International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:9, No:3, 2015

Real-Time Image Encryption Using a 3D Discrete Dual Chaotic Cipher

M. F. Haroun, T. A. Gulliver

Abstract**—**In this paper, an encryption algorithm is proposed for real-time image encryption. The scheme employs a dual chaotic generator based on a three dimensional (3D) discrete Lorenz attractor. Encryption is achieved using non-autonomous modulation where the data is injected into the dynamics of the master chaotic generator. The second generator is used to permute the dynamics of the master generator using the same approach. Since the data stream can be regarded as a random source, the resulting permutations of the generator dynamics greatly increase the security of the transmitted signal. In addition, a technique is proposed to mitigate the error propagation due to the finite precision arithmetic of digital hardware. In particular, truncation and rounding errors are eliminated by employing an integer representation of the data which can easily be implemented. The simple hardware architecture of the algorithm makes it suitable for secure real-time applications.

Keywords**—**Chaotic systems, image encryption, 3D Lorenz attractor, non-autonomous modulation, FPGA.

I. Introduction

CHAOTIC systems have properties which have been extensively studied due to their complex behavior. They derive their inherent complexity from the extreme sensitivity of the system to the initial conditions. This characteristic and others such as ergodicity and random like behavior, are connected with conventional cryptographic properties such as confusion and diffusion [1].

In 1991, chaotic systems were shown to be controllable using master/slave synchronization [2]. In this case, the received signal is used as a driving state variable at the receiver, with the condition that the driven subsystem has negative Lyapunov exponents for all remaining state variables. The popularity of this approach comes from its simplicity. Subsequently, a wide variety of approaches have been proposed to achieve synchronization between the transmitter and receiver of chaotic communication systems. Continuous cryptographic systems have been developed which use the synchronization between the transmitter and receiver to retrieve data transmitted through an insecure medium. These include the first generation masking [3] and switching [4] techniques, and the second generation parameter and non-autonomous modulation techniques [5]-[7]. With chaotic masking, an analog message is added to the output of the chaotic generator at the transmitter. At the receiver, the chaotic signal is subtracted to recover the message. Several attacks on this cryptosystem have been developed [8]. Chaotic switching is a digital transmission technique and includes chaos shift keying (CSK), chaos on-off keying (COOK), differential chaos shift keying (DCSK), and FM-differential chaos shift keying (FM-DCSK). With this approach, the message data is used to select the signal to be transmitted from two or more chaotic attractors. At the receiver, the received signal is used to drive chaotic systems identical to those at the transmitter. The system that becomes synchronized with this signal determines the transmitted symbol. Successful attacks on this technique have been developed [9].

Chaotic modulation is considered to be the second generation of chaotic cryptosystems. Two methods have been proposed to modulate the data. The first is chaotic parameter modulation and uses the data to modulate one or more parameters of the chaotic attractor [10]. The second method is chaotic non-autonomous modulation. In this case, the data is injected into the dynamics of the chaotic attractor. Techniques developed to break chaotic parameter modulation include the return map [11], and adaptive observer [12]. While non-autonomous modulation is considered to be more secure than parameter modulation, for the Lorenz attractor return map and geometry attacks have been developed under the assumption that the data signal is sinusoidal and synchronization is done at the receiver [13]-[15].

Third generation techniques have been developed to provide a much higher level of security than the previous approaches. They can be implemented using dual chaotic systems which consist of a combination of two chaotic generators, or classical cryptographic techniques in conjunction with a high dimensional chaotic attractor [16]. Digital chaotic cryptosystems have also been developed which use chaotic maps directly to provide security rather than employing chaotic synchronization for this purpose [17]-[20].

In theory, chaotic systems used in communications applications are infinite precision systems. However, in practice they must be implemented using digital hardware with finite precision arithmetic, so that all computations are subject to truncation or rounding. The resulting degradation in the system means that the attractor orbits must eventually be periodic [21]. Refer to [22], the authors proposed three solutions to this problem. These solutions employ random perturbations with the digital chaotic systems to increase the orbits of the dynamic systems. This enhances the randomness and thus also the security.

The use of finite precision arithmetic also introduces noise due to truncation and rounding. This noise affects the dynamics

M. F. Haroun and T. A. Gulliver are with the Electrical and Computer Engineering Department, University of Victoria, Victoria BC, Canada (e-mail: mharoun@uvic.ca, agullive@ece.uvic.ca).

of the chaotic attractor and grows exponentially, quickly leading to a significant variation from the original orbit. Because of these issues, most chaotic encryption systems employ chaos based pseudo random number generators (PRNGs) to encrypt the data, thus avoiding the error between the transmitter and the receiver. These numbers can be generated using either floating point or integer arithmetic. The initial conditions and control parameters play the role of the secret key. One dimensional chaotic systems are simple and efficient [23], and thus the Logistic map has been widely used [24], [25], but they suffer from a small key space and weak security [26]-[28].

