(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년02월20일
(11) 등록번호 10-0805888
(24) 등록일자 2008년02월14일

(51) Int. Cl.
H04L 7/00 (2006.01) *G09C 5/00* (2006.01)
H04K 1/00 (2006.01)
(21) 출원번호 10-2004-0050901
(22) 출원일자 2004년06월30일
심사청구일자 2004년06월30일
(65) 공개번호 10-2006-0001738
(43) 공개일자 2006년01월06일
(56) 선행기술조사문헌
JP10093549 A
JP2000049771 A
JP2000089182 A
전체 청구항 수 : 총 10 항

(73) 특허권자
배재대학교 산학협력단
대전 서구 도마동 439-6
(72) 발명자
김칠민
대전 대덕구 오정동 신동아아파트 2동509호
(74) 대리인
권혁성, 이노성

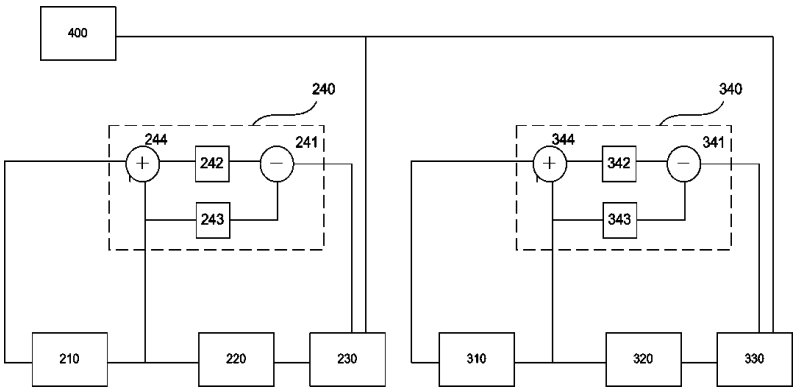
심사관 : 전용해

(54) 지연시간 변조에 의한 혼돈의 동기화 장치 및 이를 이용한통신 장치

(57) 요 약

본 발명은 지연시간 변조를 이용하여 혼돈 장치를 동기화하는 동기화장치 및 통신장치에 관한 것으로, 초기값이 달라 서로 다른 혼돈신호를 만드는 두개의 동일한 혼돈장치가 서로 동일한 신호를 발생시키도록 하기 위해, 동일한 지연시간 변조에 의해 두 혼돈 시스템을 동기화 시키고, 이 혼돈장치에서 발생한 혼돈신호를 이용하여 정보신호를 암호화, 복호화하는 혼돈장치의 동기화장치 및 이를 이용한 통신장치에 관한 것이다. 이를 위하여 본 발명은, 소정의 혼돈계에 따른 변수들이 함수적으로 서로 연결되어 혼돈특성을 갖는 적어도 하나 이상의 혼돈신호를 발생하는 주혼돈장치와, 상기 주혼돈장치와 동일하게 구성되며, 상기 주혼돈장치가 발생하는 혼돈신호에 대응되는 혼돈신호를 발생하는 종속혼돈장치로 이루어진 혼돈시스템에 있어서, 변조신호를 발생하는 변조신호 발생수단과, 상기 주혼돈장치로부터 발생되는 혼돈신호를 시간지연시키는 제1시간지연수단과, 상기 시간지연된 혼돈신호를 상기 변조신호 발생수단에서의 변조신호로 상기 제1시간지연수단에서 출력되는 지연시간을 변조하는 제1지연시간변조수단와, 상기 종속혼돈장치로부터 발생되는 혼돈신호를 시간지연시키는 제2시간지연수단과, 상기 시간지연된 혼돈신호를 상기 변조신호 발생수단에서의 변조신호로 상기 제2시간지연수단에서 출력되는 지연시간을 변조하는 제2지연시간변조수단과, 상기 제1지연시간변조수단으로부터 변조된 지연시간을 상기 주혼돈장치로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치로 되먹임하는 제1동기화부와, 상기 제2지연시간변조수단으로부터 변조된 지연시간을 상기 주혼돈장치로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치로 되먹임하는 제2동기화부로 이루어진다.

대표도 - 도3



특허청구의 범위

청구항 1

소정의 혼돈계에 따른 변수들이 함수적으로 서로 연결되어 혼돈특성을 갖는 적어도 하나 이상의 혼돈신호를 발생하는 주혼돈장치(210)와, 상기 주혼돈장치(210)와 동일하게 구성되며, 상기 주혼돈장치(210)가 발생하는 혼돈신호에 대응되는 혼돈신호를 발생하는 종속혼돈장치(310)로 이루어진 혼돈시스템에 있어서,

변조신호를 발생하는 변조신호발생수단(400)과;

상기 주혼돈장치(210)로부터 발생되는 혼돈신호를 시간지연시키는 제1시간지연수단(220)과;

상기 변조신호발생수단(400)에서의 변조신호로 상기 제1시간지연수단(220)에서 출력되는 지연시간을 변조하는 제1지연시간변조수단(230)과;

상기 종속혼돈장치(310)로부터 발생되는 혼돈신호를 시간지연시키는 제2시간지연수단(320)과;

상기 변조신호발생수단(400)에서의 변조신호로 상기 제2시간지연수단(320)에서 출력되는 지연시간을 변조하는 제2지연시간변조수단(330)과;

상기 제1지연시간변조수단(230)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치(210)로 되먹임하는 제1동기화수단(240)와;

상기 제2지연시간변조수단(330)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치(310)로 되먹임하는 제2동기화수단(340);

로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 동기화 장치

청구항 2

제 1항에 있어서, 상기 제1동기화수단(240)는

상기 주혼돈장치(210)의 임의의 혼돈신호를 제1스케일링 계수로 스케일링하는 제1스케일링부(242)

상기 제1지연시간변조수단(230)의 변조된 지여시간으로부터 스케일링된 상기 주혼돈장치(210)의 혼돈신호를 감산하는 감산기(241);

상기 감산기(241)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(243); 및

상기 제2스케일링부(243)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호를 가산하여 상기 주혼돈장치(210)로 되먹임하는 가산기(244)

로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 동기화 장치

청구항 3

제 1항에 있어서, 상기 제2동기화수단(340)는

상기 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 제1스케일링 계수로 스케일링하는 제1스케일링부(342)

상기 제2지연시간변조수단(330)의 변조된 지연시간으로부터 스케일링된 상기 종속혼돈장치(310)의 혼돈신호를 감산하는 감산기(341);

상기 감산기(341)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(343); 및

상기 제2스케일링부(343)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 가산하여 상기 종속혼돈장치(310)로 되먹임하는 가산기(344)

로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 동기화 장치

청구항 4

제 1항 내지 제3항의 어느 한 항에 있어서, 상기 변조신호는 주기적 신호, 혼돈신호, 난수신호, 잡음신호 등을 포함하는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 동기화 장치

청구항 5

소정의 혼돈계에 따른 변수들이 함수적으로 서로 연결되어 혼돈특성을 갖는 적어도 하나 이상의 혼돈신호를 발생하는 주혼돈장치(210)와;

변조신호를 발생하는 변조신호발생수단(400)과;

상기 주혼돈장치(210)로부터 발생되는 혼돈신호를 시간지연시키는 제1시간지연수단(220)과;

상기 변조신호발생수단(400)에서의 변조신호로 상기 제1시간지연수단(220)에서 출력되는 지연시간을 변조하는 제1지연시간변조수단(230)과;

상기 제1지연시간변조수단(230)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치(210)로 되먹임하는 제1동기화수단(240)와;

상기 제1지연시간변조수단(230)에서 출력되는 변조된 지연시간을 가지는 혼돈신호와 외부로부터 입력되는 정보신호를 가산하여 암호화 하는 암호화수단(250)과;

