ON AN IMPROVED CHAOTIC SHIFT KEYING COMMUNICATION SCHEME

Timothy J. Wren[1] **and Tai C. Yang**[2]

Engineering and Design, University of Sussex
Brighton, East Sussex, England, BN1 9RH

Abstract: There is a great interest in secure communications within industry and various sectors of society. One common approach of achieving this is by encoding the information using shift-keying methods such as Binary Phase Shift Keying and Quadrature Phase Shift Keying. Proposed in this paper is a new robust yet simple multilevel differential chaotic shift-keying scheme. Compared with the schemes currently in use it has advantages of good noise rejection and increased data transmission rates. Under this scheme, instead of using one or two-dimensional encoding, an extendable m dimensional coding method is used and its effectiveness is demonstrated by presenting simulation results for a four-dimensional system. The potential of implementing this scheme in real-time applications is under investigation.

Keywords: Nonlinear Systems, Communication Schemes, Orthogonal Sequences, Secure Communications, Singular Value Decomposition

1. INTRODUCTION

Over recent years a great deal of research has focused on chaotic communication schemes. The primary driver for this interest is that chaos based schemes are inherently highly secure and have good spectral efficiencies which give good noise rejection. There are two basic types of method utilizing these chaotic signals. The first methods rely on ideas first introduced by Pecora and Carroll (Pecora *et al.*, 1990, 1991) and employed by (Cuomo *et al.*, 1993), which choose a particular state of a chaotic system to transmit. In turn this is used in the receiver to synchronize a similar chaotic circuit and allow regeneration of the complete set of chaotic states needed for decoding the incoming message sequences. These methods, although attractive, have not proved to be sufficiently robust with noisy transmission channels (Kolumbán *et al.*, 1998). The second types of method are characterized by the transmission of a reference signal. The most successful has been Differential Chaos Shift Keying (DCSK) which introduced chaotic processes into existing correlation based schemes. This method transmits a chaotic function for half of the symbol interval and then a duplicate or inverted version of the same signal in the second half representing a ‘1’ or ‘0’. This is exactly analogous to a BPSK scheme and decoding is achieved by correlation of both halves of the signal. As with BPSK there are extensions that include QPSK, M-ary constellations and QAM. A method directly analogous to QPSK was introduced by Galias and Maggio (Galias, *et al.*, 2001) known as Quadrature Chaotic Shift keying (QCSK) outlined in section 2. Further work on DCSK by Salberg and Hanssen (Salberg A. *et al.*, 2006) characterizes a chaotic signal within an orthonormal subspaces and utilizes this to choose the transmitted signal.

The QCSK method and its obvious extensions rely on complex two-dimensional orthogonality of the sine and cosine functions. This paper the introduces the idea of extending the dimensionality of encoding to an m dimensional space and deriving m orthogonal functions as the range space of a series of vectors in n space mapped from m times n samples of the chaotic signal. The result is a robust yet simple communication scheme.

In section 3. the method of orthogonal chaos shift keying is outlined and some simulation results and conclusions are presented in sections 4. and 5. respectively.

2. QUADRATURE CHAOTIC SHIFT KEYING

This is a derivation of the well-known Quadrature Phase Shift Keying (QPSK), which itself is related to the Binary

[1] tjw22@sussex.ac.uk
[2] T.C.Yang@sussex.ac.uk
Permanent address: Dept. of Engineering and Design, University of Sussex, Brighton, East Sussex, England, BN1 9RH

Phase Shift Keying (BPSK). In both of these methods the underlying carrier signal is sinusoidal. For the BPSK technique a portion of the sinusoid signal is transmitted to represent a ‘0’ and its anti-phase counterpart is transmitted to represent a ‘1’. QPSK requires two orthogonal signals, which are added together in a combination of four ways to give a four state transmitted signal. In the receiver the signal parameters are determined by correlating them with each of the orthogonal signals and hence the exact meaning of the received signal can be deciphered. The signals used in this technique are sinusoidal and the orthogonal counterparts are therefore cosine functions.