In this paper, a discrete dual chaotic cryptographic system which consists of two discrete chaotic generators is proposed. Previously, dual chaotic cryptographic systems were developed with one generator used to drive the other and synchronize the receiver to retrieve the data. Conversely, the proposed approach uses one (permutation) generator to permute the other (master) generator to increase the key length, orbit length, and conserve the randomness. At the receiver, the master generator cannot achieve synchronization with the transmitter without the permutation signal from the permutation generator. This prevents an eavesdropper from synchronizing their receiver using the transmitted signal only. In addition, the data is encrypted using non-autonomous modulation as in the continuous chaotic systems [6], [7]. With this technique, the data is injected into the dynamics of the master generator. Since the data to be encrypted appears as a random source, it results in a random permutation of the dynamics of the master generator. This random permutation increases the length of the orbit, which enhances the security of the cryptosystem. Further, the method suggested in [22] is used to eliminate the degradation due to the use of finite precision arithmetic. The simplicity of the algorithm hardware implementation will be shown using FPGA technology which is widely employed in real-time applications. The speed of the proposed approach makes it very suitable for use in secure real time systems, particularly real-time image encryption applications which require high data rates.

The rest of the paper organized as follows. The proposed dual chaotic cryptographic system is introduced in Section II. The chaotic properties of this system are examined in Section III, and Section IV presents a security analysis of the system. An FPGA hardware implementation is given in Section V which shows the practicality of this approach to encrypting and decrypting data. Finally, Section VI presents some conclusions.

II. The Proposed Lorenz Dual Chaotic System

The state variables of the continuous Lorenz attractor are described by the following differential equations:

$$\begin{aligned} \dot{u} &= A(v-u) \\ \dot{v} &= Bu - v - 20uw \\ \dot{w} &= 5uv - Cw \end{aligned} \tag{1}$$

Instead of that, the proposed system consists of two 3D chaotic generators based on the discrete Lorenz attractor, this is because a discrete attractor provides greater signal complexity and can be implemented simply in hardware [29]. A master generator is used to transmit the encrypted signal, while the permutation generator is used to permute the master generator dynamics. This permutation enhances the security of the system. The state equations of the discrete Lorenz generator are:

$$\begin{aligned} U_{n+1} &= \Delta t\big(A(V_n - U_n)\big) + U_n \\ V_{n+1} &= \Delta t(BU_n - V_n - 20U_nW_n) + V_n \\ W_{n+1} &= \Delta t(5U_nV_n - CW_n) + W_n \end{aligned} \tag{2}$$

where A, B and C are constants, which differ for the master and permutation generators. The data is encrypted using non-autonomous modulation via insertion into a state equation of the master generator, while the permutation signal is injected into another state equation of this generator.

The state equations of the master generator at the transmitter are:

$$\begin{aligned} U_{n+1} &= \Delta t(A(V_n - U_n) + m_n) + U_n \\ V_{n+1} &= \Delta t(\mathrm{BU_n - V_n - 20U_nW_n + p_n}) + \mathrm{V_n} \\ W_{n+1} &= \Delta t(5U_nV_n - CW_n) + W_n \end{aligned} \tag{3}$$

where m_n represents the data and p_n represents the permutation signal which can be one of the state variables of the permutation generator as defined in (2). State variable U is used as the transmitted signal.

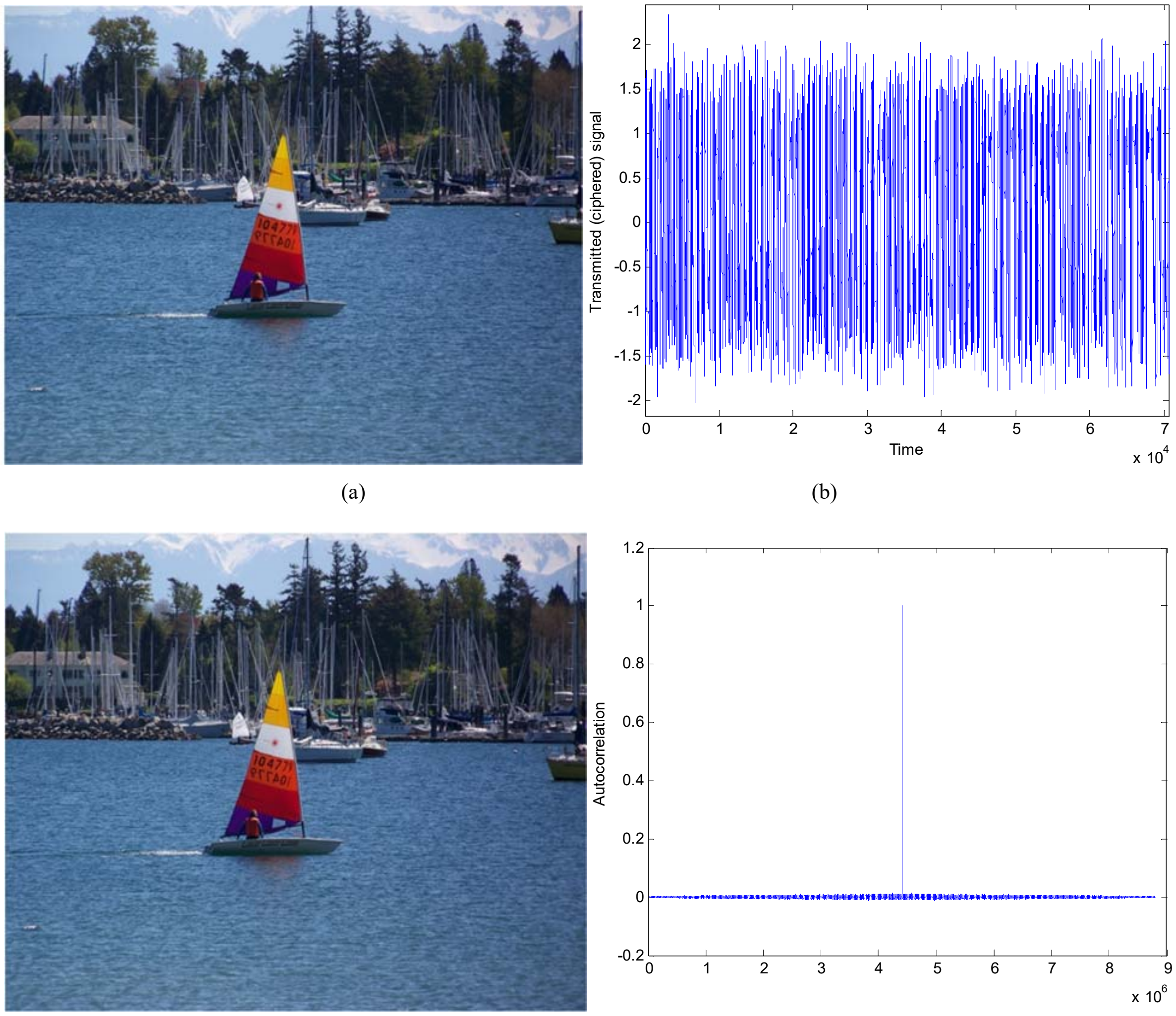
At the receiver, the received signal is used with the signal generated by the permutation generator at the receiver to synchronize the master generator, and hence retrieve the data. Since the U state is transmitted, the receiver uses this received state variable to update its own difference equations, and hence the retrieved data is given by:

$$\tilde{m}_n = round[\tfrac{1}{\Delta t}(U_{n+1} - U_n) - A(\tilde{V}_n - U_n)] \tag{4}$$

where *round* denotes rounding to the nearest integer. This is used to eliminate the noise due to finite precision arithmetic in the digital hardware. Since the data to be encrypted is digital (e.g. image, text or audio files), it is transmitted in blocks of bits (bytes or words). These blocks are represented as integers, and then scaled to floating point numbers. Scaling of the resulting values is used to preserve the chaotic behavior of the system [4]. These values are injected into the dynamics of the master generator to obtain the chaotic cipher signal. At the receiver, the real values are rounded to the nearest integers using (4), and these values are reused as m_n in (3) to update the receiver state variables. This removes the noise and thus prevents these errors from propagating through the system dynamics.

III. Chaotic Properties of the Proposed System

The proposed system was simulated using MATLAB with double precision floating point. The constants for the master generator are A= 10, B= 28, C= 8/3 and Δt= 0.024, while the constants for the permutation generator are A= 9.8, B= 27, C= 2.8 and Δt = 0.024. The state variable V of the permutation generator is used as the permutation signal p_n. An image file of size 4,405,713 bytes (3072 × 2304 pixels), was used to investigate the system properties. This size was chosen to test the practicality of the proposed encryption algorithm to overcome the noise due to finite precision arithmetic. The data integers m_n are scaled by a factor of 0.00001 to preserve the chaotic behavior, while the permutation values p_n are scaled by a factor of 0.01 to blur the return map. Fig. 1 shows the original image, the transmitted signal, and the recovered image.



(a) (b)

(c) (d)

Fig. 1 An example of image file encryption: (a) the original image, (b) the transmitted signal, (c) the autocorrelation of the transmitted signal, and (d) the recovered image

