CHAOTIC SCRAMBLING FOR WIRELESS ANALOG VIDEO

Ned J. Corron*, Billy R. Reed, Jonathan N. Blakely, Krishna Myneni, and Shawn D. Pethel
U. S. Army RDECOM
AMSRD-AMR-WS-ST, Redstone Arsenal, AL 35898

ABSTRACT

We report the implementation of an in-band chaotic scrambler for securing wireless analog video. In this demonstration system, an analog video signal is injected into a chaotic oscillator and the output is transmitted through a standard wireless video link. At the receiver, a descrambler separates the video from the chaotic signal in real time. Experimental results show the scrambled signal effectively hides the original video image, yet the descrambler recovers the original color video with reasonable clarity and detail. Compared to digital encryption, chaotic scrambling offers an efficient, low-cost alternative for masking time-critical analog communications.

1. INTRODUCTION

The combination of digital video and modern encryption technologies virtually assures that the next generation of wireless video links will be secure. However, unsecured analog wireless video systems are still widely used in many existing systems. For many of these legacy systems, it may be impractical to upgrade to a secure digital link due to prohibitive cost and power requirements. Effectively, the signals in these systems will continue to be transmitted in the open, where they are easily detected and intercepted.

To deny casual eavesdropping, we have developed and demonstrated a low-cost, low-power analog video scrambler based on synchronized chaos. This in-band scrambler system is compatible with existing wireless video transmission links while meeting minimal cost and power requirements. Although this technology cannot provide the same security as digital encryption (Kocarev, 2001), chaotic scrambling provides an effective retrofit for time-critical communications in legacy systems where low-cost and low-power needs are critical (Myneni *et al.*, 2004).

2. CHAOTIC SCRAMBLING

As shown in Fig. 1, a chaotic scrambler is located between the video source and the radio transmitter in an analog video wireless link (Corron, 1997). The baseband video signal is injected into a chaotic oscillator that overlaps the spectral bandwidth of the video signal. As a result, the signal is nonlinearly mixed with the random, unpredictable chaotic oscillations, resulting in a noise-like scrambled output. Since the scrambled signal is contained within the video bandwidth, it can be transmitted via a standard analog video radio link. A descrambler is located just after the radio receiver and contains a second chaotic oscillator. If the descrambler is matched to the scrambler, the oscillators synchronize and the modulation process can be inverted, recovering the original video signal. Without synchronization, the chaotic signal cannot be easily deciphered and the original video waveform remains hidden.

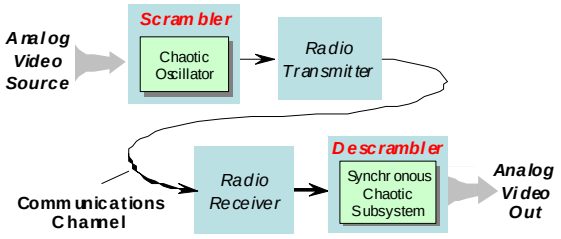

Fig. 1. Block diagram depicting a chaotic analog scrambling system.

Chaotic scrambling exploits the synchronization properties of coupled nonlinear oscillators (Pecora and Carroll, 1990). The video signal drives the first oscillator, which is located in the transmitter. A typical chaotic oscillator can be modeled by a third-order nonlinear system

$$\begin{aligned} \frac{dx}{dt} &= f(x,y,z) + s(t) \\ \frac{dy}{dt} &= g(x,y,z) \\ \frac{dz}{dt} &= h(x,y,z) \end{aligned} \tag{1}$$

where x, y, and z represent scrambler's dynamic states, $s(t)$ is the input video signal, and f, g, and h are functions defining a chaotic flow. The resulting oscillation is a complicated, nonlinear combination of the unpredictable chaos and the input video signal. The state $x(t)$ is the scrambled signal that is transmitted in place of the video waveform $s(t)$. To an eavesdropper, the transmitted signal looks nothing like the original video input.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Chaotic Scrambling For Wireless Analog Video	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U. S. Army RDECOM AMSRD-AMR-WS-ST, Redstone Arsenal, AL 35898**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002187. Proceedings of the Army Science Conference (26th) Held in Orlando, Florida on 1-4 December 2008, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**7**	

