應用模糊混沌同步與國際數據加密演算法之密碼系統
Cryptology Using Fuzzy Chaos Synchronization and International Data Encryption Algorithm

余國瑞
義守大學電機研究所
gwoyu@isu.edu.tw

吳東軒
義守大學電機研究所
thalin@ms48.hinet.net

摘要

本文應用國際數據加密演算法，設計以混沌訊號為基礎之對稱密碼系統。明文訊號被後勤映射遮蔽後，密文訊號經由混沌同步可還原成原始訊號。由於模糊控制具有強健性，可抑制傳送端與接收端初始值不同與系統參數變動之影響，因此本文以模糊邏輯設計觀測器增益，使傳送端與接收端之後勤映射系統同步。最後以國際數據加密演算法結合混沌同步設計，架構後勤映射密碼系統，並應用於語音訊號與圖像加密。電腦模擬顯示，基於密碼學與混沌遮蔽之加密系統，可提升資訊安全性能。

關鍵詞：混沌同步，國際數據加密演算法，模糊邏輯。

Abstract

In this paper, the international data encryption algorithm is applied to design the symmetric cryptosystem based on chaotic signals. Plain text are masked by means of the logistic map. Cipher text could be recovered to the original signals through chaos synchronization. Since the fuzzy controller is robust, it can restrain effects of different initial values and variant system parameters between the transmitter and the receiver. To synchronize the logistic map between the transmitter and the receiver, hence the observer gain is designed using fuzzy logic. At last, the logistic map cryptosystem are structured by combining the international data encryption algorithm and chaos synchronization and applied to the encryption of voice and picture. Computer simulations demonstrate that the cryptosystem based on cryptography and chaotic masking could promote the performance of information security.

Keywords：chaos synchronization, international data encryption algorithm, fuzzy logic.

一、緒論

由於電腦網路技術的蓬勃發展和廣泛應用，使得資訊流通與存取更為快速與便捷。諸如無線行動通訊網路、政府行政數位 *e* 化、金融機構電子交易、民間企業電子商務等，均已將網路技術應用於實務上，因此資訊安全非常重要 [4]。密碼系統可對資訊安全提供下列功能：(1) 秘密性：主要為防止竊密者竊取明文訊號。(2) 完整性：使傳送之明文訊號不會遭破密者竄改。(3) 可鑑性：確保明文訊號是由傳送端所發送，而非他人偽造傳送 [3]。資訊安全為相當複雜之研究課題，但多以編碼技術為重要核心，透過加密傳輸來確保資訊安全。故本研究將應用模糊邏輯理論，開發以混沌信號為基礎之對稱密碼系統，提升國際數據加密演算法之安全。

混沌信號為高度非線性動態系統，具有寬頻功率頻譜、週期無限、軌跡難以估測、及易從非線性電路中產生等特性 [14]，因此混沌系統常被使用於資料之保密。混沌信號於資訊安全之應用方法包括 (1) 混沌遮蔽（Chaotic Masking）[15]:使用混沌信號對傳輸資料進行遮蔽。在傳送端將原明文訊號加於混沌信號之中，以遮蔽其原來資料之型態，在接收端將資料減去原先之混沌信號，即可還原明文訊號。(2)混沌切換（Chaotic Switch） [13]:將混沌參數針對不同吸子（attractor），進行位元編碼與交換。(3)混沌調變（Chaotic Modulation） [5]:混沌訊號之系統參數依傳送訊號而變動，於接收端則利用卡曼濾波器將資料回復。Chua 首先將混沌同步應用於通訊安全，並且以非線性電路實現 [10]。本文以後勤映射混沌訊號應用於密碼系統，在傳送端將明文訊號與離散混沌訊號作遮蔽，送至接收端予以解調，使資料在傳遞過程中具有保密及回復的特性。由於混沌系統於初始值微小變化時，會呈現不同混沌現象 [8]，所以對傳送端及接收端之混沌系統參數無法完全相同時，仍保有同步之效果為重要研究課題。故本文以模糊控制器具強健性之優