상기 암호화수단(250)을 통해 출력되는 신호를 무선 또는 유선으로 전송하는 암호송신수단(270)과;

변조신호를 송신하는 변조신호송신수단(260);

을 포함하는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 암호화 장치

청구항 6

제 5항에 있어서, 상기 제1동기화수단(240)는

상기 주혼돈장치(210)의 임의의 혼돈신호를 제1스케일링 계수로 스케일링하는 제1스케일링부(242)

상기 제1지연시간변조수단(230)의 변조신호로부터 스케일링된 상기 주혼돈장치(210)의 혼돈신호를 감산하는 감산기(241);

상기 감산기(241)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(243); 및

상기 제2스케일링부(243)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호를 가산하여 상기 주혼돈장치(210)로 되먹임하는 가산기(244)

로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 암호화 장치

청구항 7

제5항 또는 제6항에 있어서, 상기 변조신호는 주기적 신호, 혼돈신호, 난수신호, 잡음신호 등을 포함하는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 암호화 장치

청구항 8

암호화 신호를 수신하는 암호수신수단(370)과;

변조신호를 수신하는 변조신호수신수단(360)과;

주혼돈장치(210)와 동일하게 구성되며, 상기 주혼돈장치(210)가 발생하는 혼돈신호에 대응되는 혼돈신호를 발생하는 종속혼돈장치(310)와;

상기 종속혼돈장치(310)로부터 발생되는 혼돈신호를 시간지연시키는 제2시간지연수단(320)과;

상기 수신된 변조신호로 상기 제2시간지연수단(320)에서 출력되는 지연시간을 변조하는 제2지연시간변조수단(330)과;

상기 제2지연시간변조수단(330)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치(310)로 되

먹임하는 제2동기화수단(340);

상기 지연시간변조수단을 거쳐 출력되는 상기 종속혼돈장치(310)의 혼돈신호와 상기 암호수신수단(370)을 통해 수신된 암호화신호와의 차이를 구하여 정보신호를 복호화 하는 복호화수단(350);

으로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 복호화 장치

청구항 9

제 8항에 있어서, 상기 제2동기화수단(340)는

상기 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 제1 스케일링 계수로 스케일링하는 제1스케일링부(342);

상기 제2지연시간변조수단(330)의 변조된 지연시간으로부터 스케일링된 상기 종속혼돈장치(310)의 혼돈신호를 감산하는 감산기(341);

상기 감산기(341)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(343); 및

상기 제2스케일링부(343)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 가산하여 상기 종속혼돈장치(310)로 되먹임하는 가산기(344)

로 이루어지는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 복호화 장치

청구항 10

제8항 또는 제9항에 있어서, 상기 변조신호는 주기적 신호, 혼돈신호, 난수신호, 잡음신호 등을 포함하는 것을 특징으로 하는 지연시간 변조에 의한 혼돈시스템의 복호화 장치

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<19> 본 발명은 지연시간 변조를 이용하여 혼돈 장치를 동기화하는 동기화장치 및 통신장치에 관한 것으로, 초기값이 달라 서로 다른 혼돈신호를 만드는 두개의 동일한 혼돈장치가 서로 동일한 신호를 발생시키도록 하기 위해, 동일한 지연시간 변조에 의해 두 혼돈 시스템을 동기화 시키고, 이 혼돈장치에서 발생한 혼돈신호를 이용하여 정보신호를 암호화, 복호화하는 혼돈장치의 동기화장치 및 이를 이용한 통신장치에 관한 것이다.

<20> 최근 들어 '혼돈'에 의한 동기화방법에 대한 관심이 집중되면서 이러한 혼돈에 의한 동기화방법을 이용하여 산업의 각분야 특히 비밀통신 등에 적극적으로 응용하려는 연구들이 활발하게 진행되고 있다. 여기서, '혼돈'이란 널리 알려진 바와 같이 비선형적 물리계에서 발생되는 복잡한 물리적현상의 하나로서, 동일한 구성을 갖고 있는 두 혼돈계에서는 초기조건이 극히 조금만 달라도 시간이 지남에 따라 서로 전혀 다른 양상을 보여주기 때문에 예측이 불가능하게 되는 특성을 갖고 있는데, 이와 같이 혼돈시스템이 초기조건에 민감하게 반응하게 되는 특성을 혼돈이라고 하며, 또한, '나비효과'라고도 한다.

<21> 그런데 혼돈시스템을 산업상의 각 분야에서 응용하기 위해서는 기본적으로 혼돈현상을 제어하거나 동기화시킬 필요가 있다. 이러한, 혼돈시스템의 동기화란 여러 상태 변수들(State Variables)을 갖는 적어도 두 개 이상의 서로 동일한 혼돈장치로 구성된 혼돈시스템에서 각 혼돈장치의 상태변수가 서로 동일해지는 것을 의미한다.

<22> 즉, 서로 동일한 상태변수를 갖는 동일한 구성의 혼돈장치가 2개 있다고 할 때(이중 하나는 주 혼돈장치라 하고, 다른 하나는 종속 혼돈장치라 한다). 앞서 설명한 바와 같이 초기조건에서의 민감성 때문에 동기화되지 않은 각 혼돈시스템은 전혀 서로 다른 시간적 궤적을 보여 각 혼돈계는 서로 독립적인 혼돈시스템이 된다.

<23> 그런데, 주 혼돈장치의 임의의 한 상태변수를 종속 혼돈장치에 전달하고, 종속 혼돈장치가 이 상태변수를 적절히 이용하여 주 혼돈장치와 동기화되면, 주 혼돈장치의 모든 상태변수와 종속 혼돈장치의 모든 상태변수가 동일하게 변동하여 같아지게 되는 것이다. 이러한 혼돈시스템의 동기화 기술은 산업상의 여러분야에 응용될 수 있는

데 특히 비밀통신에 매우 적합하게 응용할 수 있다

<24> 이와 같은 혼돈시스템을 제어하여 동기화시키기 위한 종래 기술로는 국내등록특허공보 제0208309호 '잡음 혹은 혼돈신호를 변수에 되먹임시키는 것에 의한 혼돈 시스템 동기화장치 및 이를 이용한 비밀통신시스템'이 있으며, 이는 잡음 혼돈신호를 주혼돈계의 소정의 변수와 이에 대응하는 종속혼혼돈계의 변수에 되먹임시키는 것에 의해 동기화를 이루게 된다.

<25> 상기 종래기술을 도시된 도1을 중심으로 설명하면 다음과 같다.

<26> 동일한 두 혼돈장치가 하나의 혼돈시스템을 형성하고 있을 때, 한 혼돈장치가 주혼돈장치(30)이고, 다른 혼돈장치가 종속혼돈장치(36)이며, 주혼돈장치(30)와 종속혼돈장치(36)를 동기화시키기 위한 장치가 제1동기화부(31) 및 제2동기화부(37)이다. 여기서 제1동기화부(31)는 주혼돈장치(30)와 종속혼돈장치(36)를 동기화시키기 위하여, 잡음 혹은 혼돈신호(여기서는 g(t))를 제1스케일링 계수(α)로 스케일링하는 스케일링부(32), 스케일링부(32)에서 스케일링된 잡음 혹은 혼돈신호로부터 주혼돈장치(30)로부터 임의의 변수값(예컨대, x(t))을 감산하는 감산기(33), 감산기(33)의 출력신호로부터 다시 제2스케일링 계수(β)로 스케일링하는 스케일링부(34), 스케일링부(34)의 출력신호와 상기 변수값(x(t))을 가산하여 주혼돈장치(30)로 되먹임하는 가산기(35)로 구성된다. 한편, 제2동기화부(37)는 주혼돈장치(30)와 종속혼돈장치(36)를 동기화시키기 위하여, 잡음 혹은 혼돈신호(여기서는 g(t))를 제1스케일링 계수(α)로 스케일링하는 스케일링부(38), 스케일링부(38)에서 스케일링된 잡음 혹은 혼돈신호로 부터 주혼돈장치(30)로부터의 변수값(x(t))에 대응되는 종속혼돈장치(32)로부터의 변수값(x'(t))을 감산하는 감산기(39), 감산기(39)의 출력신호로 부터 다시 제2스케일링 계수(β)로 스케일링하는 스케일링부(40), 스케일링부(40)의 출력신호와 상기 변수값(x'(t))을 가산하여 종속혼돈장치(36)로 되먹임하는 가산기(41)로 구성된다. 이때 두 혼돈장치(30,36)는 모두 n개의 변수를 가지고 있는데, 주혼돈장치(30)의 변수들은 x(t), y(t), z(t), ... 이고, 종속혼돈장치(36)의 변수들은 x'(t), y'(t), z'(t), ... 이다. 여기서, α와 β는 음의 값이나 양의 값 모두가 될 수 있다.