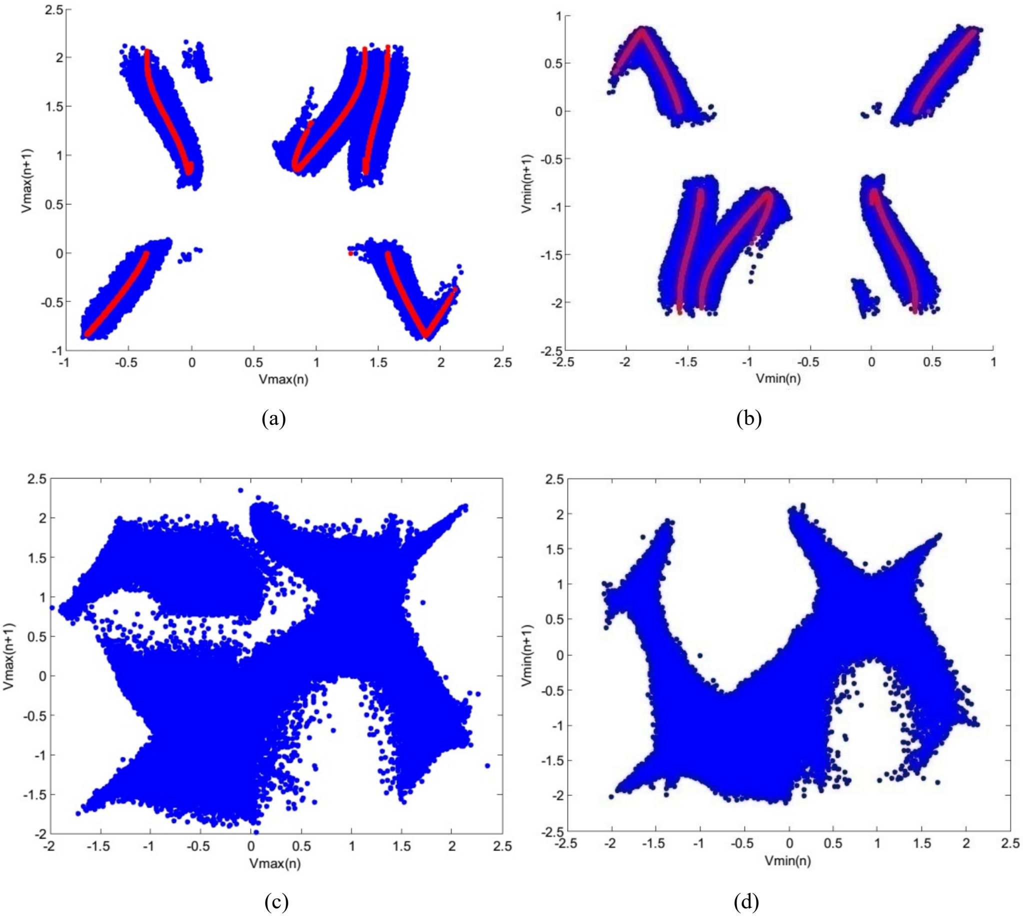
IV. Security Analysis

Although the chaotic behavior of the continuous Lorenz attractor is very complex, there have been numerous attempts to break ciphers based on this attractor [30]-[33]. All of these approaches are based on the system synchronization for the continuous Lorenz system. The attacker uses the transmitted signal as the driving signal to synchronize their receiver to obtain the Lorenz attractor parameters. However, these methods cannot be used against the proposed system because the driven subsystem is non-autonomous with an external signal from the permutation generator injected into the second state equation.

Fig. 2 shows the return map of the proposed algorithm. In Fig. 2 (a), the red dots represent the return map of the Lorenz attractor [30], and the blue dots represent the return map using the dual chaotic system without the data signal injected. This indicates that the return map of the proposed system is blurred by the signal from the permutation generator. Fig. 2 (b) shows the effect of the injected data on the return map. Clearly the data signal increases the blurriness of the return map, which is desirable.

The importance of a blurry return map is that it prevents an attacker from extracting any useful information about the generator control parameters, and hence breaking the algorithm

[30]. The return map of the proposed algorithm is blurred using two random signals, namely the permutation signal and the data signal. This is much stronger than using a periodic signal to blur the return map as in [31], which was broken by [14].



(a) (b)

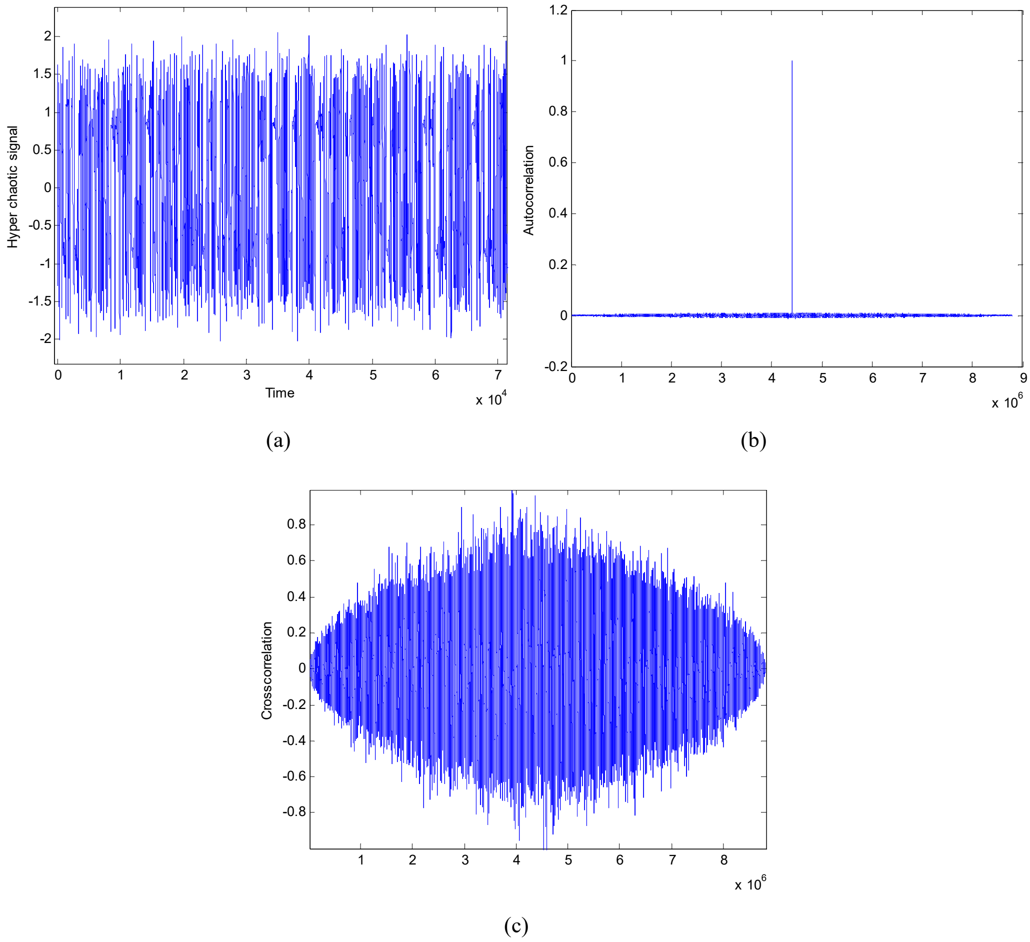
(c) (d)