點 [11]，設計混沌同步觀測器。

此外，本文將結合密碼學金匙之觀念，架構混沌同步密碼系統，提升資訊安全性能。現有的秘密金匙密碼系統包括:傳統加密法（換位及替換加密法）、美國資料加密標準（Data Encryption Standard）、快速資料加密演算法（Fast Data Encipherment Algorithm）、國際數據加密演算法（International Data Encryption Algorithm）等 [9]。國際數據加密演算法（IDEA）是由 Lai 及 Massey 於 1990 所發展出來的對稱式區段加密法，使用金匙長度為 128 位元，編碼資料區塊為 64 位元 [6]。近年來 IDEA 已逐漸取代 DES 之傳統加密法，PGP（Pretty Good Privacy）軟體之加解密演算法亦採用 IDEA。因此本文所設計之密碼系統，所使用的加密函數為國際數據加密演算法。

二、模糊混沌同步

混沌系統初始條件有微小差異，會導致混沌行為明顯不同，即混沌系統具有對“初始值敏感依賴”的特性 [1]。1990 年 Pecora 和 Carrol 提出混沌同步的觀念 [2]，以發射端之混沌系統驅動接收端之混沌系統，使之達到相同或近似的混沌現象。近年來，混沌同步應用於通訊安全方面逐漸受到重視，許多研究皆以如何將傳送訊號引入混沌系統以確保安全。本文以後勤映射為混沌系統，定義如下

$$\begin{aligned} x(k+1) &= f_\mu(x(k)) \\ &= \mu\, x(k)(1-x(k)) \end{aligned} \tag{1}$$

其中 $0 \le x(k) \le 1, 0 \le \mu \le 4$，當 μ 介於 3.58 和 4 之間時，混沌現象會愈加明顯。

將兩個完全相同或相似的混沌系統，控制在同步或逐漸穩定於相似之響應，稱之為混沌同步。發射端與接收端之後勤映射系統動態方程式分別為

$$x(k+1) = f_\mu(x(k)) \tag{2}$$

$$\hat{x}(k+1) = f_\mu(\hat{x}(k)) \tag{3}$$

其中初始值 $x(k)$ 與 $\hat{x}(k)$ 並不一定相同，當 $k \to \infty$ 時，狀態誤差 $e(k) = (x(k) - \hat{x}(k)) \to 0$，稱為後勤映射同步。

模糊理論由 Zadeh 教授提出，模擬人類思考決策模式，以模糊邏輯對受控系統加以描述進而控制，現今已經被廣泛的應用於控制、分類及預測等各種領域 [12]。由於傳統控制方法必須依賴明確數學模式之推導與演算，方能對系統進行控制。但非線性、時變性和資訊不完整之系統，不易建構數學模式。而模糊控制運用專家經驗掌握受控系統特性，可作有效控制。當系統參數改變或受外加雜訊干擾時，具較佳之強健性。故本文以模糊邏輯設計觀測器增益，使發射端與接收端之後勤映射系統同步。

模糊控制係以口語式系統運作法則，代替系統精確數學模式之描述，經由系統輸出回授，反覆修正系統誤差，以得到符合要求之控制結果。模糊控制器設計步驟主要包含模糊化、模糊規則庫、模糊推論引擎和解模糊化：