In Quadrature Chaotic Shift Keying the sinusoidal signal is replaced by a chaotic reference signal, generated over a fixed time interval, by a chaotic system. A signal that is orthogonal to this is then generated and these signals are used in a similar way to the QPSK set of orthogonal signals. There are two principal advantages to using chaotic signals. The first is that it allows messages to be transmitted in a secure or covert way where a potential intruder could easily reject the transmitted signals as noise. Secondly, the signal now has spread spectrum characteristics that improve the noise rejection properties.

Consider a signal $x(t) \forall t \in [0,T]$, which is generated by a chaotic process and is modified so that is has zero mean; that is

$$\frac{1}{T}\int_0^T x(t)dt = 0 \tag{1}$$

then a Fourier expansion of this signal can be expressed as

$$x(t) = \sum_{m=1}^{\infty} f_m \sin(m\omega t + \phi_m) \tag{2}$$

where $\omega = 2\pi / T$ and $f_0 = 0$

Define the average power of this signal as

$$P_x = \frac{1}{T}\int_0^T x^2(t)dt \tag{3}$$

which because of the following properties of sinusoidal functions

$$\frac{1}{T}\int_0^T f_m \sin(m\omega t + \phi_m - \alpha) f_n \sin(n\omega t + \phi_n - \beta)dt$$

$$= \frac{1}{2} f_m^2 \cos(\alpha - \beta) \qquad \forall \;\; m = n$$

$$= 0 \qquad \forall \;\; m \neq n \tag{4}$$

can be expressed as

$$P_x = \frac{1}{2}\sum_{m=1}^{\infty} f_m^2 \tag{5}$$

Now to derive a signal that is orthogonal to $x(t)$ by applying a Hilbert Transform to the signal with a phase shift of $\pi / 2$. This can be achieved by taking a Fourier Transform of the signal and rotating the positive frequencies by $\pi / 2$ and the negative ones by $-\pi / 2$ and finally inverting the transform to give

$$y(t) = \sum_{m=1}^{\infty} f_m \sin(m\omega t + \phi_m + \frac{\pi}{2}) \tag{6}$$

then

$$x \perp y \Leftrightarrow \frac{1}{T}\int_0^T x(t)y(t)dt = 0 \tag{7}$$

it follows then that

$$P_x = P_y \Leftrightarrow \frac{1}{T}\int_0^T x^2(t)dt = \frac{1}{T}\int_0^T y^2(t)dt \tag{8}$$

Consider now two possible maximally separated constellations of signals that consist of an addition of a proportion of each orthogonal signal. These can be represented on an Argand diagram

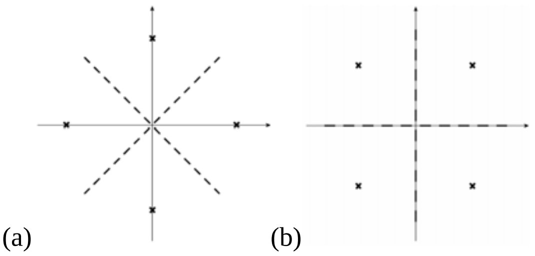
(a) (b)

Fig. 1. Maximal Separation Quadrature Constellations existing on a two dimensional hypersphere: (a) symbol encoding contains the reference signal whereas (b) encodes all symbols.

	Symbol	0	1	2	3
(a)	**c**	1 0	0 1	-1 0	0 -1
(b)	**c**	$1/\sqrt{2}$ $1/\sqrt{2}$	$-1/\sqrt{2}$ $1/\sqrt{2}$	$-1/\sqrt{2}$ $-1/\sqrt{2}$	$1/\sqrt{2}$ $-1/\sqrt{2}$

Table 1. Maximal separation quadrature constellation encoding symbol maps

Each symbol can be represented as

$$c = \alpha + j\beta \tag{9}$$

Orthogonality is assured in the complex plane and its analogy can therefore be represented along the real time axis if the two complimentary signals are orthogonal; that is

$$s(t) = \alpha x(t) + \beta y(t) \tag{10}$$

this is the message signal for each symbol in the message.