<27> 일반적으로 혼돈장치는 초기치에 매우 민감하기 때문에 만약 두 혼돈장치(30,36)가 서로 동기화되지 않고 각각 동작한다면, 주혼돈장치(30)가 발생하는 상태변수 x(t)신호의 궤적과 종속혼돈장치(36)가 발생하는 상태변수 x'(t)신호의 궤적은 완전히 서로 다르게 된다. 따라서, 도 1에 도시된 주혼돈장치(30)와 종속혼돈장치(36)에서 제1동기화부(31)와 제2동기화부(37)가 없다면 두 혼돈장치(30,36)의 서로 대응되는 변수들이 모두 서로 다른 궤적으로 움직일 것이다. 이때 두 혼돈장치(30,36)를 동기화시키기 위하여 두 혼돈장치(30,36)에서 서로 대응되는 한 종류의 변수(예컨대, 여기서는 x(t)와 x'(t)) 혹은 그 이상의 변수들을 택해, 똑 같은 잡음 혹은 혼돈신호(여기서는 g(t))를 주혼돈장치(30)의 변수(x(t))와 종속혼돈장치(36)의 변수(x'(t))에 각각 더해 주어 되먹임시킨다. 여기서, 잡음 혹은 혼돈신호(g(t))의 크기를 α배로 스케일링하고, 스케일링된 잡음 혹은 혼돈신호(즉, αg(t))에서 두 혼돈계의 변수(x(t)와 x'(t))를 각각 뺀 다음 모두 β배로 스케일링하여 두 혼돈계의 변수(x(t)와 x'(t))와 각각 더해주어 각각 주혼돈계와 종속혼돈계로 되먹임시키면, 두 혼돈계는 서로 동기화되어 대응되는 변수들끼리는 똑같은 궤적을 그리게 된다. 이러한 방법으로 두 혼돈계가 서로 동기화되는 것이 종래기술에서의 혼돈시스템의 동기화기술이다.

<28> 종래의 발명에서는 이 방법을 이용하여 주 혼돈계의 혼돈시스템에서 나오는 신호에 정보신호를 더하여 잡음신호와 함께 송신하고, 종속 혼돈계에서는 이 신호를 받아 잡음신호는 두 혼돈시스템을 동기화시키는데 사용하고 동기화된 종속 혼돈계의 신호와 주 혼돈계의 신호와의 차는 정보신호가 됨으로 이러한 혼돈 시스템을 정보신호를 암호화하고 복호화하는 통신 시스템에 적용하고 있다. 그러나 이러한 통신 시스템은 혼동의 차원이 낮아 잡음신호의 차이가 크게 나더라도 이를 쉽게 정보신호를 복원할 수 있기 때문에 외부에서의 공격에 매우 취약하여 보안성과 안정성이 떨어지는 문제점을 안고 있다.

<29> 또한, 혼돈시스템을 제어하여 동기화시키기 위한 종래 기술로는 국내등록특허공보 제0312035호 '혼돈시스템의 동기화방법 및 이를 이용한 비밀통신방법'이 있으며, 이는 잡음, 혼돈신호를 주혼돈계의 여러 계수값과 이에 대응하는 종속혼혼돈계의 여러 계수값에 각각 더하여 변조시킴으로써 각 변수들의 변화가 일치되어 동기화가 이루어진다.

<30> 상기 종래기술을 도시된 도2를 중심으로 설명하면 다음과 같다.

<31> 동일한 두 혼돈장치가 하나의 혼돈시스템을 형성하고 있을 때, 한 혼돈장치가 주 혼돈장치(130)이고, 다른 혼돈장치가 종속 혼돈장치(150)이며, 주 혼돈장치(130)와 종속 혼돈장치(150)를 동기화시키기 위한 제 1 및 제 2 동기화부(140,160)로 구성된다.

<32> 여기서, 제 1 동기화부(140)는 주 혼돈장치(130)와 종속 혼돈장치(150)를 동기화시키기 위하여 잡음 혹은 혼돈신호(f(t))를 일정의 스케일링(scaling) 계수(α)로 스케일링하는 제 1 스케일링부(41)와, 제 1 스케일링부(141)에서 스케일링된 잡음 혹은 혼돈신호(αf(t))와 주혼돈장치(130)로부터의 임의의 한 변수($x_1(t)$)의 계수(예를들면, λ_1)에 가산하는 제 1 가산기(142)로 구성된다.

<33> 또한, 제 2 동기화부(160)는 주 혼돈장치(130)와 종속 혼돈장치(150)를 동기화시키기 위하여, 잡음 혹은 혼돈신호(f(t))를 제 1 동기화부(40)의 스케일링 계수와 동일한 스케일링 계수(α)로 스케일링하는 제 2 스케일링부(161)와, 제 2 스케일링부(161)에서 스케일링된 잡음 혹은 혼돈신호(αf(t))와 주 혼돈장치(130)로 부터의 임의의 계수(λ_1)를 갖는 변수($x_1(t)$)에 대응되는 종속 혼돈장치(150)의 변수($x_1'(t)$)가 가지는 계수(λ_1)를 가산하는 제 2 가산기(162)로 구성된다.

<34> 여기서, 잡음신호는 혼돈신호가 아닌 일반적 잡음신호이고, 또 다른 혼돈신호는 주 혼돈장치(130)와 종속 혼돈장치(150)가 아닌 새로운 혼돈장치에서 만들어지는 혼돈신호이다.

<35> 이때, 두 혼돈장치(130, 150)를 동기화시키기 위하여 두 혼돈장치(130, 150)에서 서로 대응되는 한 종류의 변수(예컨대, 여기서 $x_1(t)$와 $x_1'(t)$) 혹은 그 이상의 변수들을 택해 그 변수들의 계수(여기서, λ_1)에 동일한 잡음 혹은 혼돈신호(f(t))를 주 혼돈장치(30)의 계수(λ_1)와, 종속 혼돈장치(150)의 계수(λ_1)에 각각 더해 준다.

<36> 여기서, 잡음 혹은 혼돈신호(f(t))의 크기를 α배로 스케일링하여 두 혼돈계의 계수(λ_1)에 각각 더해주어 섭동시키면 두 혼돈계는 서로 동기화가 되어 대응되는 변수들끼리는 똑같은 궤적을 그리게 된다

<37> 즉, 상태변수 x_1, x_2, ... 로 주어지는 주 혼돈계와, 주 혼돈계와 동일한 혼돈계로서 상태변수 x_1',x_2',...로 주어지는 종속 혼돈계가 있을 때, 주 혼돈계와 종속 혼돈계는 대응되는 변수들의 계수가 $\lambda_1, \lambda_2, ...$로 동일하며, 주 혼돈계의 임의의 계수와 이에 대응하는 종속 혼돈계의 임의의 계수에 동일한 잡음 혹은 혼돈신호를 더하여 섭동시키는 것에 의해 두 혼돈계를 동기화시키는 것이 종래의 동기화 기술이다.