The second oscillator is located at the receiver and forms the descrambler. It is specifically chosen to match the first oscillator, and it is modeled as

$$\begin{aligned} \frac{dY}{dt} &= g(x, Y, Z) \\ \frac{dZ}{dt} &= h(x, Y, Z) \\ S(t) &= \frac{dx}{dt} - f(x, Y, Z) \end{aligned} \tag{2}$$

where Y and Z are the response states, and f, g, and h are the same functions as in the scrambler oscillator. The descrambler forms an inverse system for recovering the modulated signal (Feldmann *et al.*, 1996). The first two of these equations represent a synchronous subsystem, which reproduces the scrambler's states as $Y(t) \rightarrow y(t)$ and $Z(t) \rightarrow z(t)$. The last equation "inverts" the scrambling process, reconstructing the video signal with $S(t) \rightarrow s(t)$.

If the descrambler does not match the scrambler, the circuits will not synchronize and the video remains hidden. Thus, synchronization relies on the descrambler using exactly the same nonlinear functions f, g, and h as used in the scrambler, and the parameters of these functions constitute the security key. Without a matched descrambler, an adversary would likely have to resort to sophisticated and expensive digital signal processing in order to extract useful video information (Pérez and Cerdeira, 1995).

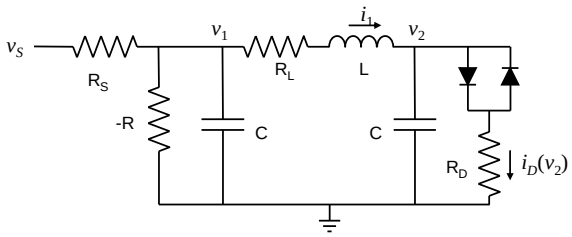

Fig. 2. Chaotic scrambler circuit with input video signal v_S and scrambled output v_1.

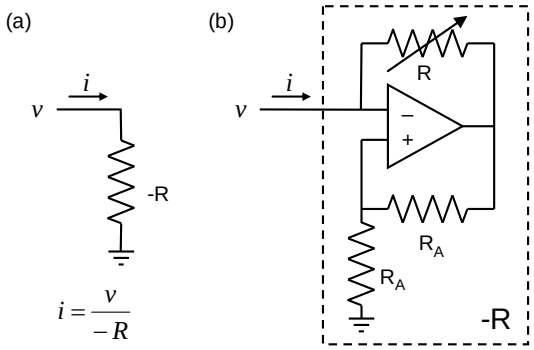

Fig. 3. Circuit representations showing (a) the current-voltage relationship and (b) a practical circuit realization for a negative resistor device.

3. CHAOTIC OSCILLATOR

Communication with chaos was first theoretically proposed in the early 1990s (Cuomo *et al.*, 1993). However, practical realizations of such systems for analog video has been hindered by a lack of suitable high-frequency chaotic oscillator circuits. Recently, we developed a new chaotic rf circuit that is suitable for scrambling video-rate and faster signals (Corron *et al.*, 2004, 2005). A variant of this oscillator is used in the video scrambler system.

A schematic of the oscillator design is shown in Fig. 2. This circuit consists of a number of standard linear components, as well as two diodes, which provide the nonlinearity essential for chaos. A negative resistor is the only active component. The circuit is modeled as

$$\begin{aligned} C\frac{dv_1}{dt} &= \frac{v_1}{R} - i_1 + \frac{v_S - v_1}{R_S} \\ L\frac{di_1}{dt} &= v_1 - v_2 - i_1 R_L \\ C\frac{dv_2}{dt} &= i_1 - i_D(v_2) \end{aligned} \tag{3}$$

where v_1 and v_2 are voltages and i_1 is a current. The diode current i_D is a nonlinear function of the voltage v_2, which can be modeled using the piecewise-linear approximation

$$i_D(v) = \begin{cases} \dfrac{v + V_D}{R_D} & v < -V_D \\ 0 & |v| \le V_D \\ \dfrac{v - V_D}{R_D} & v > V_D \end{cases} \tag{4}$$

where V_D is the switching voltage for an individual diode.