At the receiver the symbols can be retrieved by determining the coefficients of each individual orthogonal component by using the two correlation integrals

$$\alpha = \frac{1}{P_x T}\int_0^T s(t)x(t)dt \tag{11}$$

$$\beta = \frac{1}{P_y T}\int_0^T s(t)y(t)dt \tag{12}$$

From

$$\begin{aligned}\int_0^T s(t)x(t)dt &= \int_0^T (\alpha x(t) + \beta y(t))x(t)dt \\ &= \int_0^T \alpha x^2(t) + \beta y(t)x(t)dt \\ &= \alpha P_x T\end{aligned} \tag{13}$$

$$\begin{aligned}\int_0^T s(t)y(t)dt &= \int_0^T (\alpha x(t) + \beta y(t))y(t)dt \\ &= \int_0^T \alpha x(t)y(t) + \beta y^2(t)x(t)dt \\ &= \beta P_y T\end{aligned} \tag{14}$$

3. ORTHOGONAL CHAOS SHIFT KEYING

3.1 *Introduction*

The Quadrature Chaos Shift Keying method can clearly be developed into an M-ary type constellation method that allows the transmission of more symbols improving the symbol cycle efficiency. A disadvantage of this method is that all points on the constellation lie on a fixed radius circle that is normally represented on the complex plane. Large numbers of symbols require an equally large number of points on the fixed circle which becomes crowded and hence gives rise to potential misinterpretation on decoding. One way to avoid this is to also vary the amplitude of the symbol representations as well as the phase (QAM). This form of variation of circle radius is not desirable, as this would make the signals more easily detectable. Presented is a method of overcoming this problem by the use of a system of orthogonal sequences derived by the method of singular value decomposition.

3.1 *Theoretical Analysis*

Consider an n dimensional space. Any point can be represented by an n dimensional vector that is a linear sum of the set of orthonormal basis vectors.

$$\mathbf{p} = \rho_1\mathbf{i}_1 + \rho_2\mathbf{i}_2 + \rho_3\mathbf{i}_3 + \ldots + \rho_n\mathbf{i}_n \tag{15}$$

Now consider a subset of size m of these basis vectors that describe an m dimensional subspace within the n dimensional space. Further consider the set of vectors describing some hypersurface within this m dimensional subspace.

$$\mathbf{c} = a_1\mathbf{i}_1 + a_2\mathbf{i}_2 + a_3\mathbf{i}_3 + \ldots + a_m\mathbf{i}_m \tag{16}$$

The selected subspace vectors can now be mapped onto the real time axis so that each basis vector represents a set of discrete time values of a real function $u_i(t)\ \forall\ i \in [1, m]$. Orthogonal encoding of our message can now be represented as

$$s(t) = a_1u_1(t) + a_2u_2(t) + a_3u_3(t) + \ldots + a_mu_m(t) \tag{17}$$

which in vector notation becomes

$$s(t) = \mathbf{u}^T(t)\mathbf{c} \tag{18}$$

where

$$\mathbf{u}^T(t) = [u_1(t), u_2(t), u_3(t), \ldots, u_m(t)] \tag{19}$$

$$\mathbf{c}^T = [a_1, a_2, \ldots, a_m] \tag{20}$$

this is the message signal for each symbol in our message.

At the receiver the symbols can be retrieved by determining the coefficients of individual orthogonal components by using the m correlation integrals

$$a_i = \frac{1}{P_i T}\int_0^T s(t)u_i(t)dt \quad \forall \quad i \in [1, m] \tag{21}$$

$$P_i = \frac{1}{T}\int_0^T u_i^2(t)dt \tag{22}$$

or from (18) (19) (20)

$$\int_0^T \mathbf{u}(t)s(t)dt = \int_0^T \mathbf{u}(t)\mathbf{u}^T(t)\mathbf{c}dt \tag{23}$$

Therefore

$$\mathbf{c} = \left[\int_0^T \mathbf{u}(t)\mathbf{u}^T(t)dt\right]^{-1}\int_0^T \mathbf{u}(t)s(t)dt \tag{24}$$

This will work with any set of signals if they are independent. If the signal sets are orthogonal then the matrix being inverted becomes diagonal and the noise rejection is greatly improved.

