *et al.* [18]**
Security	High	Medium	Medium	Secure enough	High	Medium
Cryptanalysis Attack Prevention	Brute Force and Chosen Cipher text	Not Enough	Known and Chosen Plaintext	Chosen Cipher text	All Four Attack	-
Cipher type	Block	Block	Stream and Block	Block	Block	Stream and Block
Application Area	Communication System	Real Life	Communication System	Communication System	CCTV in Airport and Bank	Communication System
Space Complexity	High	High	Medium	High	Enough High	High
Implementation of algorithm	Complex	Medium	Easy	More Complex	Complex	Much Complex
Used technique	Chaotic mixing System	Baptista System	Discrete Time Chaotic System	TDCM System	ROI and FMO in H.264	Aggregation Technique
Efficiency/Reliability	High	Medium	Medium	Comparatively High	High	Medium
Methodology/Environment	-	-	-	-	NIST Environment	-
Speed (Processing)	Low	Low	Comparatively High	Medium	Acceptable	Medium
Prediction Possibility	No	No	No	Slightly	No	No
Feasible	Yes	Slightly	At Some Condition	Yes	Reasonable	No
Accuracy	Medium	Medium	Medium	High	Reasonable	High
Key length	Large	Large	Large Enough	Short	Enough Large	Large
Cost	High	High	Medium	High	Slightly High	High
Quality Assurance	Applicable	Medium	Resemblance	Medium	Applicable	Resemblance

Table 4. *Cont.*

Features	Authors Name & Performance Comparison of Their Research Papers					
	G. Alvarez *et al.* [49]	**Ganesh Babu S. *et al.* [19]**	**Goce Jakimoski *et al.* [20]**	**Gonzalo Alvarez *et al.* [50]**	**Gouping Tang *et al.* [21]**	**I.A. Kamil *et al.* [23]**
Security	High	High	Secure enough	Medium	Reasonable	High
Cryptanalysis Attack Prevention	All Four	Chosen and Known Plain Text	All Four	Linear and Differential	Chosen Cipher Text	-
Cipher type	Block	Stream and Block	Block	Block	Block	-
Application Area	Communication System	Internet Banking	Communication System	Telecommunication System	Communication System	Mobile Communication System and Internet
Space Complexity	High	High	Medium	Enough High	Medium	High
Implementation of algorithm	Complex	Complex	Easy	Easy	Easy	Easy
Used technique	Non Linear Dynamic System	Discrete Time Chaotic System	Block Encryption Cipher	Chaotic Masking and Switching	Chaotic Masking	CM, CSK, COOK and DCSK
Efficiency/Reliability	Medium	High	Medium	Comparatively High	High	High
Methodology/Environment	-	-	Feistel Network	-	-	Matlab environment
Speed (Processing)	Medium	Low	Comparatively High	Medium	High	High
Prediction Possibility	Yes	No	No	Slightly	No	No
Feasible	No	Slightly	At Some Condition	Yes	Reasonable	Yes
Accuracy	Low	Medium	Medium	High	Medium	High
Key length	Large enough	Large	Large Enough	Large	Large	Large
Cost	Medium	High	Medium	High	Slightly High	High
Quality Assurance	Applicable	Medium	Resemblance	Medium	Applicable	Medium

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers					
Features	**Ismail Mansour *et al.* [25]**	**Jinhong Luo *et al.* [29]**	**Jing Pan *et al.* [8]**	**J.M. Amigo *et al.* [30]**	**J M Blackledge *et al.* [1]**	**Jun Wei *et al.* [26]**
Security	High	Medium	Secure enough	Medium	Reasonable	Secure Enough
Cryptanalysis Attack Prevention	Except Brute Force	-	-	All Four	All Four	Differential
Cipher type	Stream	Stream	Stream	Stream and Block	Stream	Block
Application Area	Industrial and Military	Multimedia System	Mobile System	Industrial and Communication System	Stream Coding and Spread Spectrum	Commercial Field
Space Complexity	Low	High	Medium	Enough High	Medium	High
Implementation of algorithm	Complex	Easy	Complex	Complex	Easy	Complex
Used technique	PWLCM and LFSR	Nonlinear Dynamic System	A5/1 Algorithm	AM, CSK, TCC and ME	Vernam Cipher Technique	PLCM
Efficiency/Reliability	High	Medium	Medium	High	High	Medium
Methodology/Environment	TelosB and Matlab Environment	-	GSM and FPGA System	Chebyshev Map	Lyapunov Exponent	-
Speed (Processing)	High	Low	Low	Medium	High	High
Prediction Possibility	No	Yes	No	Slightly	No	No
Feasible	Yes	Slightly	At Some Condition	Yes	Reasonable	Yes
Accuracy	High	Medium	Medium	High	Medium	High
Key length	Large	Large Enough	Large Enough	Large	Large	Large
Cost	High	Medium	Medium	High	Slightly High	High
Quality Assurance	Applicable	Resemblance	Medium	Medium	Applicable	Medium