<38> 그러나 상기와 같은 종래의 동기화 기술은 계수 값을 비밀키로 사용하였으나 실제는 계수 값의 차이가 웬만큼 커도 실제 신호를 복원할 수 있다. 이는 외부에서의 공격으로 정보 신호를 복원할 수 있다는 것이다. 즉 계수는 시스템에 들어가는 각종 부품들의 조그만 차이가 모여 큰 계수의 차이를 보임으로 이 경우 까지 정보 신호를 복원할려면 외부의 공격에 대하여 제대로 방어하지 못하는 단점이 있다. 그러므로, 이러한 동기화기술을 적용한 통신 시스템은 혼동의 차원이 낮아 잡음신호의 차이가 크게 나더라도 이를 쉽게 정보신호를 복원할 수 있기 때문에 외부에서의 공격에 매우 취약하여 보안성과 안정성이 떨어지는 문제점을 안고 있다.

발명이 이루고자 하는 기술적 과제

<39> 상기의 문제점을 해결하고자 본 발명은 제안된 것으로서, 초기값이 달라 서로 다른 혼돈신호를 만드는 두개의 동일한 혼돈장치에서 각각의 지연시간을 동일한 잡음 혹은 혼돈신호로 각각 변조하여 동일한 두 혼돈장치를 동기화 시키는 혼돈의 동기화장치를 제공함을 목적으로 하고 있다. 또한 동일한 두 혼돈장치가 동일한 지연시간 변조에 의해 서로 동기화되었을 때 한 혼돈장치의 신호에 전보 신호를 더하여 다른 혼돈장치에 전송하고 이를 수신한 다음 혼돈장치는 자신의 혼돈 신호와 비교하여 정보 신호를 복원하는 통신장치를 제공하는 것을 목적으로 하고 있다.

발명의 구성 및 작용

<40> 상기의 목적을 이루기 위하여 혼돈시스템의 동기화 장치는, 소정의 혼돈계에 따른 변수들이 함수적으로 서로 연결되어 혼돈특성을 갖는 적어도 하나 이상의 혼돈신호를 발생하는 주혼돈장치(210)와, 상기 주혼돈장치(210)와 동일하게 구성되며, 상기 주혼돈장치(210)가 발생하는 혼돈신호에 대응되는 혼돈신호를 발생하는 종속혼돈장치(310)로 이루어진 혼돈시스템에 있어서, 변조신호를 발생하는 변조신호발생수단(400)과, 상기 주혼돈장치(210)로부터 발생되는 혼돈신호를 시간지연시키는 제1시간지연수단(220)과, 상기 시간지연된 혼돈신호를 상기 변조신호발생수단(400)에서의 변조신호로 상기 제1시간지연수단(220)에서 출력되는 지연시간을 변조하는 제1지연시간 변조수단(230)과, 상기 종속혼돈장치(310)로부터 발생되는 혼돈신호를 시간지연시키는 제2시간지연수단(320)과, 상기 시간지연된 혼돈신호를 상기 변조신호발생수단(400)에서의 변조신호로 상기 제2시간지연수단(320)에서 출

력되는 지연시간을 변조하는 제2지연시간변조수단(330)과, 상기 제1지연시간변조수단(230)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치(210)로 되먹임하는 제1동기화수단(240)와, 상기 제2지연시간변조수단(330)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치(310)로 되먹임하는 제2동기화수단(340)로 이루어지는 것을 특징으로 한다.

<41> 또한, 상기의 목적을 이루기 위하여 혼돈시스템의 암호화 장치는, 소정의 혼돈계에 따른 변수들이 함수적으로 서로 연결되어 혼돈특성을 갖는 적어도 하나 이상의 혼돈신호를 발생하는 주혼돈장치(210)와 변조신호를 발생하는 변조신호발생수단(400)과 상기 주혼돈장치(210)로부터 발생되는 혼돈신호를 시간지연시키는 제1시간지연수단(220)과 상기 변조신호발생수단(400)에서의 변조신호로 상기 제1시간지연수단(220)에서 출력되는 지연시간을 변조하는 제1지연시간변조수단(230)과 상기 제1지연시간변조수단(230)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치(210)로 되먹임하는 제1동기화수단(240)와 상기 제1지연시간변조수단(230)에서 출력되는 변조된 지연시간과 외부로부터 입력되는 정보신호를 가산하여 암호화 하는 암호화수단(250)과 상기 암호화수단(250)을 통해 출력되는 신호를 무선 또는 유선으로 전송하는 암호송신수단(270)과 변조신호를 송신하는 변조신호송신수단을 포함하는 것을 특징으로 한다.

<42> 또한, 상기의 목적을 이루기 위하여 혼돈시스템의 복호화 장치는, 암호화 신호를 수신하는 암호수신수단(370)과 변조신호를 수신하는 변조신호수신수단(360)과 주혼돈장치(210)와 동일하게 구성되며, 상기 주혼돈장치(210)가 발생하는 혼돈신호에 대응되는 혼돈신호를 발생하는 종속혼돈장치(310)와 상기 종속혼돈장치(310)로부터 발생되는 혼돈신호를 시간지연시키는 제2시간지연수단(320)과 상기 수신된 변조신호로 상기 제2시간지연수단(320)에서 출력되는 지연시간을 변조하는 제2지연시간변조수단(330)과 상기 제2지연시간변조수단(330)으로부터 변조된 지연시간을 상기 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치(310)로 되먹임하는 제2동기화수단(340) 상기 지연시간변조수단에서 출력된 지연시간과 상기 암호수신수단(370)를 통해 수신된 암호화신호와의 차이를 구하여 정보신호를 복호화 하는 복호화수단(350)으로 이루어지는 것을 특징으로 한다.

<43> 이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명한다.

<44> 도 3은 본 발명에 따른 혼돈 시스템의 동기화 장치이다.

<45> 동일한 두 혼돈장치가 있을 때 한 혼돈장치를 주혼돈장치(210)라 하고 다른 혼돈장치를 종속혼돈장치(310)라고 한다. 여기서 두 혼돈장치는 동일한 임의의 변수들을 가지고 있는데 주혼돈장치(210)의 변수들은 x(t) , y(t) , z(t) , ... 이고 종속혼돈장치(310)의 변수들은 x'(t), y'(t), z'(t) , ... 이다. 여기서 두 혼돈장치는 초기 값에 매우 민감하기 때문에 서로 초기 값이 다르면 두 혼돈장치는 서로 동기화되지 않고 각각 움직이므로 서로 같은 변수라도 그 궤적은 서로 매우 다르다. 이것을 나비효과라 하는데 여기서 주혼돈장치(210)와 종속혼돈장치(310)에서 서로 대응되는 변수들은 모두 서로 다른 궤적으로 움직이고 있다. 이때 각 혼돈장치는 서로 대응되는 변수뿐 만 아니라 혼돈이 생길 수 있는 똑 같은 계수를 가지고 있으며 동일한 혼돈계라 함은 대응되는 계수들 끼리는 서로 똑 같은 값을 가진다.

<46> 이때 두 혼돈계에서 서로 대응되는 변수를 골라 동일한 지연 시간 만큼 시간 지연 시킨 후 두 혼돈계에 각각 되먹인다. 예를 들어 두 혼돈계에서 서로 대응되는 y(t) 와 y'(t)를 일정 시간 τ만큼 시간 지연 시킴 후 되먹이면 두 혼돈계는 다음의 변수 들로 이루어진 혼돈계로 재구성 할 수 있는데 그러면 주혼돈계의 변수들은 x(t), y(t), z(t), y(t-τ).....가 되고 종속혼돈계의 변수들은 x'(t), y'(t), z'(t), y'(t-τ)....가 된다. 잡음이나 혼돈 신호로 지연 시간 τ를 동일하게 서로 변조시키면 동일한 상기 두 혼돈계를 동기화 시킬 수 있다.