Fig. 2 The return map of the proposed dual chaotic cryptosystem based on the Lorenz attractor: (a) and (b) without a data signal, (c) and (d) with a data signal

A. Attacks on the System

A known plaintext attack, a chosen plaintext attack, and a chosen ciphertext attack, the goal of these attacks is to obtain information about the secret key. When the encryption algorithm is based on non-autonomous modulation, the complex dynamics of the chaotic cipher are modified by the data being encrypted, and the second generator. Thus, the permutation and diffusion in the chaotic system are directly affected by external forces. In addition, this modulation is done over two of the three state equations of the discrete Lorenz generator. At the receiver, the decrypted plaintext values are used to update the chaotic generator. Thus, the generator dynamics are related to: the plaintext being encrypted, the permuting chaotic signal, and the ciphertext being decrypted. Therefore, without knowledge of the particular plaintext being encrypted and the permuting chaotic signal, an attacker will not be able to reproduce the particular system dynamics, so the proposed algorithm is resistant to these attacks.

One situation that should be considered is when the attacker has access to the encryption system and can encrypt null message. In this case the transmitted signal will reflect the dynamics of the chaotic generator without any variations due to the data, but still permuted due to the second generator. The attacker still cannot perform a geometric attack on the Lorenz generator, as in [13]-[15], [30]-[33]. In addition, these attacks will not work because the discrete Lorenz generator used in the proposed technique has an additional parameter Δt which appears in all three difference equations. Since each Δt can be assigned a different value, they represent three additional key parameters beyond those of the differential equations of the continuous Lorenz generator, and so provide an additional level of security. This greatly decreases the probability of a geometric attack on the proposed cipher being successful as will be shown later when attacks on the Lorenz generator are considered.



(a)

(b)

(c)

Fig. 3 The encrypted signals and their correlations using the proposed dual chaotic encryption system: (a) transmitted signal, (b) its autocorrelation without an injected data signal, (c) cross-correlation of the transmitted signals with and without an injected data signal

B. Key Space Analysis and Brute-Force Attack

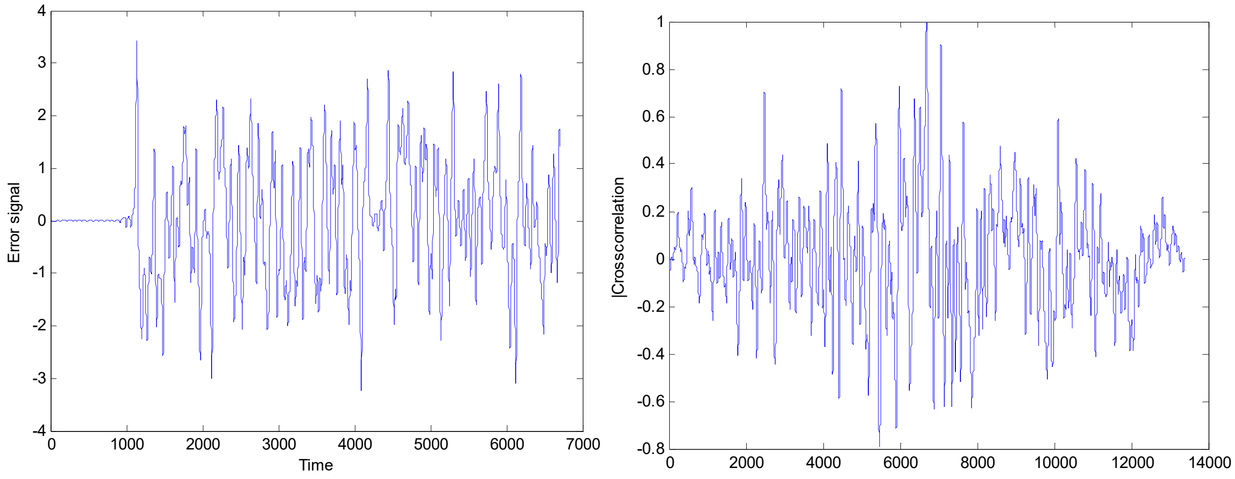
At present, a key length of 2^{100} is sufficient to protect an algorithm against a brute-force attack [34]. Table I shows the sensitivity of each control parameter of the discrete Lorenz attractors for both the master and the permutation generators using double precision floating point. This sensitivity is the value below which the dynamics of the generators at the transmitter and receiver converge. Conversely, the dynamics differ for larger parameter differences. The product of the sensitivities (or equivalently the sum of their digits), gives the key length for the algorithm. This gives a key-length of 60 decimal digits, and $10^{60} > 2^{100}$. Note that this does not include the initial values of the master generator. This is because synchronization of this generator can be achieved even if the initial values are not known exactly. On the other hand, the initial values of the permutation generator are very important since the output is used to permute the master generator. This greatly increases the robustness against a brute force attack, as indicated in Table I.