An important component in the circuit is the negative resistor. This active device provides gain to sustain the chaotic oscillations. For our implementations, we realize the negative resistor using a feedback amplifier circuit such as shown in Fig. 3. In this realization, the magnitude of the negative resistance is set directly by the variable resistor R.

For this model, typical values that yield chaotic dynamics are C = 1 nF, L = 22 μH, R_L = 25 Ω, R_S = 510 Ω, and R = 150 Ω. We use these as nominal values in designing our the scrambler system. For the diode model, we use V_D = 0.3 V and R_D = 40 Ω. A typical waveform

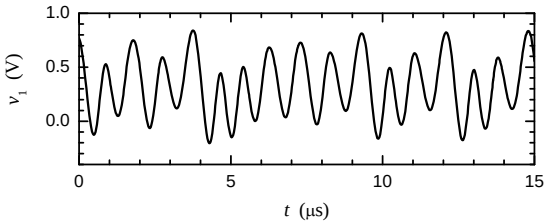

Fig. 4. Typical chaotic waveform $v_1(t)$ obtained from numerical simulation of the oscillator model with $v_S = 0$.

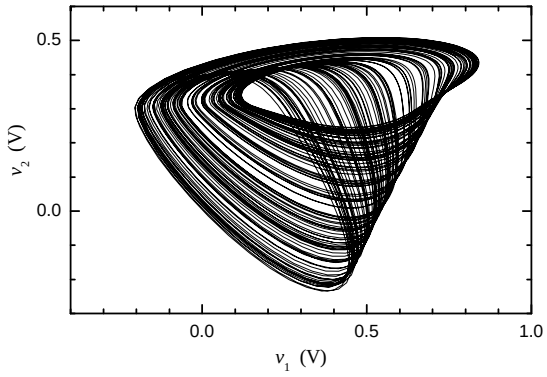

Fig. 5. Chaotic attractor projected in the v_1-v_2 plane obtained from numerical simulation of the oscillator model with $v_S = 0$.

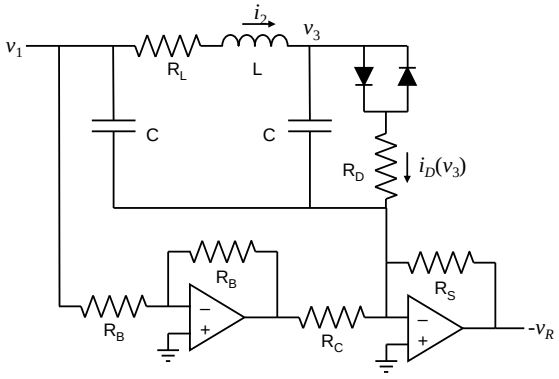

Fig. 6. Descrambler circuit with scrambled input v_1 and the recovered video output v_R.

obtained from numerical simulations with $v_S = 0$ is shown in Fig. 4. The waveform exhibits sinusoidal-like oscillations with cycle-to-cycle fluctuations in amplitude. The average peak-to-peak return time is 0.92 μs, corresponding to an average frequency of 1.1 MHz. A v_1-v_2 phase-space projection is shown in Fig. 5. For the nominal parameter values, the oscillator has two attractors

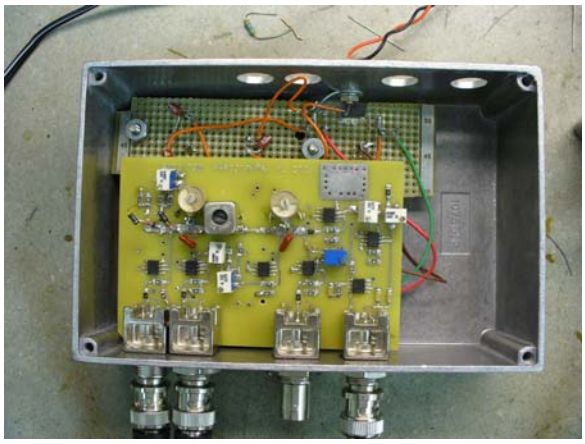

Fig. 7. Prototype chaotic scrambler circuit.