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers					
Features	**Jun Wei *et al.* [28]**	**Jun Wei *et al.* [27]**	**Jun Wei *et al.* [33]**	**K. Prasadh *et al.* [32]**	**Kristina Kelber *et al.* [51]**	**Kwok Wo Wong *et al.* [34]**
Security	Medium	High	Secure enough	Medium	High	Secure Enough
Cryptanalysis Attack Prevention	Brute Force	All Four	Brute Force	Chosen Plain text	-	Except Known plain Text
Cipher type	Stream	Stream andblock	Stream and Block	Block	Stream and Block	Block
Application Area	Signal Processing	Multimedia System	Multimedia System	Image and Video Encryption System	Image and Video Encryption System	Commercial Field
Space Complexity	Medium	High	Medium	Enough High	Medium	High
Implementation of algorithm	Complex	Easy	Complex	Complex	Complex Enough	Easy
Used technique	Wei Scheme and Unicity distance	PLCM Map	PLCM	Multilevel Scrambling and Hash	3D Baker Map	Huffman Coding
Efficiency/Reliability	Medium	Medium	High	High	High	Medium
Methodology/Environment	-	-	C++	Chebyshev Map	-	Baptista Map
Speed (Processing)	High	Low	Low	High	High	High
Prediction Possibility	No	Yes	No	No	No	No
Feasible	Yes	Slightly	At Some Condition	Yes	Reasonable	Yes
Accuracy	High	Medium	High	High	Medium	High
Key length	Large	Large Enough	Large	Large Enough	Large	Large Enough
Cost	High	Medium	High	High	Slightly High	High
Quality Assurance	Medium	Resemblance	High	Medium	Applicable	Medium

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers					
Features	**Kwok Wo Wong *et al.* [35]**	**Ljupco Kocarev *et al.* [31]**	**Ljupco Kocarev [22]**	**Long Jye Sheu *et al.* [52]**	**Mohamed I. Sobhy *et al.* [24]**	**M. S. Azzaz *et al.* [53]**
Security	Medium	High	High	Medium	Secure Enough	Secure Enough
Cryptanalysis Attack Prevention	Known Plain Text	Linear and Differential	All Four	-	Brute Force Attack	-
Cipher type	Block	Block	Block	Stream	Stream	Stream
Application Area	Image and Audio Encryption System	Communication System	Multimedia System	Communication System	Real Time Applications	Real Time Embedded Applications
Space Complexity	High	High	High	Enough High	Medium	Medium
Implementation of algorithm	Complex	Easy	Complex	Complex	Complex Enough	Hard
Used technique	Shannon Coding	Feistel Cipher System	Symbolic Dynamic System	Fractional Lorenz System	FPGA	Virtex Xilinx FPGA
Efficiency/Reliability	Medium	High	High	Medium	High	Medium
Methodology/Environment	NIST Environment	Chebyshev Map	Lyapunov Exponent System	-	Rosseler System	Chen's and Rossler's 3D chaotic systems
Speed (Processing)	High	Low	Low	High	High	Medium
Prediction Possibility	No	Yes	No	No	No	No
Feasible	Slightly	Yes	At Some Condition	Yes	Reasonable	Yes
Accuracy	High	Medium	Medium	Medium	Medium	Medium
Key length	Large	Large Enough	Large	Large Enough	Large	Large Enough
Cost	High	High	High	High	Slightly High	Medium
Quality Assurance	Applicable	High	Medium	Applicable	Applicable	High