3.2 *Orthogonal Signal Generation*

The generation of a set of m orthogonal signal sets is required. Consider a chaotic signal sampled at regular intervals and the values placed into a series of m vectors $\mathbf{x}_i \ \forall \ i \in [i, m]$ of length n and arrange these vectors into an nxm matrix $\mathbf{X}$. Now consider the singular value decomposition of this matrix.

$$\mathbf{X} = \mathbf{UWV}^T \tag{25}$$

where

$$\mathbf{U}^T\mathbf{U} = \mathbf{V}^T\mathbf{V} = \mathbf{I}_m \tag{26}$$

The matrix $\mathbf{X}^T\mathbf{X}$ is symmetric and the chaotic process is sufficiently varying so that the columns of $\mathbf{X}$ are independent; then the eigenvalues are all real and positive. This implies that if $\mathbf{V}$ is the matrix of eigenvectors of $\mathbf{X}^T\mathbf{X}$ then it is orthonormal. $\mathbf{W}$ is a diagonal matrix of the square roots of the eigenvalues of $\mathbf{X}^T\mathbf{X}$ and $\mathbf{U}$ is an orthonormal set of vectors describing the range space of $\mathbf{X}$ calculated as

$$\mathbf{U} = \mathbf{XVW}^{-1} \tag{27}$$

$$\mathbf{W} = diag\left(\sqrt{\lambda_i}\right) \quad \forall \ i \in [1, m] \tag{28}$$

λ_i are the eigenvalues of $\mathbf{X}^T\mathbf{X}$.

The algorithms available for finding the eigenvalues and vectors of matrices are well understood and robust so the generated signals sets are easily generated. The $\mathbf{U}$ matrix can be split into a set of vectors $\mathbf{u}_i \ \forall \ i \in [i, m]$, which can be seen as samples of a set of continuous signals with zero mean over the interval $t \in [0, T]$ and average powers of $1/n$. These can now be encoded according to an encoding scheme, power balanced and transmitted.

3.3 *Encoding Scheme*

Consider the nxm signal matrix $\mathbf{X}$; produced by taking nxm samples of the chaotic process and the nxm orthonormal matrix $\mathbf{U}$ generated from it.
A transmittable signal sequence is generated from the columns of $\mathbf{U}$ by using an encoding vector for each symbol to be represented. The transmitted sequence for the symbol is therefore only n long whereas the transmitted reference is m times longer.
A simple 'symmetric' solution is to transmit m symbols with m encoded sequences for each reference sequence. Each encoded sequence can represent 2^m states or symbols with each transmission set of reference and encoded sequences it is possible to transmit a possible $\left(2^m\right)^m$ different symbols by shifting in a bit register m bits left for each of the m sequences as shown in fig. 2.

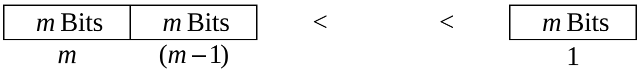

Fig. 2. Shift register of m bits for each of the m sequences.

3.4 *Encoding Parameter Inversion*

When the reference signal is received a matrix $\mathbf{X}$ is formed which produces a set of orthonormal sequences $\mathbf{U}$ which, if uncorrupted by noise, should be exactly the same as the one produced in the transmitter. A problem arises however in the production of the eigenvector matrix $\mathbf{V}$ which, while being orthonormal and being derived from $\mathbf{X}^T\mathbf{X}$, is not unique. The eigenvalues of $\mathbf{V}$ are unique but can generate eigenvectors that can be inverted. This would manifest itself by effectively inverting one of the parameters in encoding vectors for each of the m sequences. If the symbol map is fully defined and symmetric then these inverted encoding parameters are undetectable since the vector with certain parameters inverted has a complement that is a valid encoding vector for a different symbol.