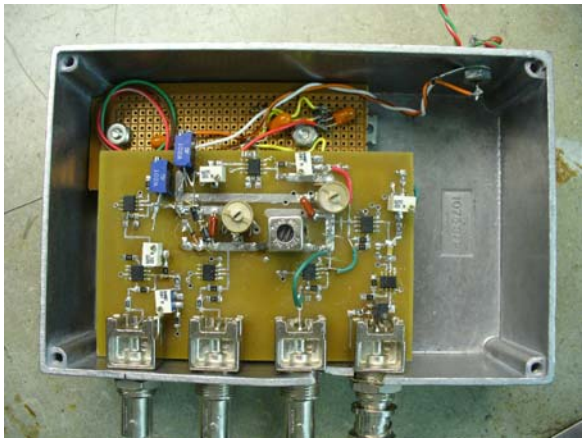

Fig. 8. Prototype chaotic descrambler circuit.

related by the symmetry $(v_1, i_1, v_2) \rightarrow (-v_1, -i_1, -v_2)$. Physically, each of these attractors corresponds to oscillations about an operating point for the symmetric diodes. The attractor observed in a simulation depends on the initial conditions used.

To operate as a scrambler, the oscillator is modulated by the input video signal v_S, with the strength of the modulation set by the coupling resistor R_S. The output of the scrambler is the voltage signal v_1. For $v_S \neq 0$, the coupling is such that the input modulation is only a small perturbation to the natural dynamics of the oscillator, and the chaotic character of the oscillator is retained. As a result, the scrambled output signal v_1 is a complicated, nonlinear combination of the unpredictable chaos and the input video signal.

The corresponding descrambler circuit is shown in Fig. 6. This circuit is designed to satisfy the inverse equations