<47> 도3으로부터 상세하게 설명하면, 변조신호발생수단(400)은 변조신호를 발생하게 되는데, 변조신호는 주기적 신호, 혼돈신호, 난수신호, 잡음신호 등을 포함한다. 제1시간지연수단(220)은 상기 주혼돈장치(210)로부터 발생되는 혼돈신호를 시간지연시키며, 제1지연시간변조수단(230)은 변조신호발생수단(400)에서의 변조신호로부터 제1시간지연수단(220)에서 출력되는 지연시간을 변조하게된다. 제1지연시간변조수단(230)으로부터 변조된 지연시간은 제1동기화수단(240)에서 주혼돈장치(210)로부터 발생하는 적어도 하나 이상의 혼돈신호에 부가하여 상기 주혼돈장치(210)로 되먹임하게 된다.

<48> 또한 제2시간지연수단(320)은 종속혼돈장치(310)로부터 발생되는 혼돈신호를 시간지연시키며, 변조신호발생수단(400)에서의 변조신호로부터 제2지연시간변조수단(330)이 제2시간지연수단(320)에서 출력되는 지연시간을 변조하게된다.

<49> 상기 제2지연시간변조수단(330)으로부터 변조된 지연시간은 제2동기화수단(340)에서 상기 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 상기 종속혼돈장치(310)로 부터 발생하는 혼돈신호에 부가하여 상기 종속혼돈장치(310)로 되먹임하게 된다.

<50> 이때, 제1동기화수단(240)는 주혼돈장치(210)의 임의의 혼돈신호를 제1스케일링 계수로 스케일링하는 제1스케일링부(242)와, 제1지연시간변조수단(230)의 변조된 지여시간으로부터 스케일링된 주혼돈장치(210)의 혼돈신호를 감산하는 감산기(241)와 감산기(241)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(243)와 제2스케일링부(243)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호를 가산하여 상기 주혼돈장치(210)로 되먹임하는 가산기(244)로 이루어진다.

<51> 또한, 제2동기화수단(340)는 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 제1스케일링 계수로 스케일링하는 제1스케일링부(342)와 제2지연시간변조수단(330)의 변조된 지연시간으로부터 스케일링된 상기 종속혼돈장치(310)의 혼돈신호를 감산하는 감산기(341)와 감산기(341)의 출력신호를 제2스케일링 계수로 스케일링하는 제2스케일링부(343)와 제2스케일링부(343)에서 출력되는 신호와 상기 주혼돈장치(210)의 임의의 혼돈신호에 대응하여 종속혼돈장치(310)로 부터 발생하는 혼돈신호를 가산하여 종속혼돈장치(310)로 되먹임하는 가산기(344)로 이루어진다.

<52> 이러한 동기화 방법을 수식적으로 설명하면 처음 외부의 임의의 잡음 혹은 혼돈 신호의 크기를 적당히 스케일링하여서 β배하여 이 신호로 주혼돈장치(210)와 종속혼돈장치(310)의 시간 지연 신호의 지연 시간을 각각 변조시키면 두 혼돈장치는 서로 동기화 되어 서로 대응되는 변수들 끼리는 똑같은 궤적을 그리게 된다. 즉 동기화가 일어나면 x(t) = x'(t), y(t) = y'(t), z(t) = z'(t), ... 와 같이 된다. 이를 수식으로 표현하면 다음과 같이 된다.

<53> 주혼돈계 종속혼돈계

<54> $\dot{x}$ = f(x, y, z, ...) $\dot{x'}$ = f(x', y', z', ...)

<55> $\dot{y}$ = g (x, y, z, ...) $\dot{y'}$ = g(x', y', z' , ...)

<56> $\dot{z}$ = h (x, y, z, ...) $\dot{z'}$ = h(x', y', z', ...)

<57> ....

<58> 여기서 앞의 설명처럼 임의의 신호 ξ(t) 를 이용하여 각각의 혼돈장치의 되먹임 신호의 지연 시간을 변조하여 두 혼돈장치를 서로 동기화시키는 것을 수식으로 표현하면 다음과 같이 된다.

<59> 주혼돈계 종속혼돈계

<60> $\dot{x}$ = f(x, y+α[y(t-τ)-y], z ,...) $\dot{x'}$ = f(x', y'+α[y'(t-τ)-y'], z' ,...)

<61> $\dot{y}$ = g(x, y+α[y(t-τ)-y], z ,...) $\dot{y'}$ = g(x', y'+α[y'(t-τ)-y'], z' ,...)

<62> $\dot{z}$ = h(x, y+α[y(t-τ)-y], z ,...) $\dot{z'}$ = h(x', y'+α[y'(t-τ)-y'], z' ,...)

<63> ....

<64> $\tau = \tau_0 + \xi(t)$

<65> 여기서 두 혼돈장치는 ξ(t)의 진폭에 따라 혹은 주파수에 따라 두 혼돈장치가 서로 동기화 되는 조건을 구할 수 있다. 이것은 일반화된 동기화의 얼개와 비슷하게 두 혼돈장치가 서로 동기화된다. 이때 똑 같은 잡음 혹은 혼돈 신호 혹은 주기적 신호로 동일한 두 혼돈계의 시간지연 되먹임 변수의 지연 시간을 변조시킬 때 두 혼돈계가 서로 동기화가 되는 것이 본 발명에 따른 혼돈장치의 동기화 방법이다.

<66> 이 혼돈계에서 동기화 현상을 분석하기 위해 간단한 로지스틱 맵(logestic map)을 이용하여 분석하면 쉽게 알

수 있다. 로지스틱 맵(logestic map)은 다음의 식으로 주어지게 된다.

<67> $y_{n+1} = A y_n(1 - y_n)$

<68> 이 식 A의 값에 따라 다양한 주기배가 갈래질(periodic doubling bifurcation)과 혼돈이 생기는데, 예를 들어 A가 0 에서 1사이의 값을 가지면 x_n 의 값은 0이며, A가 1과 3 사이의 값을 가지면 x_n 은 1-1/A의 값을 가지며, A가 3과 3.75사이의 값을 가지면 2개의 안정점이 생기며, 이 2개의 안정점은 A의 값의 증가에 따라 4개의 안정점, 8개의 안정점 등으로 나누어지게 되고, 결국 혼돈에 이르게 되는데 A가 3.8 정도에서는 완전한 혼돈이 생기게 된다. 이때 A = 4.0으로 고정시킨 뒤 나오는 y_n의 신호로 두 로지스틱 혼돈계 인 주혼돈계 $x_n = \Lambda x_n(1-x_n)$ 와 동일한 종속혼돈계 $x_n' = \Lambda x_n'(1-x_n')$ 를 각각 시간 지연 변수로 되먹임 시킬 때 지연 시간을 임의의 난수로 변조시켜 두 혼돈계를 동기화 시키는 방법을 분석해보면 다음과 같다.

<69> 로지스틱 맵(logistic map)에서 시간 지연 변수를 되먹임 시키면 그 식은 다음과 같이 된다.