C. Statistical Analysis

The transmitted chaotic signal U of the master generator was subjected to a statistical analysis in an attempt to obtain information about the dynamics of the chaotic system. Fig. 1 (b) and 1 (c) show the transmitted signal in time and the autocorrelation of this signal, respectively. The nearly flat autocorrelation illustrates the randomness of the transmitted signal, and thus the difficulty in exploiting it via correlation techniques. Further, Fig. 3 shows the low correlation between the transmitted signal with and without the injected data signal.

D. Differential Analysis

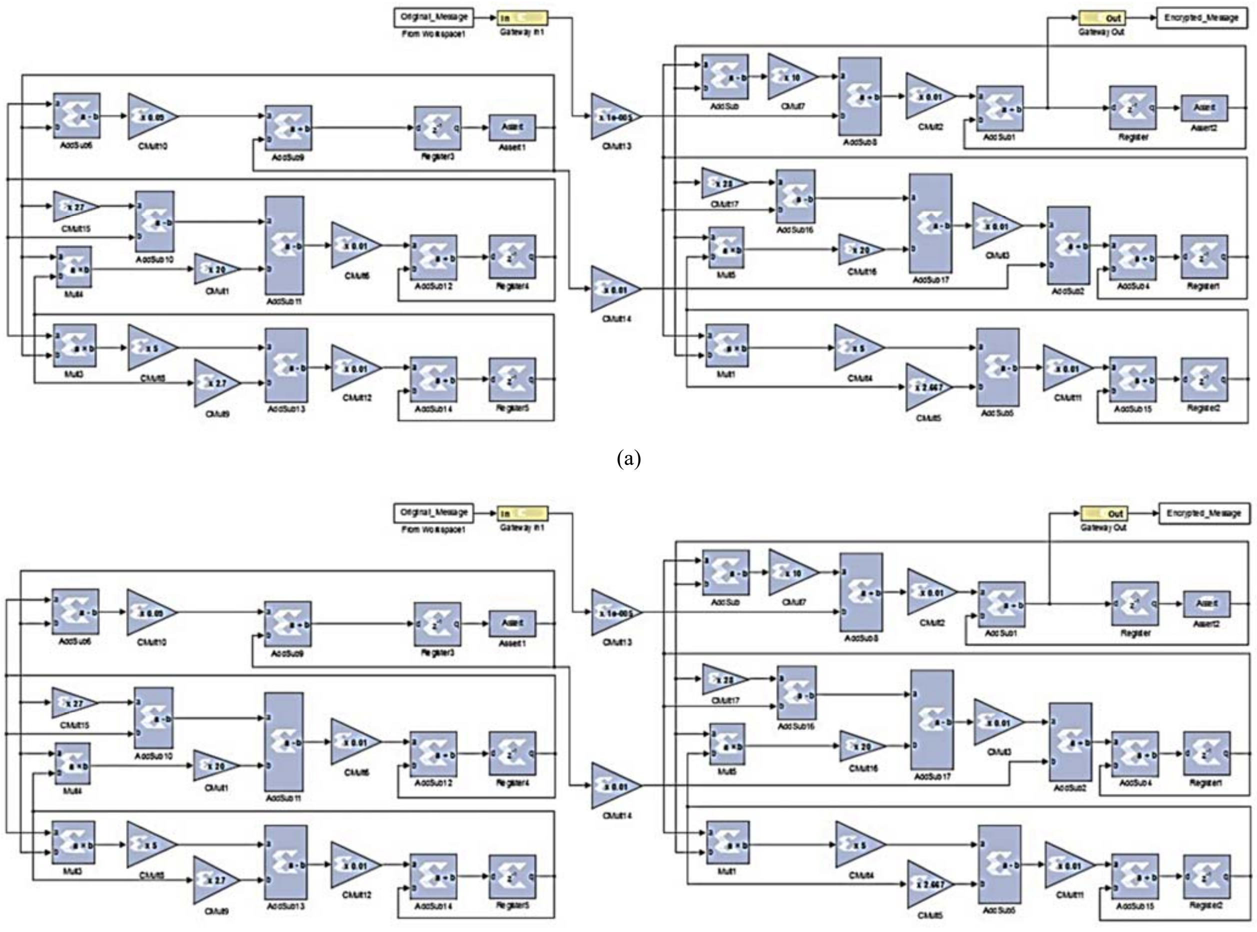
In a differential attack, the cryptanalyst is assumed to have the capability of modifying individual values of the plaintext (data) and observing the resulting encrypted signal. If such a change results in a significant change in this signal, then the attack is considered to be inefficient and impractical. The proposed algorithm was used to encrypt an image as shown in Fig. 1, and the file with the first byte changed. Figs. 4 (a) and 4 (b) show the difference between the two transmitted signals in time, and their cross-correlation, respectively.