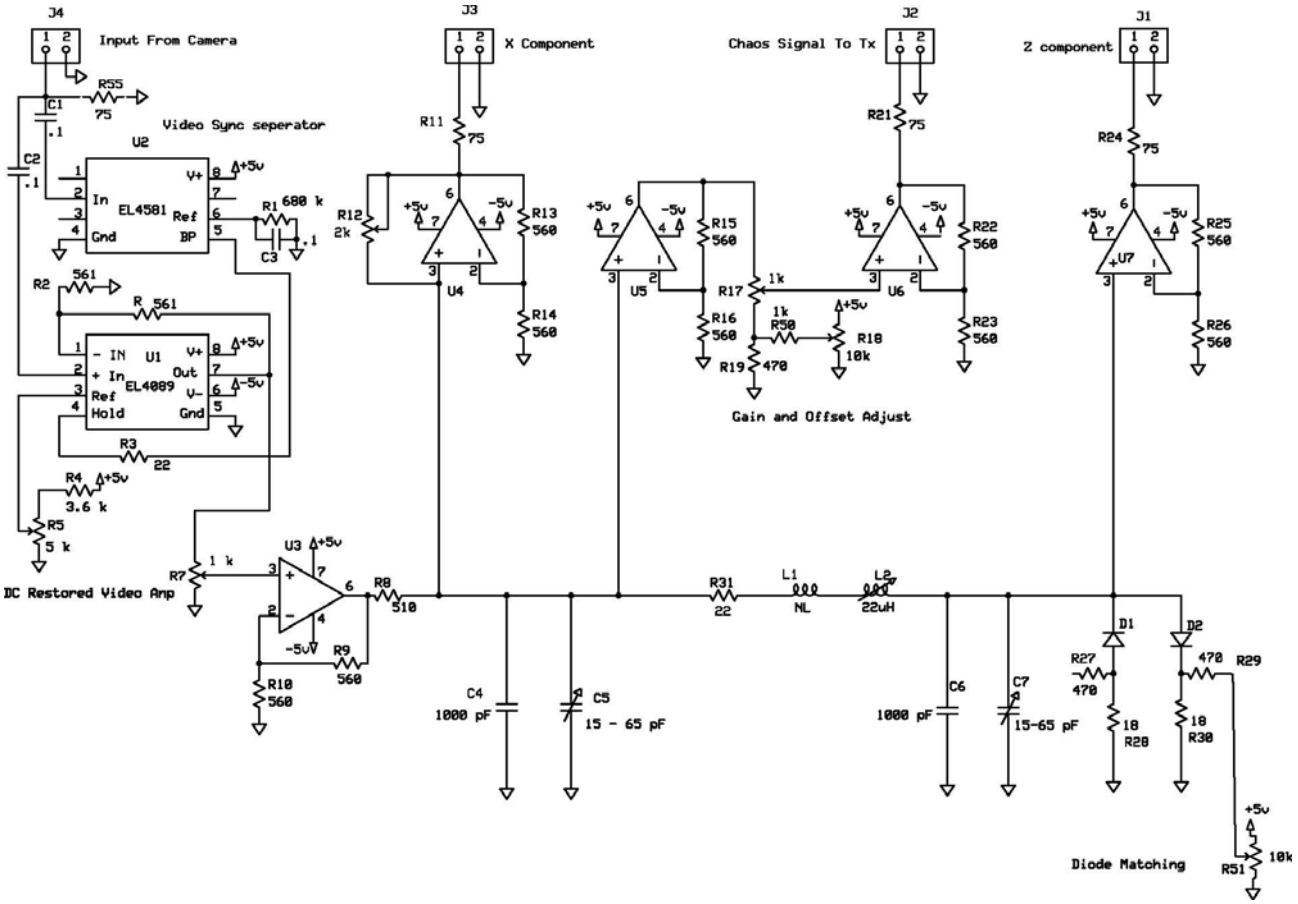

Fig. 9. Detailed schematic of prototype chaotic scrambler circuit.

$$L\frac{di_2}{dt} = v_1 - v_3 - i_2 R_L$$
$$C\frac{dv_3}{dt} = i_2 - i_D(v_3) \qquad (5)$$
$$v_R = R_S\left\{C\frac{dv_1}{dt} + \left(\frac{1}{R_S} - \frac{1}{R}\right)v_1 + i_2\right\}$$

where $v_R \to v_S$ is the recovered signal. In the inverse system, the first two equations form a synchronous subsystem that recreates the other states of the scrambler oscillator that are not transmitted. Specifically, the descrambler states asymptotically approach $i_2 \to i_1$ and $v_3 \to v_2$. The last equation inverts the unused scrambler equation and solves for the modulation. In the descrambler circuit, the design constraint

$$\frac{1}{R_C} = \frac{1}{R} - \frac{1}{R_S} \qquad (6)$$

is required to match the descrambler model. However, in practice the variable resistor R_C is simply adjusted for optimal signal recovery.

4. DEMONSTRATION SYSTEM

The chaotic video scrambler demonstration system was built using standard, commercially available components. As shown in Figs. 7 and 8, the scrambler and descrambler circuits are constructed on printed circuit boards with layouts designed for high-frequency operation. Surface mount and chip-packaged components are used to minimize parasitic reactance. The boards are mounted in metal boxes to provide mechanical and electrical shielding. Connections to the circuits are provided via coaxial feed-through connectors mounted on the boxes. Since the boxes are designed to work in the field using automotive 12-volt sources, separate voltage converter circuitry is included to provide the scrambler and descrambler with regulated ±8-V power supplies. In each box, this supply circuitry is mounted behind the scrambler and descrambler circuits on a separate breadboard, which is visible in each figure.

A detailed schematic for the chaotic scrambler is shown in Fig. 9. Component values were selected to yield chaotic oscillations with a broad spectrum that overlaps the 4.5 MHz bandwidth of baseband NTSC video signals.