Table 4. *Cont.*

Features	**Authors Name & Performance Comparison of Their Research Papers**					
	P. Jhansi Rani *et al.* [36]	**R. Hasimoto Beltran *et al.* [54]**	**Ronald Schmitz *et al.* [15]**	**Safwan EI Assad [37]**	**Shujun Li *et al.* [55]**	**Shujun Li *et al.* [56]**
Security	High	High	Medium	Medium	High	Secure Enough
Cryptanalysis Attack Prevention	All Four	Brute Force Attack	-	Message Recovery Attack	All Four	All Four
Cipher type	Stream	Block	Block and Stream	Block	Block	Block
Application Area	Communication System	Real Time Multimedia Applications	Communication System	Medical and Enterprises System	Distributed System	Communication System
Space Complexity	High	High	Medium	Enough High	Medium	Medium
Implementation of algorithm	Complex	Complex Enough	Complex	Complex	Easy	Hard
Used technique	Logistic Encryption	Three-level Periodic Perturbation Scheme	Chaotic Dynamic System	PWLCM	Bernoulli Probabilistic System	Chaotic Masking and Switching System
Efficiency/Reliability	Medium	High	Desirable	High	Medium	High
Methodology/Environment	-	-	-	NIST Environment	-	-
Speed (Processing)	Medium	High	Low	High	High	Medium
Prediction Possibility	No	Yes	No	No	No	Yes
Feasible	No	No	No	Yes	Reasonable	Yes
Accuracy	High	Medium	High	High	Medium	High
Key length	Large	Large	Large Enough	Large Enough	Large	Large Enough
Cost	High	High	Medium	High	Medium	Slightly High
Quality Assurance	Applicable	Medium	Medium	Reasonable	Applicable	High

Table 4. *Cont.*

	Authors Name & Performance Comparison of Their Research Papers						
Features	**Shun Cheng Hong *et al.* [57]**	**Stamatios V. Kartalopoulos [39]**	**Sundarapandian Vaidyanathan [58]**	**Suying Sheng *et al.* [38]**	**Tao Yang [59]**	**Wang Xing Yuan *et al.* [40]**	**Renz Lozi *et al.* [60]**
Security	High	High	Medium	High	High	Secure Enough	High
Cryptanalysis Attack Prevention	All Four	-	-	Message Recovery Attack	All Four	All Four	-
Cipher type	Stream and Block	Stream	Block	Stream	Block	Block	-
Application Area	Multimedia Application	Communication Systems	Physical and Chemical System	Mutual Authentication System	Secure Communication	Communication System	Noise Reduction system
Space Complexity	High	Medium	High	Enough High	Medium	Medium	High
Implementation of algorithm	Complex	Complex Enough	Complex	Complex	Highly Complex	Hard	Hard
Used technique	REC/RPB Scheme	BB84 Algorithm	Hyperchaotic Lu and Xu System	Digital Anticounterfeiting Technique	Impulsive Synchronization System	Dynamic Chaotic System	Cascade Chaotic Syncronization Technique
Efficiency/ Reliability	High	High	Desirable	High	Medium	High	Medium
Methodology/ Environment	PWLCM and Zhu's Circuits	NIST Environment	-	C# Environment	-	-	-
Speed (Processing)	Medium	High	Low	High	Medium	High	Medium
Prediction Possibility	No	Yes	No	Yes	No	Yes	No
Feasible	Yes	No	No	Yes	Reasonable	Yes	Reasonable
Accuracy	High	High	Medium	Medium	High	High	Medium
Key length	Large	Large	Large Enough	Large Enough	Large	Large Enough	Large Enough
Cost	High	High	High	High	High	Slightly High	Slightly High
Quality Assurance	High	Medium	Medium	Reasonable	Medium	High	Reasonable