（一）模糊化：由於真實世界中所量測之物理量幾乎為明確值，因此須經由適當之歸數函數將輸入、輸出用模糊變數表示。本文輸入變數為同步誤差 E 和同步誤差變化量 DE，及模糊增益 F 為輸出變數，所使用之歸屬函數為高斯函數。

$$\mu_{A_i}(x) = \exp\left[-(x - m_i)^2 / \sigma_i^2\right] \tag{4}$$

（二）建立模糊規則庫：主要由資料庫和規則庫組成。其中資料庫為提供變數所需之定義，規則庫則以“*if* … ,*than* …”的語意陳述表示，如

Rule 1：*if x is* A_1 *and y is* B_1，*then z is* C_1

Rule 2：*if x is* A_2 *and y is* B_2，*then z is* C_2

：

Rule n：*if x is* A_n *and y is* B_n，*then z is* C_n

其中 A_n、B_n 和 C_n 為分佈於 x、y、z 論域之模糊變數值。

（三）定義模糊推論：模糊推論是模糊控制器設計時之核心，藉由推論進行來模擬人類思考決策模式。推論方式有 Mamdani 和 Sugeno 等數種模式，本文採用 Mamdani 型式之模糊推論，推論公式如下：

$$\mu_{B'}(f) = \max_{l=1}^{m} [\mu_{A_1^l}(e) \wedge \mu_{A_2^l}(de) \wedge \mu_{B^l}(f)] \tag{5}$$

其中 e、de、f 分別代表模糊集合之誤差、誤差變化量、控制輸出，$\mu_{A_1^l}(e)$ 為誤差之歸屬函數、$\mu_{A_2^l}(de)$ 為誤差變化量之歸屬函數、$\mu_{B^l}(f)$ 為控制輸出之歸屬函數，l 為各模糊集

合歸屬函數之指標，m 為觸發之規則數，$\mu_{B'}(f)$為推論結果。

（四）解模糊化：本文採用重心解模糊化法，推導公式為

$$F=\frac{\sum_{i=1}^{m}\mu_{B'}(f_i)\cdot f_i}{\sum_{i=1}^{m}\mu_{B'}(f_i)} \tag{6}$$

其中 i 為推論輸出規則，F 為模糊控制器輸出。

本文所探討之後勤映射為一離散混沌系統，動態方程式亦可描述如下

$$x(k+1)=Ax(k)+f(x) \tag{7}$$

其中 $x(k)\in R$ 為系統狀態，A 為系統參數 μ，$f\in R$ 為非線性函數。經由模糊邏輯推論，設計模糊增益使後勤映射系統達混沌同步之目的。藉由（7）式來驅動另一後勤映射系統，其動態方程式如下

$$\hat{x}(k+1)=A\hat{x}(k)+f(\hat{x})+F\cdot(x(k)-\hat{x}(k)) \tag{8}$$

其中 $\hat{x}(k)$ 是發射端 $x(k)$ 之估測狀態，F 為模糊控制增益值。

由（7）式與（8）式可得狀態誤差

$$e(k)=x(k)-\hat{x}(k) \tag{9}$$

其誤差動態方程式可表示如下

$$e(k+1)=Ae(k)-F\cdot e(k)+f(x)-f(\hat{x}) \tag{10}$$

經由設計模糊控制增益值 F，使得（10）式趨近於穩定，而構成後勤映射同步。

三、密碼系統設計

國際數據加密演算法為一種區塊加密法，運用 128 位元之密鑰對 64 位元之明文訊號連續加密，而產生 64 位元密文區塊 [7]。IDEA 具有優異之混淆性（Confusion）與擴散性（Diffusion），可增加統計分析攻擊之抗性並強化編碼器之雪崩效應。IDEA 的混淆性藉由三種不同函數達成：(1)XOR 運算(2)定義在 2^{16} 的整數同餘加法運算，其運算元皆為非負 16 位元整數(3)定義在 $2^{16}+1$ 的整數同餘乘法運算，其運算元皆為非負 16 位元整數。IDEA 的擴散性藉由乘法／加法（MA）結構提供，運算部分包括兩個加法與兩個乘法四個元素，輸入為兩個 16 位元明文與兩個 16 位元次密鑰，產生兩個 16 位元輸出。此架構在 IDEA 加密系統中，將數據經過八回合之運算處理，可達擴散之特性。