3.5 *Non-Complementary Encoding*

In fig. 1. of section 2. the encoding vectors can be derived from the diagrams and consist of either ± 1 's and 0's or $\pm 1/\sqrt{2}$'s, each scheme has a complement on inversion representing another symbol in the symbol map. These two schemes are fully defined symmetric maps for two dimensions with maximal separation of encoding parameters on a spherical hypersurface of order two and are therefore complementary. As described in section 3.4 this complementary characteristic has a fatal flaw for encoding symbols. This can be overcome by employing a non symmetric and hence a non-complementary symbol map. This consists of a map where the positive values of the encoding vectors are not the same as the negative ones, which makes each symbol encoding vector unique. If the hypersurface for a complementary symbol map in m dimensions is defined as points on the hypersphere then this surface can be made non complementary by not centring it about the origin. If the centre of the hypersphere is moved by $-1/3\sqrt{m}$ in all dimensions a two to one complement is formed.
fig 3. and table 2. shows a non-complementary symbol map for m =2 with the origin shifted but the radius of unity is retained.

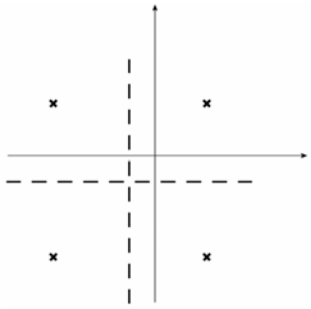

Fig. 3. Maximal Separation Quadrature Constellations existing on an offset two-dimensional hypersphere with all signals encoded.

	Symbol	0	1	2	3
(a)	$\mathbf{c}$	$\sqrt{2}/3$ $-2\sqrt{2}/3$	$-2\sqrt{2}/3$ $\sqrt{2}/3$	$-2\sqrt{2}/3$ $\sqrt{2}/3$	$\sqrt{2}/3$ $-2\sqrt{2}/3$

Table 2. Maximal Separation Quadrature Constellation Encoding

3.6 *Decoding Method*

The equivalent of the correlation integral in equation (24) is a least squares approximation of the encoding vector given a noisy received signal matrix $\overline{\mathbf{X}}$. If the received signal of the i^{th} column is considered then

$$\bar{\mathbf{s}}_i = \mathbf{UPc}_i + \sigma\boldsymbol{\varepsilon}_i \tag{29}$$

where $\boldsymbol{\varepsilon}_i$ is Gaussian White noise so $E\{\boldsymbol{\varepsilon}_i\} = \mathbf{0}$ with variance σ^2 and $\mathbf{P}$ is a diagonal power balance matrix. In the following equations the $^{-}$ notation indicates a variable derived from received signal data and the ^ indicates an estimated value.

Let

$$\hat{\mathbf{s}}_i = \overline{\mathbf{UP}}\hat{\mathbf{c}}_i \tag{30}$$

$$\mathbf{e}_i = \mathbf{s}_i - \hat{\mathbf{s}}_i \tag{31}$$

And

$$\varepsilon_i = \mathbf{e}_i{}^T \mathbf{e}_i \tag{32}$$

Now minimize ε_i with respect to the estimate of the encoding vector $\hat{\mathbf{c}}_i$

$$2\mathbf{e}_i{}^T \frac{\partial \mathbf{e}_i}{\partial \hat{\mathbf{c}}_i} = \mathbf{0}^T \tag{33}$$

$$\frac{\partial \mathbf{e}_i}{\partial \hat{\mathbf{c}}_i} = -\overline{\mathbf{UP}} \tag{34}$$

So (33) can be rearranged as

$$\overline{\mathbf{P}}^T \overline{\mathbf{U}}^T (\bar{\mathbf{s}}_i - \overline{\mathbf{UP}}\hat{\mathbf{c}}_i) = \mathbf{0} \tag{35}$$

And finally

$$\hat{\mathbf{c}}_i = \left[\overline{\mathbf{P}}^T \overline{\mathbf{U}}^T \overline{\mathbf{UP}}\right]^{-1} \overline{\mathbf{P}}^T \overline{\mathbf{U}}^T \bar{\mathbf{s}}_i \tag{36}$$