Table 4. *Cont.*

Features	Authors Name & Performance Comparison of Their Research Papers						
	William Ditto *et al.* [4]	**Xianfeng Guo *et al.* [2]**	**Yong Peng Xiao *et al.* [41]**	**Zhao Geng *et al.* [7]**	**Zheng Guang Wu *et al.* [61]**	**Zheng Guo Li *et al.* [62]**	**Zhong Zhang *et al.* [42]**
Security	High	High	Medium	High	High	Secure Enough	Secure Enough
Cryptanalysis Attack Prevention	All Four	Replaying attack	All Four	All Four	Message Recovery Attack	Cipher text only	Brute Force
Cipher type	Stream and Block	Stream	Stream	Block	Block	Stream	Stream
Application Area	Chemical and Physical Application	Watermarking and Communication Systems	Secure Communication System	Real Time Applications	Biological Applications	Wireless and Video Phones System	Communication Systems
Space Complexity	Low	High	High	High	Medium	High	Medium
Implementation of algorithm	Complex	Complex Enough	Complex	Complex Enough	Highly Complex	Hard	Easy
Used technique	Synthesized Chaos System	Han Chang's Schemes	Periodic Switching	One Time One Algorithm	Lyapunov and Lur'e System	Chua's circuit	Dual Chaotic System
Efficiency/Reliability	High	Medium	Desirable	High	Desirable	High	Medium
Methodology/Environment	-	-	Lorenz System	Henon and Chebyshev System	Neural Network	-	Matlab Environment
Speed (Processing)	Medium	High	Low	Medium	High	Medium	Medium
Prediction Possibility	No	No	No	Yes	No	No	No
Feasible	Yes	No	No	Yes	Reasonable	Yes	Yes
Accuracy	High	Medium	Medium	High	High	High	Medium
Key length	Large Enough	Large	Large Enough	Large Enough	Large	Large Enough	Large
Cost	High	High	High	Medium	High	Slightly High	High
Quality Assurance	High	Medium	Medium	Reasonable	Applicable	High	High

11. Summary

Security and reliability of chaos-based encryption algorithms is enhanced by using PWLCM and Periodic Switching in C++ and a Matlab environment but at the same time implementation and maintenance cost of techniques are also increased because of the complexity of the algorithms. These applications are very useful for industrial and medical applications [3,9,16]. If an algorithm is compromised with security and feasibility then the cost and space-time complexity is reduced [3,6,43]. Qualities of techniques depend upon the accuracy, cost and processing time of the algorithm. If the feasibility of an algorithm is not possible then it shows the low quality and efficiency of the encryption technique [10,11,46]. Key length is also used to measure the prediction possibility and the complexity of algorithms. Large key length enhances the security and also space and time complexity but also increases the processing and memory cost [5,45–47].

Security of algorithms is analyzed against security attacks, *i.e.*, linear and differential cryptanalysis attacks using the Baptista system and TDCM system [13,17]. Some proposed algorithms are very strong against all cryptanalysis (plain text attack, known plaintext attack, *etc.*) attacks but the cost of these cryptosystems also enhanced with the quality and accuracy [12,13,17,18]. Key length is taken to be very large for increasing the complexity and security of algorithms [12–14]. Feasibility and efficiency are also used to describe the quality of maintenance and accuracy [18,48].

Chaotic masking and switching used for block and stream cipher in non-linear dynamic systems enhances the security, speed, accuracy and reliability of encryption systems without compromising the quality and feasibility [23,24,50,57]. Complexity of the algorithms is also increased with large key size, large space complexity and high processing speed by using discrete time chaotic systems for internet banking and communication systems, but also this also enhances the processing and maintenance costs [19,20,23,49]. Industrial and communication systems widely use unpredictable and feasible encryption techniques for secure and fast transmission of information [8,26,29]. Speed and accuracy of algorithms are also important factors for measuring the complexity and quality of algorithms. Security is a major issue for military and industrial applications [1]. It is the strength of the algorithms against different intruder attacks and cryptanalysis attacks [25,26,30].