IDEA 加密程序是由八回合的編碼運算與最後一次的輸出轉換函數所組成。將欲加密之訊號變換成 64 位元的明文區塊，在每回合中分成四個 16 位元的輸入區塊，且每回合中有六個不同的子密鑰參與加密過程，最後一次的變換運算則用到另外四個子密鑰。所以 IDEA 加密過程中，共運用了 52 個子密鑰，每一個子密鑰皆由 128 位元的加密密鑰所產生。IDEA 每一回合都具相同之架構，且每一回合加密程序是由兩個部份所組成。第一部份為變換運算，利用乘法與加法運算將四個 16 位元輸入資料與子密鑰結合，再經 XOR 運算產生兩個 16 位元輸出資料區塊。第二部份即為 MA 運算，將兩個 16 位元輸出資料區塊與兩個子密鑰經乘法與加法同餘運算，產生兩個 16 位元輸出區塊。此 MA 運算的輸出區塊再與變換運算的輸出進行 XOR 運算，產生最終四個 16 位元子區塊進入下一回合。經過八回合編碼運算後，IDEA 最後處理步驟為輸出轉換，此部分只包括每回合之變換運算並無 MA 運算，故只需四個子密鑰。

本文引用密碼學中金匙之製作，將混沌同步與國際數據加密演算法結合，以確保資料在通訊過程中之安全性。圖 1 為後勤映射密碼系統架構圖，加密函數為國際數據加密演算法，經由模糊邏輯推論，設計模糊增益使後勤映射系統達混沌同步之目的。首先定義加密和解密函數如下所示

$$p(k)=e_{en}(s(t),K_1(k)) \tag{11}$$

$$s(t)=d(\hat{p}(k),K_2(k)) \tag{12}$$

其中 $e_{en}(\cdot)$ 為 IDEA 加密函數，$d(\cdot)$ 為 IDEA 解密函數。$s(t)$ 為欲傳送之明文訊號，$p(k)$ 為明文加密後之訊號，$\hat{p}(k)$ 為估測之加密訊號。$K_1(k)$ 為加密金匙，$K_2(k)$ 為解密金匙。將加密後之明文訊號藉由後勤映射混沌系統遮蔽，即為公用頻道傳送之訊號

$$x(k+1)=Ax(k)+f(x)+p(k) \tag{13}$$

接收端之後勤映射狀態估測方程式設計如下，使傳送端與接收端有較佳之混沌同步狀態

$$\hat{x}(k+1)=A\hat{x}(k)+f(\hat{x})+F\cdot(x(k)-\hat{x}(k))+G \quad (14)$$

其中 G 為非線性函數，若選取

$$G=f(x)-f(\hat{x}) \quad (15)$$

則同步誤差 $e(k)$ 之動態方程式為

$$\begin{aligned} e(k+1) &= x(k+1)-\hat{x}(k+1) \\ &= Ax(k)+f(x)+p(k) \\ &\quad -(A\hat{x}(k)+f(\hat{x})+F\cdot(x(k)-\hat{x}(k))+G) \\ &= Ae(k)-F\cdot e(k)+p(k) \end{aligned} \quad (16)$$

本文以模糊控制器設計後勤映射同步系統，使 $t\to\infty$ 時，系統之同步誤差 $e(k)\to 0$ 。達成後勤映射同步後，即 $\hat{x}(k)\to x(k)$，則可經由解密函數還原欲傳送之明文訊號 $s(t)$ 。

四、電腦模擬

首先定義 IDEA 加密密鑰「1 2 3 8 2 3 4 8 3 4 5 9 4 5 6 9」，在本節中依加密順序，分別討論在傳送端以 IDEA 將明文資料加密後再經由混沌訊號遮蔽，並於接收端先除去混沌遮蔽訊號再以 IDEA 還原明文訊號之安全通訊系統。反之，先以混沌訊號遮蔽明文訊號再以 IDEA 加密之安全通訊系統。後勤映射混沌系統可表式如下

$$x(k+1)=\mu_1 x(k)-\mu_1 x^2(k) \quad (17)$$

其中 $\mu_1=4.0$ ； $x(0)=0.7$ 。根據（14）式定義欲驅動之後勤映射混沌系統如下

$$\hat{x}(k+1)=\mu_2\hat{x}(k)-\mu_2\hat{x}^2(k)+F\cdot(x(k)-\hat{x}(k)) \quad (18)$$