<70> $$x_{n+1} = \gamma \overline{x_n}(\tau)(1-\overline{x_n}(\tau))$$, : 주혼돈장치(210)

<71> $$x'_{n+1} = \gamma \overline{x'_n}(\tau)(1-\overline{x'_n}(\tau))$$, : 종속혼돈장치(310)

<72> 여기서 $\overline{x}_n(\tau) = (1-\alpha)x_n + \alpha x_{n-\tau}$ 이고 α는 결합 상수, τ는 지연 시간으로 $\tau=[\Lambda y_n]$으로 두었다. Λ는 지연 시간의 진폭이고 로지스틱 맵에서의 지연 시간은 정수이기 때문에 $[\Lambda y_n]$은 Λy_n 보다 작은 정수 중 가장 큰 정수를 택했다. 그러면 Λ 값에 따라 지연 시간이 바뀌게 되는 지연 시간을 변조의 폭을 조절할 수 있다. 이러한 시간 지연 변조에 의하여 동일한 두 혼돈계는 초기 값이 서로 다르더라도 지연 시간의 동일한 변조에 의해 두 혼돈계는 동기화 될 수 있는데 이 동기화를 찾는 조건이 두 혼돈장치의 방정식의 해인 조건 랴푸노브(Lyapunov) 지수 혹은 가로 랴푸노브(Lyapunov) 지수라 불리는 값이 음수가 되면 된다. 이 값을 구하면 두 혼돈계가 동기화되는 얼개를 명확히 이해할 수 있다.

<73> 도 4는 로지스틱 맵에 의한 혼돈시스템의 분석 그래프이다.

<74> 도 4는 r=3.5 와 Λ=60일 때의 혼돈 신호이다. 도 4(a)는 τ의 지연 시간의 시간적 변화를 보여주고 도 4(b)는 α=0.7일 때 x_n 신호이고, 도 4(c)는 α= 0.8일 때 x_n 의 신호 이다. 이때 동기화가 일어나는지를 확인하기 위해서는 두신호의 차이값을 구해보면, 다음과 같다. 도 4(d)는 α = 0.7일 때 x_n-x'_n의 값이고 도 4(e)는 α = 0.8일 때 x_n-x'_n의 값이다. 도 2(d)와 2(e)의 차이값 분포를 살펴 보면, α = 0.7일 때는 두 혼돈 시스템은 동기화 되지 않으나, α = 0.8일 때는 주 혼돈계와 종속 혼돈계가 서로 동기화 됨을 알 수 있다.

<75> 도 5는 혼돈 시스템을 차분방정식으로 모델링하여 구한 해를 도시한 그래프이다.

<76> 혼돈시스템의 동기화를 을 정확히 이해하기 위해서는 두 혼돈계의 차로 만들어지는 새로운 혼돈계를 정의하고 이 혼돈계의 조건 랴푸노브(Lyapunov) 지수를 구하면 된다. 그러면 두 변수의 차이$x_n - x_n' = \Delta x_n$ 이라 두면 두 혼돈계의 차이 식은 다음의 식으로 쓸 수 있다.

<77> $$x_{n+1} = \gamma \overline{x_n}(\tau)(1-\overline{x_n}(\tau))$$, : 주혼돈계

<78> $\Delta x_{n+1} = J_n \Delta x_n + K_n$,

여기서, $J_n = (1-\alpha)\gamma(1-(\overline{x_n}(\tau)+\overline{x'_n}(\tau)))$ 이고,

<79> 삭제

<80> $$K_n = \alpha\gamma(1-(\overline{x_n}(\tau)+\overline{x'_n}(\tau)))(x_{n-\tau}-x'_{n-\tau})$$ 이다.

<81> 이 식은 새로운 비선형 차분 방정식의 꼴이 된다. 그런데 이 식을 보면 먼저 J_n은 쟈코비안이고 K_n은 잡음처럼 더해진 항이다. 이런 차분 방정식에서는 조건 랴푸노브 지수 값을 구해야 동기화의 조건을 구할 수 있다. 이 수식을 이용하여 조건 랴푸노브 값을 되먹임되는 세기에 따라 구했는데 이것을 보여주는 그림이 도 5이다. 도 5(a)는 조건 랴푸노브 지수의 값 λc를 Λ와 α에 따라 3차원 적으로 그린 것이다. 여기서 회색 지역이 조건 랴푸노브 지수가 음인 지역이고, 흰색 부분이 조건 랴푸노브 지수가 양인 지역이다. 조건 랴푸노브 지수가 음인 지역이 동기화가 일어나는 지역이다. 도 5(b)는 최대 랴푸노브 지수 λm을 Λ와 α 따라 그린 것으로 회색 지역은 그 지수의 값이 양으로 나타나 혼돈이 일어나는 영역을 뜻하고, 검은 영역은 그 지수가 음이 되어 주기적 신호가 생기는 영역을 말한다. 두 도면을 보면 최대 리야푸노프 지수가 양이어서 혼돈 신호가 생길 때 조건 리야푸노프 지수는 음이되어 혼돈이 동기화되는 영역이 있음을 보여 준다.

<82> 도 6은 동기화영역과 차분방정식으로 모델링하여 구한 해의 관계를 그린 그래프이다.

<83> 동기화영역과 조건 Lyapunov 지수를 더 자세히 나타낸 것이 도 6이다. 도 6(a)는 동기화 영역을 Λ와 α공간에서 그린 것이다. 이 도면을 보면 회색 영역이 동기화 영역이며, 난수로 지연 시간을 변조시킬 때는 그 영역이 더 넓어짐을 볼 수 있다. 도 6(b)는 조건 리야푸노프 지수로 α의 값에 따라 구한 것이다. 윗 쪽 선은 Λ=60일 때이고 아래 선은 Λ=40 일 때이다. 이 도면을 보면 조건 랴푸노브 지수가 음일 때 도 6(a)의 동기화 영역이 일치하는 것을 잘 볼 수 있다.

<84> 도 7은 본 발명에 따른 혼돈 시스템의 통신 장치이다. 이는 혼돈시스템의 동기화장치를 통신장치에 적용하였을 때의 블록 다이어그램이다.

<85> 도 7에 의하면 변조신호발생수단(400)의 변조신호를 이용하여, 주혼돈장치(210)와 종속혼돈장치(310)에서의 시간지연수단에 의한 지연 시간을 변조시켜서, 동기화수단에 의해 되먹임하면 두 혼돈장치는 동기화 된다. 이상은 시간지연 변조에 의한 혼돈시스템의 동기화장치에서 충분히 설명된 바와 같다. 이 때 상기 주혼돈장치(210)의 제1지연시간변조수단(230)에서 출력되는 혼돈신호에 정보 신호를 더해주는 암호화수단(250)을 거쳐 혼돈 신호에 정보 신호가 더해지면, 암호송신수단(270)에 의해 이 신호를 송신하고, 또한 변조신호송신수단(260)에 의해 변조신호도 함께 송신된다. 변조신호 수신장치에서 변조신호를 수신받고, 수신단에서는 암호화 신호를 수신받으며, 제2지연시간변조수단(330)은 수신된 변조신호로부터 제2시간지연수단(320)에서 출력되는 지연시간을 변조하게 된다. 제2동기화수단(340)는 제2지연시간변조수단(330)으로부터 변조된 지연시간을 주혼돈장치(210)로부터 발생하는 임의의 한 혼돈신호에 대응하여 종속혼돈장치(310)로부터 발생하는 혼돈신호에 부가하여 종속혼돈장치(310)로 되먹임하게되며, 종속혼돈장치(310)에서 발생하는 하나의 혼돈신호로부터 수신 신호와의 차이를 구하는 복호화수단(350)을 거치면 정보신호가 복원된다.