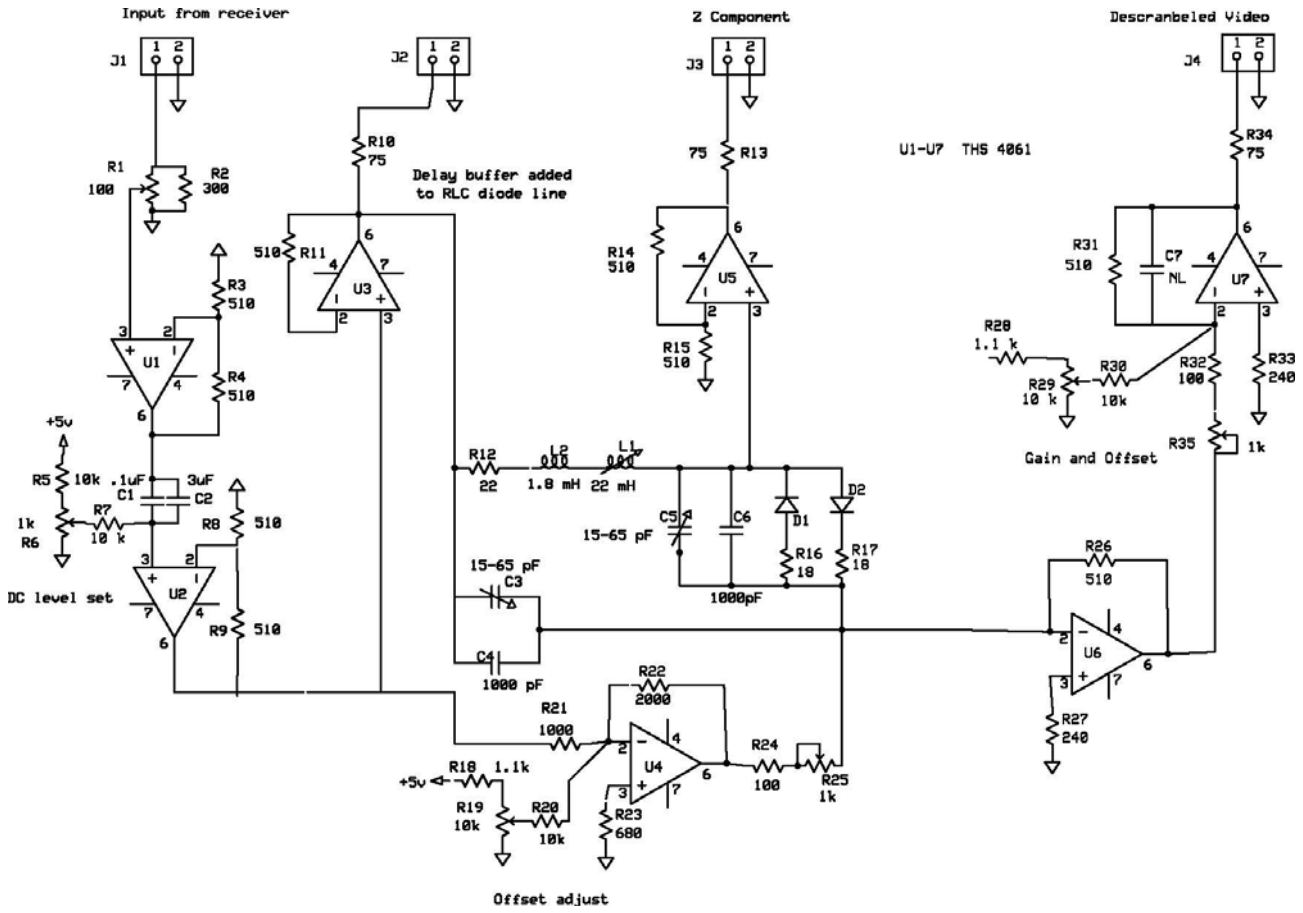

Fig. 10. Detailed schematic of prototype chaotic descrambler circuit.

The analog video enters the scrambler via connector J4. Special purpose integrated video circuits U1 and U2 with trimmer R5 are used to shift the signal to positive voltage, and trimmer R7 is used to scale the amplitude of the input modulation for the chaotic oscillator. Variable capacitors C5 and C7 and inductor L2 are used to tune the oscillator frequency. Trimmer R12 sets the effective negative resistance for the oscillator and is adjusted for chaotic oscillation. Trimmer R51 is set to balance the nonlinearity of diodes D1 and D2. The output of the scrambler is provided at J2. Trimmers R17 and R18 are used to adjust for a 1-V peak-to-peak scrambled output for compatibility with a standard RS-170 video transmitter. Buffered outputs at J1 and J3 are available to observe waveforms and test synchronization.

A detailed schematic of the descrambler is shown in Fig. 10. The received scrambled signal enters at J1. Operational amplifiers U1 and U2 restore the signal amplitude and DC offset, which are set using trimmers R1 and R6, respectively. The variable resistors R19 and R25, as well as the variable capacitors C3 and C5 and inductor L1, are used to correct parameter mismatch and tune for optimal synchronization and signal recovery. Buffered outputs at J2 and J3 are available to observe waveforms and tune synchronization quality. The recovered analog video signal is output at J4. The operational amplifier U7 corrects the polarization of the video signal and sets the DC level and amplitude of the output, which are adjusted with trimmers R29 and R35, respectively.