Data integration, repudiation, secrecy and authentication are necessary key factors of any communication system. These are achieved by using some special techniques PLCM map, 3D Baker map, Huffman coding and unicity distance which are secure, fast, reliable and accurate [27,28,32,34]. Feasible and predictive systems are easily attacked by intruders with some effort [27,37]. The secrecy and security is enhanced by using large key size and complex algorithms. These techniques are widely used in multimedia applications [33,51]. High cost is an unnecessary drawback for industrial and communication systems but systems cannot use cheap circuits and equipment because of security [31,35,52]. Cost is also increased by using large key-based encryption systems and expensive environment like the NIST, Rosseler system and Lyapunov exponent system but security and quality of the algorithm are also enhanced [24,53]. All the systems are not much stronger against different types of attacks so these are not useful for real time applications [22,52]. The running time and space complexity have much high for large key size [36,54]. These properties are useful for industrial and multimedia applications with secure, qualitative, accurate and fast transmission for authenticated and confidential communication [15,56]. Feasible systems with data integration, repudiation, secrecy and authentication are achieved by taking large key size and complex algorithms which are widely used in mutual authentication systems [38,39,59]. The quality of the techniques depends upon the accuracy of the algorithm and key which are given unpredictable and infeasible stream and block cipher [40,57]. The speed of these systems is considerable because key length and implementation complexity of algorithm is high using the REC/RPB Scheme, BB84 Algorithm, and Digital Anticounterfeiting Technique [39,57,58].

Biological, physical, chemical and communication systems are broadly used for accurate and unpredictable secure encryption techniques [4,41]. These systems use complex algorithms and large key size for encrypting and decrypting the messages [2,7,41]. This introduces unwanted processing delays but also increases the security, accuracy and quality of algorithms [4,42,62]. Fast encryption does not provide reliability and high security, but reduces processing time [2,61].

12. Conclusions

On the basis of a study of all the above mentioned research papers it is determined that chaos has a number of characteristics such as good pseudo randomness, unpredictability and extreme sensitivity to initial state and structural parameters. These properties of chaotic systems are useful for faster and secure encryption and decryption of text as well as images with less computation as compared to conventional cryptography. Chaos-based encryption techniques are easily realized and have a very large key range and need low memory capacity, so they can be used in Wi-Fi and ZigBee networks in industrial control. Chaos-based algorithms should be implemented for protecting multimedia contents and logistic maps utilized to design new cryptographic algorithms. New hash functions can be generated with the help of a logistic map which gives better results than the current existing hash functions and it can also implemented in hardware. Chaotic maps increase the strength of the algorithm as compared to the cases when no chaos is used. The confusion and diffusion of chaos functions should be used for providing better trade-offs between security and computational complexity.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Blackledge, J.M. Cryptography using Chaos. Available online: http://konwersatorium.pw.edu.pl/wyklady/2010_VLZ7_02_wyklad.pdf (accessed on 17 March 2015).
2. Guo, X.; Zhang, J. Cryptanalysis of the Chaotic-based Key Agreement Protocols. In Proceedings of the International Symposium on Biometrics and Security Technologies (ISBAST), Islamabad, Pakistan, 23–24 April 2008; pp. 1–3.
3. Masmoudi, A.; Puech, W.; Bouhlel, M.S. A new joint lossless compression and encryption scheme combining a binary arithmetic coding with a pseudo random bit generator. *Int. J. Comput. Sci. Inf. Secur.* **2010**, *8*, 170–175.
4. Ditto, W.; Munakata, T. Principles and Applications of Chaotic System. *Comm. ACM* **1995**, *38*, 96–102.