<86> 혼돈시스템의 통신장치는 두 혼돈장치가 서로 동기화 되었을 때 주혼돈장치(210)의 임의의 변수를 마스킹신호로 쓰고, 그 마스킹 신호에 주혼돈장치(210)의 혼돈 신호의 전력 스펙트럼(power spectrum)보다 훨신 작은 음성 신호를 섞어서, 잡음이나 또다른 혼돈 신호와 함께 보내면 종속혼돈장치(310)의 수신단에서 이 두 신호를 받아서 잡음이나 또 다른 혼돈 신호를 동기화 신호로 쓰고, 종속혼돈계에서 나오는 신호를 구하여 수신된 신호와의 차이를 구하면 원래의 정보 신호가 복원되는 것이다. 이것은 정보 신호에 관계없이, 주혼돈장치와 종속혼돈장치가 서로 동기화 되면 두 혼돈장치는 서로 완전히 일치한다는 조건 때문에 생기는 것이다. 이것은 두 혼돈 시스템이 동기화 되었을 때 비밀통신의 일반적 방법이다. 이것은 앞에서도 설명하였지만 송신 신호는 고차원의 혼돈 신호이고 지연 시간을 파악할 수 없으므로 외부에서의 공격이 어려운 반면, 본 발명의 동기화 장치를 쓰면 혼돈 신호 속에 감춰진 정보 신호를 쉽게 복원해 낼 수 있는 것이다. 그래서 이러한 동기화장치는 암호화, 복호화에 유용하게 응용할 수도 있다.

이상에서 살펴본 바와 같이, 본 발명의 바람직한 실시예에 대해 상세히 기술되었지만, 본 발명이 속하는 기술분야에 있어서, 통상의 지식을 가진 사람이라면, 첨부된 청구 범위에 정의된 본 발명의 정신 및 범위를 벗어나지 않으면서 본 발명을 여러 가지로 변형하여 실시할 수 있을 것이다. 따라서 본 발명에 대한 앞으로의 실시예들의 변경은 본 발명의 기술을 벗어날 수 없을 것이다.

<87> 삭제

발명의 효과

<88> 상기에서 설명한 바와 같이 본 발명에서는, 초기값이 달라 서로 다른 혼돈신호를 만드는 두개의 동일한 혼돈장

치에서의 지연시간을 동일한 잡음 혹은 혼돈신호로 각각 변조하여 동일한 두 혼돈장치를 동기화 시키는 혼돈시스템의 동기화장치과 이를 적용한 통신장치를 제공하며, 이때 본 발명의 혼돈장치에서 나오는 혼돈신호는 지연시간 변조에 의해 매우 무질서하기 때문에 실제로 외부에서의 공격에 대해서도 매우 높은 보안성과 안정성을 유지하는 효과가 있다. 또한 시간 지연을 변조함으로 인해 혼돈시스템의 차원이 높아 쉽게 분석하지 못하므로 이상적인 혼돈 동기화 시스템으로 비밀 통신에 적용할 수 있는 효과가 있다.

도면의 간단한 설명

<1> 도 1은 종래 발명에 있어서의 혼돈 시스템의 동기화 장치의 일례이다.

<2> 도 2는 종래 발명에 있어서의 혼돈 시스템의 동기화 장치의 또다른 일례이다.

<3> 도 3은 본 발명에 따른 혼돈 시스템의 동기화 장치이다.

<4> 도 4는 로지스틱 맵에의한 혼돈시스템의 분석 그래프이다.

<5> 도 5는 혼돈 시스템을 차분방정식으로 모델링하여 구한 해를 도시한 그래프이다.

<6> 도 6은 동기화영역과 차분방정식으로 모델링하여 구한 해의 관계를 그린 그래프이다.

<7> 도 7은 본 발명에 따른 혼돈 시스템의 통신 장치이다.