If all m sequences are considered then this equation becomes

$$\hat{\mathbf{C}} = \left[\overline{\mathbf{P}}^T \overline{\mathbf{U}}^T \overline{\mathbf{UP}}\right]^{-1} \overline{\mathbf{P}}^T \overline{\mathbf{U}}^T \overline{\mathbf{S}} \tag{37}$$

where

$$\hat{\mathbf{C}} = [\hat{\mathbf{c}}_1, \hat{\mathbf{c}}_2, ..., \hat{\mathbf{c}}_m] \quad \text{and} \quad \overline{\mathbf{S}} = [\bar{\mathbf{s}}_1, \bar{\mathbf{s}}_2, ..., \bar{\mathbf{s}}_m] \tag{38}$$

Now if the received orthonormal $\overline{\mathbf{U}}$ matrix is not power balanced then the matrix inversion is may not necessary but if power balancing is applied it should be approximately diagonal.

Further to this if one of the parameters is inverted due to an inversion in one of the eigenvectors then this manifests itself as a row of $\hat{\mathbf{C}}$ being inverted. If the full symbol map were considered this row would correspond to one of the map's columns or its inversion; because the symbol in not complementary it is easy to determine if $\hat{\mathbf{C}}^T$ contains any inverted map values by choosing the minimum errors between each of the columns of $\hat{\mathbf{C}}^T$ and $-\hat{\mathbf{C}}^T$. Selecting these values and replacing them with the map values results in the best estimate of $\hat{\mathbf{C}}$ being obtained.

4. SIMULATION

4.1 *Simulation*

A set of simulation results of the proposed scheme, with Gaussian White noise added in the communication channel, is presented in this section. The system diagram is shown in fig 4. The chaotic system used here is a form of the Lorenz system with the first state used as the signal $x(t)$; that is

$$\begin{aligned} \alpha\dot{x} &= -\sigma x + \sigma y \\ \alpha\dot{y} &= rx - y - xz \\ \alpha\dot{z} &= xy + \beta z \end{aligned} \tag{39}$$

where $r = 28,\ \sigma = 10$ and $\beta = 8/3$. α can be chosen to suit the sampling time of the system.