5. Zhang, B.; Jin, C. Cryptanalysis of a Chaos-based Stream Cipher. In Proceedings of the 9th International Conference for Young Computer Scientists, Hunan, China, 18–21 November 2008; pp. 2782–2785.
6. Pande, A.; Zambreno, J. A Chaotic Encryption Scheme for Real-Time Embedded Systems: Design and Implementation. *Telecommun. Syst.* **2013**, *52*, 551–561.
7. Geng, Z.; Guanrong, C.; Jingqing, F.; Gang, X. Block Cipher Design: Generalized Single-Use-Algorithm Based on Chaos. *Tsinghua Sci. Tech.* **2011**, *16*, 194–206.
8. Pan, J.; Ding, Q.; Qi, N. The Research of Chaos-based SMS Encryption in Mobile Phone. In Proceedings of the Second International Conference on Instrumentation & Measurement, Computer, Communication and Control, Harbin City, China, 8–10 December 2012; pp. 501–504.
9. Bakhache, B.; Ahmad, K.; el Assad, S. A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks. *Int. J. Intell. Comput. Res.* **2011**, *2*, 219–227.
10. Bakhache, B.; Ahmad, K.; el Assad, S. Chaos Based Improvement of the Security of ZigBee and Wi-Fi Networks Used for Industrial Controls. In Proceedings of the International Conference on Information Society (i-Society), London, UK, 27–29 June 2011; pp. 139–145.
11. Chen, C.K.; Lin, C.L. Text Encryption Using ECG signals with Chaotic Logistic Map. In Proceedings of the the 5th Conference on Industrial Electronics and Applications (ICIEA) IEEE, Taichung, Taiwan, 15–17 June 2010; pp. 1741–1746.
12. Elkamshoushy, D.H.; Aboulsoud, A.K. Cryptographic Schemes Using Chaotic System. In Proceedings of the National Radio Science Conference NRSC, Tanta, Egypt, 18–20 March 2008; pp. 1–6.
13. Curiac, D.I.; Iercan, D.; Dranga, O.; Dragan, F.; Banias, O. Chaos-Based Cryptography: End of the Road? In Proceedings of the International Conference on Emerging Security Information, System and Technologies, Valencia, Spain,14–20 October 2007; pp. 71–76.
14. Solak, E. Cryptanalysis of Observer Based Discrete-Time Chaotic Encryption Schemes. *Int. J. Bifurcat. Chaos Appl. Sci. Eng.* **2005**, *15*, 653–658.
15. Schmitz, R. Use of chaotic dynamical systems in cryptography. *J. Franklin Inst.* **2001**, *338*, 429–441.
16. Palacios, A.; Juarez, H. Cryptography with cycling chaos. *Phys. Lett.* **2002**, 345–351.
17. Solak, E.; Cokal, C. Cryptanalysis of a cryptosystem based on discretized two-dimensional chaotic maps. *Phys. Lett.* **2008**, *372*, 6922–6924.
18. Linda, F.R.; Hammami, S.; Benrejeb, M.; Borne, P. Synchronization of Discrete-Time Hyperchaotic Maps Based on an Aggregation Technique for Encryption. In Proceedings of the 9th International Multi-Conference on systems, Signals and Devices, Chemnitz, Germany, 20–23 March 2012; pp. 1–6.
19. Babu, G.S.; Ilango, P. Higher Dimensional Chaos for Audio Encryption. In Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security CICS, Singapore, Singapore, 16–19 April 2013; pp. 52–58.
20. Jakimoski, G.; Kocarev, L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. *IEEE Trans. Circ. Syst. Fund. Theor. Appl.* **2001**, *48*, 163–169.
21. Tang, G.; Liao, X.; Xiao, D., Li, C. A Secure Communication Scheme Based on Symbolic Dynamics. In Proceedings of the 2004 International Conference on Communications, Circuits and Systems, Chengdu, China, 27–29 June 2004; pp. 13–17.
22. Kocarev, L. Chaos-Based Cryptography: A Brief Overview. *IEEE Circ. Syst. Mag.* **2001**, *1*, 1–16.