5. SCRAMBLER OPERATION

A typical waveform generated by the chaotic scrambler with no video input signal and captured using a digital sampling oscilloscope (Agilent 54624A) is shown in Fig. 11. This waveform has an average return time of 0.9 μs, corresponding to a center frequency of 1.1 MHz. The corresponding captured phase-space projection is shown in Fig. 12. Qualitatively, the waveform and attractor compare reasonably well to the simulated model results in Figs. 4 and 5.

The functionality of the scrambler system was successfully demonstrated using a color video signal from

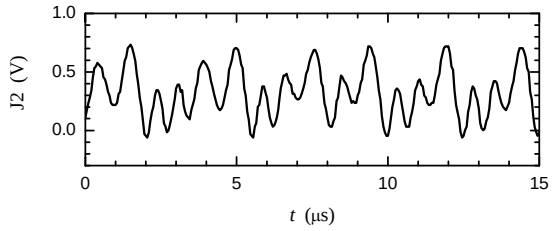

Fig. 11. Waveform captured from the chaotic scrambler output at connector J2 with no input video signal.

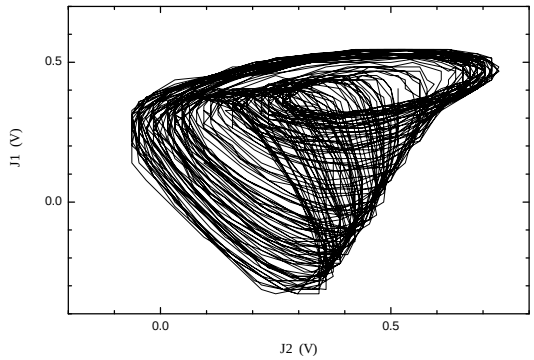

Fig. 12. Phase-space projection of waveforms captured from the chaotic scrambler output with no input video signal.

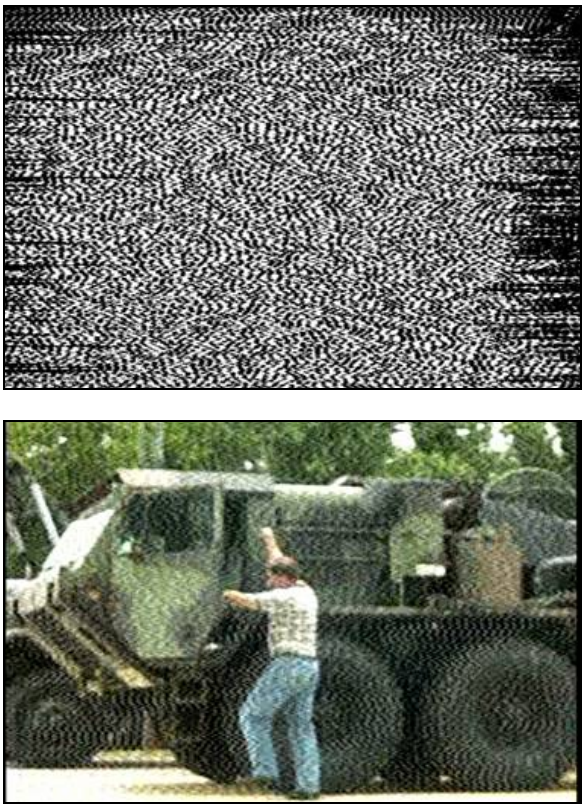

Fig. 13. Scrambled (top) and descrambled (bottom) images captured from the chaotic analog video scrambler demonstration system with direct connection.

a standard analog video camera. For initial tests, the scrambled signal was transmitted straight to the descrambler via a direct-wire connection. The received signal was descrambled and viewed in real time on a color monitor. Typical still frames captured from an initial test are shown in Fig. 13. The scrambled signal appears simply as noise, thereby denying any useful information to an eavesdropper, while the descrambled signal recovers the original image. As evident from the figure, chaotic scrambling thoroughly obscures the video and color information. Furthermore, even the video sync signals are hidden, making it difficult to determine even the start of a video frame or line. Moreover, we have conducted tests where the sync signal is known to the eavesdropper, and we observed that the video image is still successfully obscured.