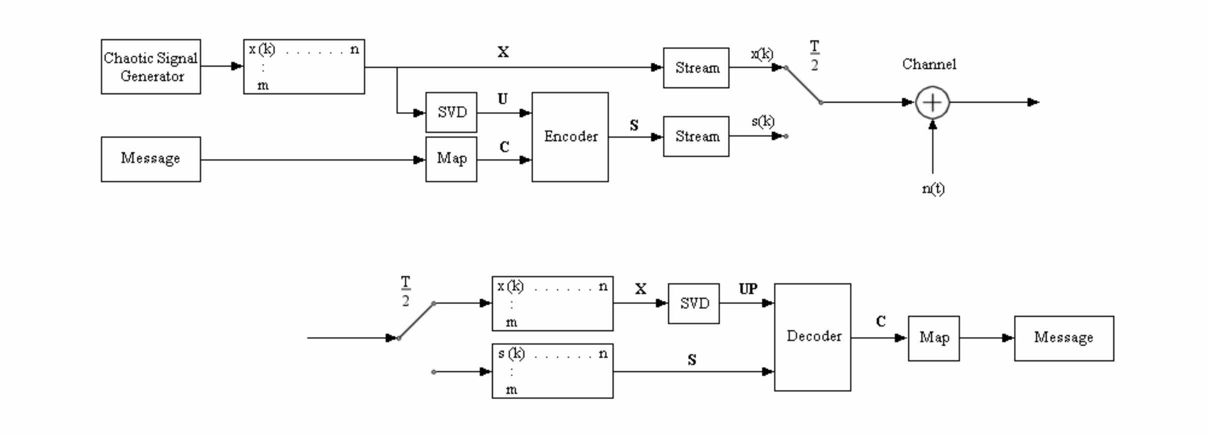

Fig. 4. Simulation Schematic Diagram

The signal sequences $\mathbf{X}$ and the resultant orthonormal sequences are show in fig 5. (a)(b) and the received signals and reconstructed orthonormal sequences with the channel noise are show in fig 5. (c)(d). The effect of the eigenvector inversion is seen in fig 5. (d) and illustrates why the decoding technique has to consider potentially inverted encoding parameters. Finally fig 6. (a) shows a random message sequence, which has been transmitted over the channel, and the resultant received message is shown in fig 6. (b). The received message is delayed by nxm sample times that corresponds to the number of samples required to fill the signal matrix $\mathbf{X}$ before encoding can begin. The simulation results do not take into account any time shift correlation that may prove necessary on a real communication channel. However it is reasonable to assume that this shift would be taken care of in the communication preamble before data communication begins.

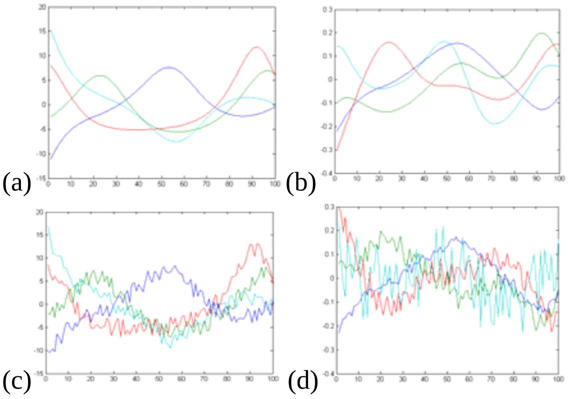

Fig. 5. (a) Transmitter zero mean chaotic reference sequences $\mathbf{X}$ for $m = 4$, (b) Resultant orthonormal sequences $\mathbf{U}$. (c) Received reference sequences, (d) Resultant receiver generated orthonormal sequences showing inversion on some signals.

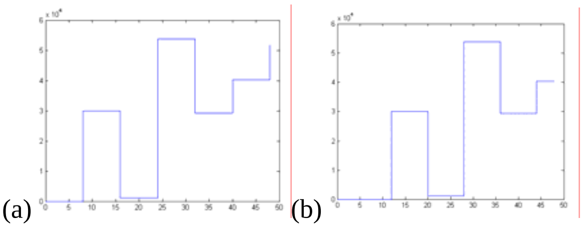

Fig 6. (a) Transmitted message and (b) Received message delayed by nxm sample intervals.

5. CONCLUSIONS

In this paper we propose a new form of multilevel chaotic communication scheme based on the DCSK schemes and a method of deriving orthogonal signals using the singular valued decomposition of vectors of signals in n space. The advantages over QCSK are that the encoding and decoding are considerably simpler and extendible to m dimensional spaces giving encoding values at maximal distances in the m space that improves noise rejection and increases data transmission rates.

REFERENCES

Pecora L.K. and Carroll T.L. (1990)
Synchronization in Chaotic Systems
Phys. Rev. Lett.,
Volume 64, Issue 8, Page(s): 821-824

Pecora L.K. and Carroll T.L. (1991)
Driving Systems with Chaotic Signals
Phys. Rev. A,
Volume 44, Number 4, Page(s): 2374-2384

Cuomo K. M. and Oppenheim A. V. (1993)
Circuit Implementation of Synchronized Chaos with Applications to Communications
Phys. Rev. Lett.,
Volume 71, Issue 1, Page(s): 65-68

Kolumbán G., Kennedy M.P. and Chua L.O. (1998)
The Role of Synchronization in Digital Communications Using Chaos – Part II: Chaotic Modulation and Chaotic Synchronization
IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,
Volume 45, Issue 11, Page(s): 1129-1140

Galias, Z. and Maggio, G.M. (2001).
Quadrature Chaos Shift Keying.
IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,
Volume 48 Issue 12, Page(s): 1510-1519.

Salberg A. and Hanssen A., G.M. (2006).
A Subspace Theory for Differential Chaos-Shift Keying.
IEEE Transactions on Circuits and Systems II: Express Briefs,
Volume 53 Issue 1, Page(s): 51-55.