23. Kamil, I.A.; Fakolujo, O.A. Lorenz-Based Chaotic Secure Communication Schemes. *Ubiq. Comput. Commun. J.* **2008**, *7*, 1248–1254.
24. Sobhy, M.I.; Shehata A.R. Chaotic Algorithm for Data Encryption. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal, Salt Lake City, UT, USA, 07–11 May 2001; pp. 997–1000.
25. Mansour, I.; Chalhoub, G.; Barkhache, B. Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks. In Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 913–919.
26. Wei, J.; Zheng, J.; Yu, J.; Shuai, Y. Selection of Chaotic States in Cryptosystem Based on Chaos with Differential Analysis. In Proceedings of the 7th International Conference on Computer Science & Education, Melbourne, Australia, 14–17 July 2012; pp. 325–330.
27. Wei, J.; Shuai, Y.; Yu, J. Cryptography with Two Discretized Chaotic Maps. In Proceedings of the 8th International Conference on Computer Science & Education, Colombo, Sri Lanka, 26–28 April 2013; pp. 977–981.
28. Wei, J.; Zheng, J.; Yu, J.; Shuai, Y. Application of Unicity distance in a cryptosystem based on chaos. In Proceedings of the 7th International Conference on Computer Science & Education, Melbourne, Australia, 14–17 July 2012; pp. 345–348.
29. Luo, J.; Shi, H. Research of Chaos Encryption Algorithm Based on Logistic Mapping. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal, Pasadena, CA, USA, 18–20 December 2006; pp. 1–3.
30. Amigo, J.M.; Kocarev, L.; Szczepanski, J. Theory and practice of chaotic cryptography. *Phys. Lett.* **2007**, *366*, 211–216.
31. Kocarev L.; Amigo, J.M.; Szczepanski, J. Chaos-based Cryptography: an overview. In Proceedings of the International Symposium on Nonlinear Theory and its Applications, Bruges, Belgium, 18–21 October 2005; pp. 453–456.
32. Prasadh, K.; Ramar, K.; Gnanajeyaraman, R. Public key cryptosystems based on chaotic Chebyshev polynomials. *J. Eng. Tech. Res.* **2009**, *1*, 122–128.
33. Wei, J.; Zheng, X.; Yu, J.; Shuai, Y. A Novel Authentication Scheme Based on Chaos. In Proceedings of the 8th International Conference on Computer Science & Education, Colombo, Sri Lanka, 26–28 April 2013; pp. 879–882.
34. Wong, K.W.; Yuen, C.H. Embedding Compression in Chaos-Based Cryptography. *IEEE Trans. Circ. Syst.* **2008**, *55*, 1193–1197.
35. Wong, K.-W.; Lin, Q.; Chen, J. Simultaneous Arithmetic Coding and Encryption Using Chaotic Maps. *IEEE Trans. Circ. Syst.* **2010**, *57*, 146–150.
36. Rani, P.J.; Bhavani, S.D. Symmetric Encryption using Logistic Map. In Proceedings of the 1st International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 15–17 March 2012; pp. 1–5.
37. Assad, S.E. Chaos Based Information Hiding and Security. In Proceedings of the 7th International Conference for Internet Technology and Secured Transactions, London, UK, 10–12 December 2012; pp. 67–72.