其中 F 為模糊增益值。模糊控制之規則庫設計方式:若誤差 *e* 為小（N）、誤差變化量 *de* 為小（N）時，因混沌系統之輸出行為無法預測，所以於控制輸出 *F* 設為小（N）；又誤差 *e* 為小（N）、誤差變化量 *de* 為大（P）時，因兩點之間誤差變化量變大會影響對混沌同步之控制，因而於控制輸出 F 設為大（P），設計之規則庫如表 1 所示。圖 2 為模糊集合之歸屬函數。

接著以不同加密順序，分別對語音訊號與影像資訊進行電腦模擬測試

（一）先以 IDEA 加密再由混沌訊號遮蔽:以鳥鳴之部份語音訊號作為欲傳送之明文資料 $s(t)$ ，如圖 3(a)所示。經由 IDEA 加密，可得明文之加密訊號如圖 3(b)所示。藉由後勤映射系統遮蔽，可得混沌傳送訊號如圖 3(c)所示。最後經由所設計之模糊增益，於接收端達成混沌同步，並以 IDEA 解密還原明文訊號，如圖 3(d)所示。

（二）先以混沌訊號遮蔽再由 IDEA 加密: 以三維之信用卡影像訊號作為欲傳送之明文資料 $s(t)$ ，如圖 4(a)所示。由混沌訊號遮蔽，得到混沌遮蔽之訊號如圖 4(b)所示。再以 IDEA 加密，可得加密訊號如圖 4(c)所示。最後經由所設計之模糊增益，於接收端達成混沌同步，並以 IDEA 解密再除去混沌遮蔽訊號還原明文訊號，如圖 4(d)所示。

不同加密順序顯示，明文訊號只以 IDEA 加密或混沌訊號遮蔽，不足以確保資訊之安全性。而經過國際數據加密演算法與後勤映射混沌遮蔽後，不論語音訊號或影像資料均有極佳之加密安全。

五、結論

由於模糊控制具有強健性，在混沌系統有參數誤差時，依然能維持混沌同步之強健穩定性能。故本文首先以非線性觀測器為基礎，運用模糊邏輯理論設計模糊增益，解決混沌同步問題。此外為提昇混沌同步資訊安全之性能，結合密碼學理論，設計應用模糊混沌同步與國際數據加密演算法之密碼系統。經由電腦模擬結果，顯示此後勤映射密碼系統，不論語音訊號或影像資料均具有優越之資訊安全。

六、誌謝

本研究由國科會補助，補助編號：NSC 92-2213-E-214-014，於此致謝。

七、參考文獻

[1] M. S. Baptista, “Cryptography with chaos”, *Physical Letters A*, Vol.240, pp.50-54, 1998.

[2] T. L. Carroll and L. M. Pecora, “Synchronization in chaotic systems”, *IEEE Trans. Circuit Sys. I*, Vol. 38, pp.453-456, 1991.

[3] D. E. Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.

[4] C. Huitema, *The New Internet Protocol*.

Upper Saddle River, NJ: Prentice-Hall, 1998.

[5] H. Leung and J. Lam, "Design of demodulator for the chaotic modulation communication system", *IEEE Trans. Circuits Syst*., Vol. 44, pp.262-267, Mar 1997.

[6] X. Lai and J. Massey, "A proposal for a new block encryption standard", *Advances in Cryptology – EUROCRYPT '90*, pp.389-404, 1990.