<8> *도면의 주요 부분에 대한 부호의 설명*

<9> 210: 주혼돈장치 220: 제1시간지연수단

<10> 230: 제1지연시간변조수단 240: 제1동기화수단

<11> 310: 종속혼돈장치 320: 제2시간지연수단

<12> 330: 제2지연시간변조수단 340: 제2동기화수단

<13> 250: 암호화수단 350: 복호화수단

<14> 241, 341: 감산기 244, 344: 가산기

<15> 242, 342:제1스케일링부 243, 343:제2스케일링부

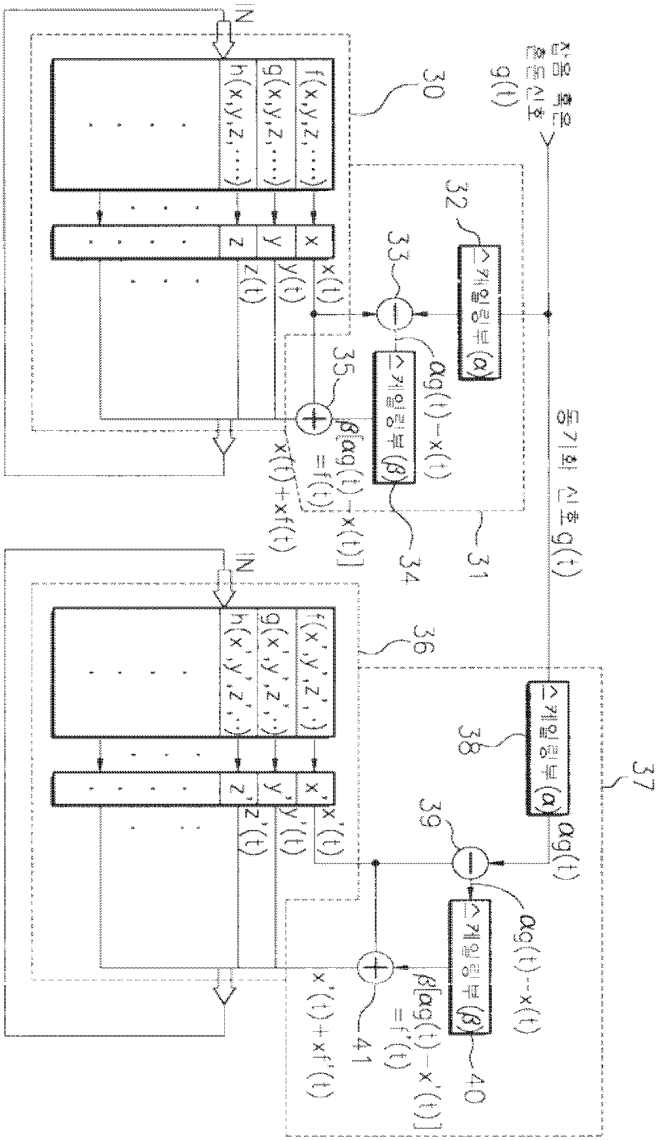
<16> 260: 변조신호 송신수단 360: 변조신호수신수단

<17> 270: 암호송신수단 370: 암호수신수단

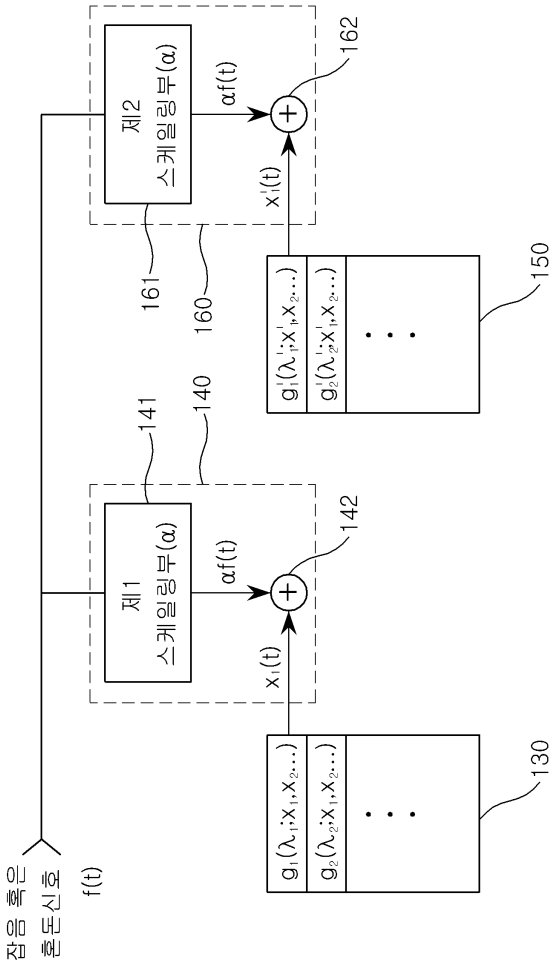
<18> 400; 변조신호발생수단

도면

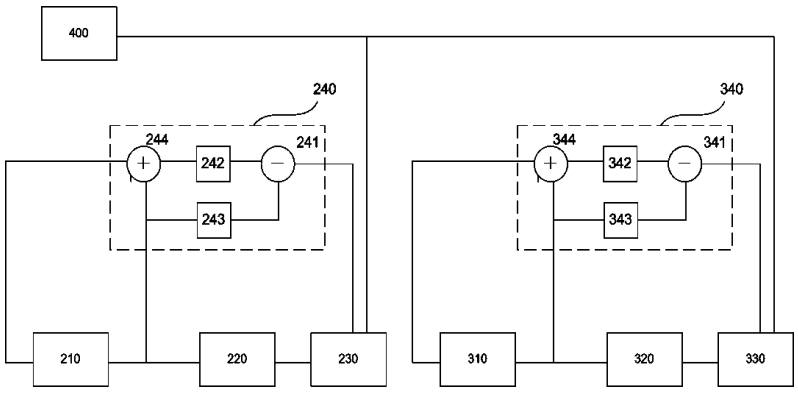
도면1


입력 동영상 g(t)
동기화 신호 g(t)
30
31
32
33
34
35
36
37
38
39
40
41
IN
f(x,y,z,....)
g(x,y,z,....)
h(x,y,z,....)
x(t)
y(t)
z(t)
αg(t)
αg(t)-x(t)
β[αg(t)-x(t)]
=f(t)
x(t)+xf(t)
f'(x',y',z',.)
g(x',y',z',.)
h(x',y',z',.)
x'(t)
y'(t)
z'(t)
αg(t)--x(t)
β[αg(t)-x'(t)]
=f'(t)
x'(t)+xf'(t)

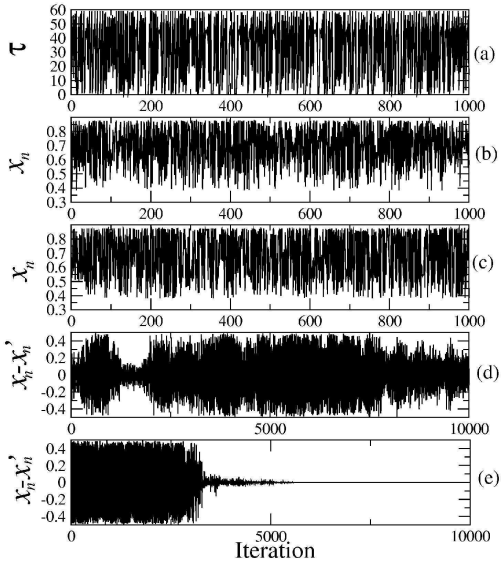
도면2


제2 스케일링부(α)
αf(t)
x'(t)
162
161
160
150
141
140
제1 스케일링부(α)
142
x(t)
130
잡음 혹은 혼돈신호
f(t)

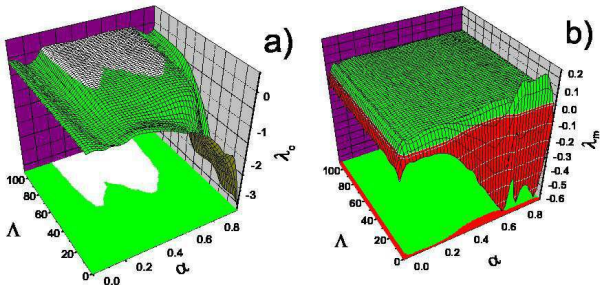
도면3


400
240
244
242
241
243
340
344
342
341
343
210
220
230
310
320
330

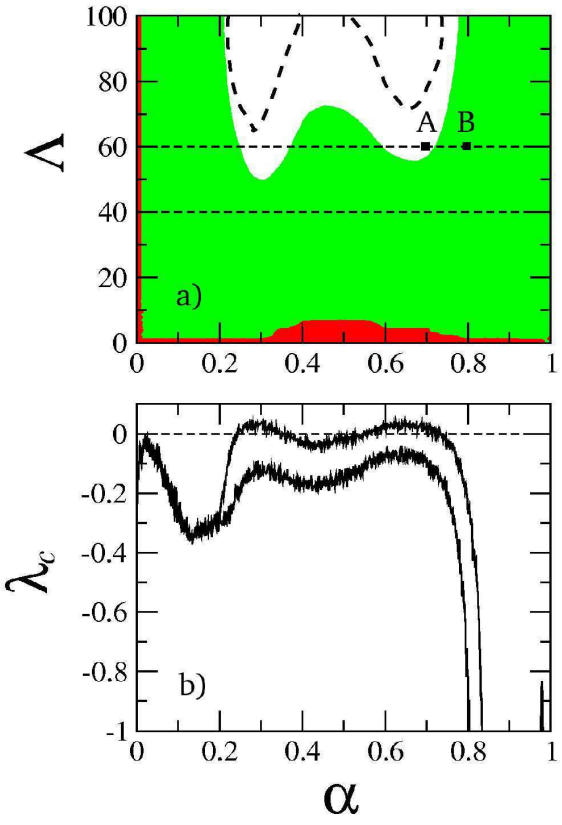
도면4



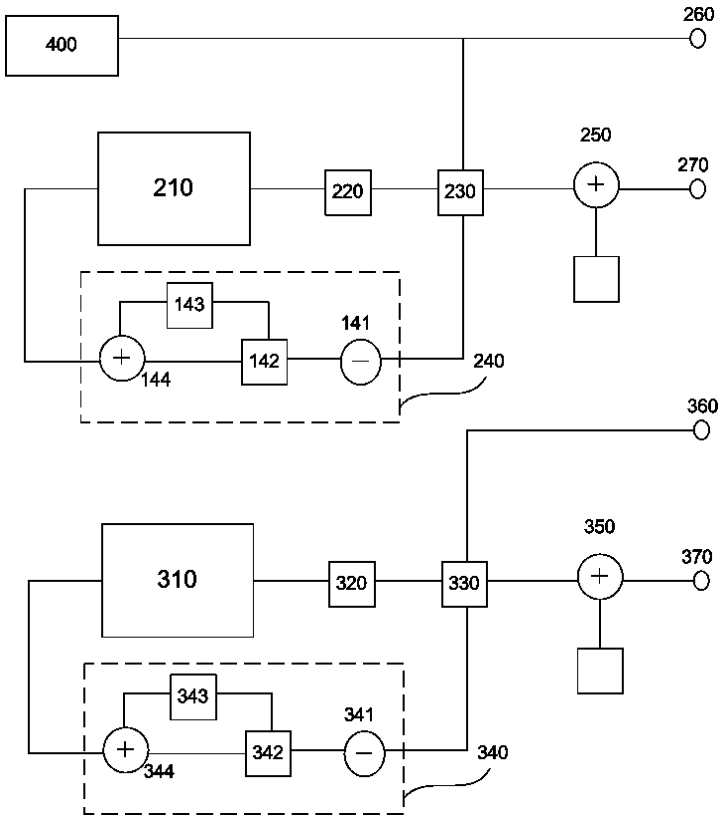
도면5



도면6


100
80
60
40
20
0
Λ
A
B
a)
0
0.2
0.4
0.6
0.8
1
0
-0.2
-0.4
-0.6
-0.8
-1
λc
b)
α

도면7


400
260
210
220
230
250
270
143
141
142
144
240
360
310
320
330
350
370
343
341
342
344
340