(a)

(b)

Fig. 4 (a) the difference between two encrypted signals in time, and (b) the cross-correlation of the two transmitted signals



(a)

(b)

Fig. 5 Xilinx blocks integrated with MATLAB for hardware implementation: (a) transmitter implementation, (b) receiver implementation

E. Encryption Time Performance

The time to execute an encryption algorithm is an important factor in many applications. The time required for the proposed algorithm is compared in Table II with several algorithms in the literature. The proposed algorithm is faster than the other 3D chaotic systems and AES, and has an acceptable speed compared with 1D and 2D systems. While 1D chaotic systems are very fast, they suffer from low security compared to higher dimensional chaotic systems.

TABLE I
THE KEY LENGTH BASED ON THE MASTER AND PERMUTATION GENERATOR PARAMETERS

Master generator parameter	Sensitivity	Number of digits	Permutation generator parameter	Sensitivity	Number of digits
Initial values			Initial values		
U_0	-	-	U_0	10^{-4}	4
V_0	-	-	V_0	10^{-4}	4
W_0	-	-	W_0	10^{-4}	4
Lorenz parameters			Lorenz parameters		
A	10^{-3}	3	A	10^{-4}	4
B	10^{-3}	3	B	10^{-4}	4
C	10^{-3}	3	C	10^{-4}	4
Δt parameter for			Δt parameter for		
U	10^{-4}	4	U	10^{-5}	5
V	10^{-4}	4	V	10^{-5}	5
W	10^{-4}	4	W	10^{-5}	5
Combination	10^{-21}	21		10^{-39}	39

TABLE II
ENCRYPTION/DECRYPTION EXECUTION TIMES FOR SEVERAL ALGORITHMS

Algorithm	System characteristics	Dimension of the chaotic generator	Execution Time
[35]	Pentium IV 2.1 GHz	1D	74.4 Mbps
[36]	Dual core 2.7 GHz	1D	15.6 Mbps
[37]	Intel core 2 duo 2.1 GHz	2D	6.69 to 22.6 Mbps
[38]		2D	AES [128 key] 11.2 Mbps AES [192 key] 9.25 Mbps AES [256 key] 9.19 Mbps Algorithm in [38] 44.9 Mbps
[39]		3D	8 Mbps
[40]	Intel core i5 2.27 GHz	3D	15.4 Mbps
Proposed algorithm	Pentium (R) dual core 1.6GHz	3D	33.6 Mbps 27.7 Mbps

V. FPGA IMPLEMENTATION

The proposed encryption system was implemented using a Field Programmable Gate Array (FPGA). Using the Xilinx tool in MATLAB, the transmitter and the receiver blocks were constructed and are presented in Fig. 5. Fig. 5 (a) shows the permutation generator on the left of the transmitter block, and the master generator on the right. The data values (integers) are converted to floating point numbers and injected after scaling. At the receiver, the information is retrieved using (4). The floating point values are rounded to integers and then used to update the receiver master generator state variables as shown in Fig. 5 (b).

VI. CONCLUSION

In this paper, an encryption algorithm was proposed based on a dual chaotic system for secure real-time image applications. A three dimensional (3D) discrete Lorenz attractor is employed with non-autonomous modulation. The dynamics of the master chaotic generator are permuted by the data values and the output of a second (permutation) chaotic generator. This permutation prevents an eavesdropper from synchronizing their receiver with the encrypted signal since they have no information about the permutation signal from the second generator. The effects of using finite precision arithmetic were mitigated by using integers to represent the data values and rounding the received floating point values to integers. These integer values are used to update the state variables at the receiver, so that it can track the transmitter. Based on an evaluation and simulation of the system, it was shown that the security of the proposed scheme is excellent, and that the execution time is suitable for secure real-time applications.

REFERENCES

[1] G. Álvarez, S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. of Bifurcation and Chaos*, 2006;16, pp. 2129–2151.

[2] T. Carroll, L. Pecora, "Synchronizing chaotic circuits," *IEEE Trans Circuits Systems I*, 1991;38, pp. 453–456.

[3] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. of Bifurcation and Chaos*, 1992;2, pp. 709-713.

[4] H. Dedieu, M.P. Kennedy, M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans Circuits Systems II: Analog Digital Signal Process*, 1993;40, pp. 634-642.

[5] T. Yang, L. Chua, "Secure communication via chaotic parameter modulation," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1996;43, pp. 817-819.

[6] L. Kocarev, U. Parlitz, "General approach for chaotic synchronization with applications to communications," *Phys. Rev. Lett.*, 1995;74, pp. 5028-5031.

[7] M. Sobhy, A. Shehata, "Secure computer communication using chaotic algorithms," *Int. J. of Bifurcation and Chaos*, 2000;10, pp. 2831-2839.

[8] G. Alvarez, S. Li, F. Montoya, G. Pastor, M. Romera, "Breaking projective chaos synchronization secure communication using filtering

and generalized synchronization," *Chaos, Solitons and Fractals*, 2005;24, pp. 775–783.

[9] T. Yang, L. Yang, C. Yang, "Breaking chaotic switching using generalized synchronization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 1998;45, pp. 1062–1067.