To demonstrate chaotic scrambling in a wireless radio link, an analog video signal was scrambled and transmitted using commercially available FM radios (Broadcast Microwave Services BMR-120). The received radio signal was descrambled and viewed on a color monitor. Fig. 14 shows a sequence of video frames captured from a wireless test conducted in our laboratory. Some distortion due to noise and losses in the radio transmission is expected to impact the descrambler's ability to recover the original video. However, despite these losses, the received signal is successfully descrambled and the color video was successfully recovered.

6. CONCLUSION

The advantage of chaotic scrambling over more sophisticated digital encryption techniques is its simple analog implementation. It is important to note the functionality obtained despite the incredible simplicity of the scrambling and descrambling circuits. Each component consists of just a few common, analog components. The details of the chaotic circuit constitute the "key", including the circuit topology, capacitances, inductance, and diode characteristics. In principle, this information can be extracted from the transmitted signal without a matched descrambling circuit, but only by using sophisticated nonlinear digital signal processing techniques that require comparatively expensive digitization and computation technology (Pérez and Cerdeira, 1995). The cost and complexity asymmetry to intercept the scrambled transmissions implies there is still an effective level of security provided by chaotic

Fig. 14. Descrambled video images captured from the chaotic analog video scrambler demonstration system using a wireless FM radio link.

scrambling. Although not true encryption, it can still provide sufficient security against casual eavesdroppers and for time-critical communications.

This technology demonstration paves the way for full exploitation of chaotic scrambling in military applications where cost and power budgets rule out the use of digital encryption. Future developments in this technology will include a programmable key and improved resistance to signal processing attacks. One approach may be to use higher-dimensional chaotic oscillators (Blakely and Corron, 2004). The technology may also be scaled in frequency for use at even higher information bandwidths. We are currently pursuing this research along with other applications of chaos engineering for military use.

REFERENCES

Blakely, J. N., and N. J. Corron, 2004: Experimental Observation of Delay-Induced Radio Frequency Chaos in a Transmission Line Oscillator, *Chaos*, **14**, 1035-1041

Corron, N. J., 1997: An Approach for Communications with Chaotic Waveforms. *Proceedings of the 4th Experimental Chaos Conference*, Boca Raton, FL, World Scientific, 395-406.

Corron, N. J., J. N. Blakely, and S. D. Pethel, 2004: Beam Steering by Lag Synchronization in Wide-Bandwidth, Chaotic Arrays. *Experimental Chaos*, S. Boccaletti, Ed., American Institute of Physics, 45-50.

Corron, N. J., J. N. Blakely, and S. D. Pethel, 2005: Lag and Anticipating Synchronization without Time-Delay Coupling, *Chaos*, **15**, 023110.

Cuomo, K. M., A. V. Oppenheim, and S. H. Strogatz, 1993: Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications, *IEEE Transactions on Circuits and Systems II*, **40**, 626-633.

Feldmann, U., M. Hasler, and W. Schwarz, 1996: Communication by Chaotic Signals : The Inverse System Approach, *International Journal of Circuit Theory and Applications*, **24**, 551-579.

Kocarev, L., 2001: Chaos-Based Cryptography: A Brief Overview, *IEEE Circuits and Systems Magazine*, **1**, 6-21.

Myneni, K., N. J. Corron, S. D. Pethel, B. R. Reed, and T. A. Barr, 2004: Masked Communications for Unmanned Systems. *Proceedings of the Workshop on Tactical Battlefield Communications for Missiles, Rotorcraft, and Unmanned Vehicles*, Redstone Arsenal, AL, U. S. Army AMRDEC, 47-57.

Pecora, L. M., and T. L. Carroll, 1990: Synchronization in Chaotic Systems, *Physical Review Letters*, **64**, 821-824.

Pérez, G., and H. A. Cerdeira, 1995: Extracting Messages Masked by Chaos, *Physical Review Letters*, **74**, 1970-1973.