38. Sheng, S.; Wu, X. A New Digital Anti-counterfeiting Scheme Based on Chaotic Cryptography. International Conference on ICT Convergence (ICTC), Jeju City, Korea, 15–17 October 2012; pp. 687–691.
39. Kartalopoulos, S.V. Chaotic Quantum Cryptography: The Ultimate for Network Security. In Proceedings of the International Conference on e-Business (ICE-B), Athens, Greece, 26–28 July 2010; pp. 1–16.
40. Yuan, W.X.; Qing, Y. A block encryption algorithm based on dynamic sequences of multiple chaotic systems. *Comm. Nonlinear. Sci. Numer. Simulat.* **2009**, *14*, 574–581.
41. Xiao, Y.P.; Han, Y. An Encrypt Approach Using Dynamic Encrypt Keys. In Proceedings of the 6th International Conference on Machine Learning and Cybernetics, Hong Kong, China, 19–22 August 2007; pp. 3273–3277.
42. Zhang, Z.; Liu, K.; Niu, X.; Bai, X. The Research of Hardware Encryption Card Based on Chaos. In Proceedings of the International Conference on Sensor Network security Technology and Privacy Communication System (SNS & PCS), Taipei, Taiwan, 18–19 May 2013; pp. 116–119.
43. Orue, A.B.; Fernandez, V.; Alvareza, G.; Pastor, G.; Shujun Lib, M.; Montoya, F. Determination of the Parameters for a Lorenz System and Application to Break the Security of Two-channel Chaotic Cryptosystems. *Phys. Lett.* **2008**, *372*, 5588–5592.
44. Elshamy, A.M.; Rashed, A.N.Z.; Mohamed, A.E.A.; Faragalla, O.S.; Mu, Y.; Alshebeili, S.A.; El-Samie, F.E.A. Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding. *J. Lightwave Tech.* **2013**, *31*, 2533–2539.
45. Agrawal, B.; Agrawal, H. Survey Report on Chaos Based Cryptography. *Int. J. Appl. Sci. Eng. Tech.* **2012**, *2*, 1–19.
46. Aimone, B.; Larson, S. Chaotic Circuits and Encryption. Available online: http://edrf.ucsd.edu/neurophysics/courses/physics_173_273/AimoneLarsonChaos.pdf (accessed on 17 March 2015).
47. Wang, C.; Ge, S.S. Adaptive synchronization of uncertain chaotic systems via backstepping design. *Chaos Solitons Fractals* **2001**, *12*, 1199–1206.
48. Peng, F.; Zhu, X.W.; Long, M. An ROI Privacy Protection Scheme for H.264 Video Based on FMO and Chaos. *IEEE Trans. Inf. Foren. Sec.* **2013**, *8*, 1688–1699.
49. Alvarez, G.; Montoya, F.; Romera, M.; Pastor, G. Cryptanalysis of a Chaotic Encryption System. *Phyc. Lett.* **2000**, *276*, 191–196.
50. Alvarez, G.; Li, S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *Int. J. Bifurcat. Chaos Appl. Sci. Eng.* **2006**, *16*, 2129–2151.
51. Kelber, K.; Schwarz, W. General Design Rules for Chaos-Based Encryption Systems. In Proceedings of the International Symposium on Nonlinear Theory and its Applications NOLTA, Bruges, Belgium, 18–21 October 2005; pp. 465–468.
52. Sheu, L.J.; Chen, W.C.; Chen, Y.C.; Weng, W.T. A Two-Channel Secure Communication Using Fractional Chaotic Systems. *Proc. World Acad. Sci. Eng. Tech.* **2010**, *41*, 1057–1061.
53. Azzaz, M.S.; Tanougast, C.; Sadoudi, S.; Dandache, A. New Hardware Cryptosystem Based Chaos for the Secure Real-Time of Embedded Applications. In Proceedings of the IEEE Workshop on Signal Processing System SIPS, Beirut, Lebanon, 4–7 October 2011; pp. 251–254.
54. Beltran, R.H. Low-complexity chaotic encryption system. *Revista Mexicana De Fisica* **2007**, *53*, 58–65.

55. Li, S.; Mou, X.; Cai,Y. Improving Security of a Chaotic Encryption Approach. *Phys. Lett.* **2001**, *290*, 127–133.
56. Li, S.; Alvarez, G.; Li, Z.; Halang, W.A. Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey. In Proceedings of 3rd International IEEE Scientific Conference on Physics and Control (PhysCon' 2007), Potsdam, Germany, 3–7 September 2007; pp. 1–6.
57. Hong, S.C.; Kuo, C.H.; Chen, H.K.; Chen, C.H. A Chaos based Multiple Security Encryption system for Compressed Video. *Int. J. Innov. Comput. Inf. Control.* **2011**, *7*, 4635–4652.
58. Vaidyanathan, S. Complete Synchronization of Hyperchaotic Xu and Hyperchaotic Lu Systems via Active Control. *Int. J. Comput. Sci. Eng. Survey* **2012**, *3*, 1–15.
59. Yang, T. A Survey of Chaotic Secure Communication Systems. *Int. J. Comput. Cognit.* **2004**, *2*, 81–130.
60. Lozi, R.; Chua, L.O. Secure Communications via Chaotic Synchronization II: Noise Reduction by Cascading Two Identical Receivers. *Int. J. Bifurcat. Chaos Appl. Sci. Eng.* **1993**, *3*, 1319–1325.
61. Wu, Z.G.; Shi, P. Su, H.; Chu, J. Sampled-Data Synchronization of Chaotic Lur'e Systems with Time Delays. *IEEE Trans. Neural Netw. Learn. Syst.* **2013**, *24*, 410–421.
62. Li, Z.; Li, K.; Wen, C.; Soh, Y.C. A New Chaotic Secure Communication System. *IEEE Trans. Commun.* **2003**, *51*, 1306–1312.