[10] Y. Zhang, Y. Wang, "A Parameter Modulation Chaotic Secure Communication Scheme with Channel Noises," *Chinese Physics Letters*, 2011;28, pp. 020505.

[11] S. Li, G. Chen, G. Alvarez, "Return-map cryptanalysis revisited," *Int. J. of Bifurcation and Chaos*, 2006;16, pp. 1157–1168.

[12] G. Alvarez, F. Montoya, M. Romera, G. Pastor, "Breaking parameter modulated chaotic secure communication system," *Chaos, Solitons and Fractals*, 2004;21, pp. 783–787.

[13] K. Short, "Unmasking a modulated chaotic communications scheme," *Int. J. of Bifurcation and Chaos*, 1996;06, pp. 367.

[14] S. Li, G. Álvarez, G. Chen, "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos, Solitons and Fractals*, 2005;25, pp. 109–120.

[15] A. Orue, V. Fernandez, G. Alvarez, G. Pastor, M. Romera, S. Li, F. Montoya, "Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems," *Physical Letters A*, 2008;372, pp. 5588–5592.

[16] T. Yang, C. Wu, L. Chua, "Cryptography based on chaotic systems," *IEEE Transaction on Circuits and Systems—I: fundamental theory and applications*, 1997;44, pp. 469-472.

[17] Y. Zhang, Di. Xiao, H. Liu, H. Nan, "GLS coding based security solution to JPEG with the structure of aggregated compression and encryption," *Communications in Nonlinear Science and Numerical Simulation*, 2013;19, pp. 1366.

[18] Y. Zhang and Y. Wang, "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation," *Nonlinear Dynamics*, 2014;77, pp. 687-698.

[19] Y. Zhang, Di. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, 2014;19, pp. 74.

[20] Y. Zhang, Di. Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption," *International Journal of Electronics and Communications*, 2014;68, pp. 361-368.

[21] N. Masuda, K. Aihara, "Dynamical characteristics of discretized chaotic permutations," *Int. J. of Bifurcation and Chaos*, 2002;12, pp. 2087-2103.

[22] S. LI, G. CHEN, X. MOU, "On the dynamical degradation of digital piecewise linear chaotic maps," *Tutorial-Review Section of Int. J. of Bifurcation and Chaos*, 2005;15, pp. 119-151.

[23] D. Socek, S. Li, S. Magliveras, B. Furht, "Enhanced 1-D chaotic key-based algorithm for image encryption," *In: Proceedings of the first international conference on security and privacy for emerging areas in communications networks* (SECURECOMM'05), 2005, pp. 406–407.

[24] H. Gao, Y. Zhang, S. Liang, D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, 2006;29, pp. 393–9.

[25] N. Pareek, V. Patidar, K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, 2006;24, pp. 926–934.

[26] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, "On the security defects of an image encryption scheme," *Image and Vision Computing*, 2009;27, pp. 1371-1381.

[27] C. Li, S. Li, G. Alvarez, G. Chen, K. Lo, "Cryptanalysis of a chaotic block cipher with external key and its improved version," *Chaos, Solitons & Fractals*, 2008;37, pp. 299–307.

[28] D. Arroyo, R. Rhouma R, G. Alvarez, S. Li, V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2008;18, pp. 033112.

[29] M.F. Haroun and T.A. Gulliver, "New Low Complexity Discrete 3D Chaotic Generators for Communication and Security Applications," *IET information security Journal*, submitted.

[30] T. Yang, L. Yang, C. Yang, "Cryptanalyzing chaotic secure communications using return maps," *Physics Letters A*, 1998;245, pp. 495-510.

[31] X. Wu, H. Hu, B. Zhang, "Analyzing and improving a chaotic encryption method," *Chaos, Solitons and Fractals*, 2004;22, pp. 367–373.

[32] A. Orue, G. Alvarez, G. Pastor, M. Romera, F. Montoya, S. Li, "A new parameter determination method for some double-scroll chaotic systems and its applications to chaotic cryptanalysis," *Communications in Nonlinear Science and Numerical Simulation*, 2010;15, pp. 3471-3483.

[33] T. Stojanovski, L. Kocarev, U. Parlitz, "A simple method to reveal the parameters of the Lorenz system," *Int. J. of Bifurcation and Chaos*, 1996;6, pp. 2645–2652.

[34] B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C," 2nd ed. Wiley, New York, 1996.

[35] H. Liu, X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers and Mathematics with Applications*, 2010;59, pp. 3320–3327.

[36] A. abdel-latif, X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *Int. J. Electronics and Commun.*, 2013;67, pp. 136–143.

[37] V. Patidar, N. Pareek, G. Purohit, K. Sud, "A robust and secure Chaotic Standard Map-Based Pseudorandom Permutation-substitution Scheme for Image Encryption," *optics communications*, 2011;284, pp. 4331–4339.

[38] S. Sayedzadeh, S. Mirzakuchaki, "A fast color image encryption algorithm based on Coupled two dimensional Piecewise chaotic map," *Signal Processing*, 2012;92, pp. 1202–1215.

[39] G. Chen, Y. Mao, C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, 2004;21, pp. 749–761.

[40] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Comm. Nonlinear sci. Numer simulate*, 2012;17, pp. 2943-2959.