[7] X. Lai and J. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis", *Advances in Cryptology – EUROCRYPT '91*, pp.17-38, 1991.

[8] S. N. Resband, *Chaotic Dynamics of Nonlinear Systems*, A Wiley – Interscience Publication, 1989.

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 1999.

[10] C. W. Wu and L.O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems", *Int. J. Bifurcation Chaos*, Vol. 3, No.6, pp.1619-1627, 1993.

[11] Li-Xin Wang, *A Course in Fuzzy Systems and Control*, New Jersey: Prentice-Hall, 1997.

[12] J. Yen, and R. Langari, *Fuzzy Logic: Intelligence, Control, and Information*, New Jersey: Prentice-Hall, 1999.

[13] T. Yang, "Recovery of digital signals from chaotic switching", *Int. J. Circuit Theory Appl*., Vol. 23, No. 6, pp.611-615, 1995.

[14] T. Yang, C. W. Wu and L. O. Chua, "Cryptography based on chaotic systems", *IEEE Trans. Circuits Sys*., Vol.44, pp.469-472, 1997.

[15] C. Zhou and T. Chen, "Extracting information masked by chaos and Contaminated with noise: some considerations on the security of communication approaches using chaos", *Physical Letters A*, Vol. 234, pp.429-435, 1997.

表 1、模糊規則庫

控制輸出		誤 差 e		
		N	Z	P
誤差變化量 de	N	N	Z	P
	Z	Z	Z	Z
	P	P	Z	N

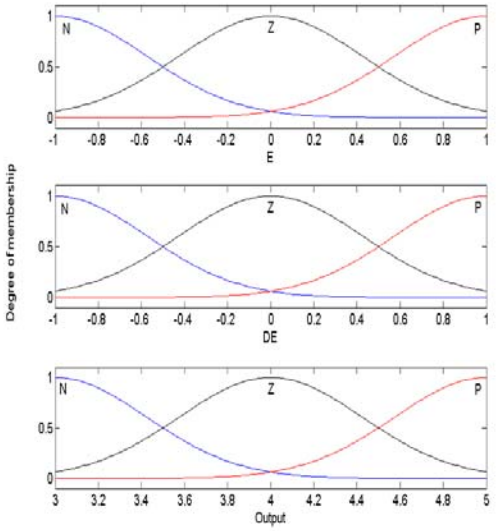


圖 2、模糊集合之歸屬函數

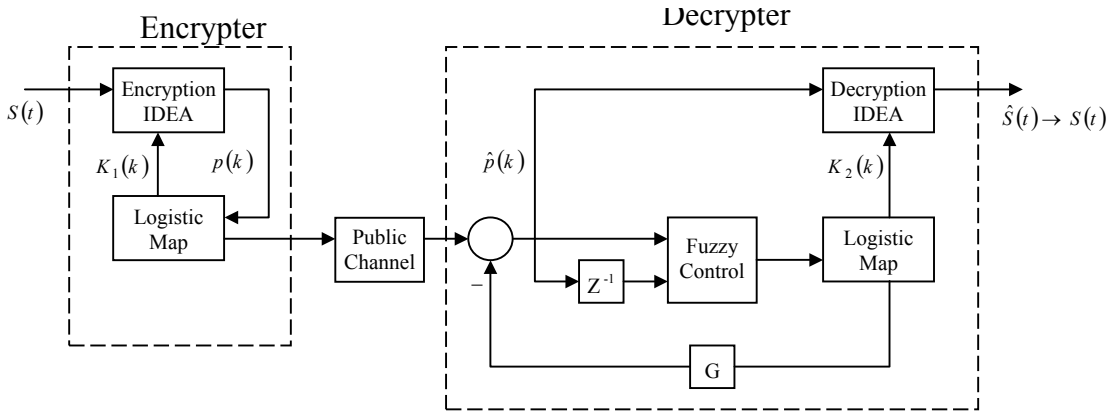
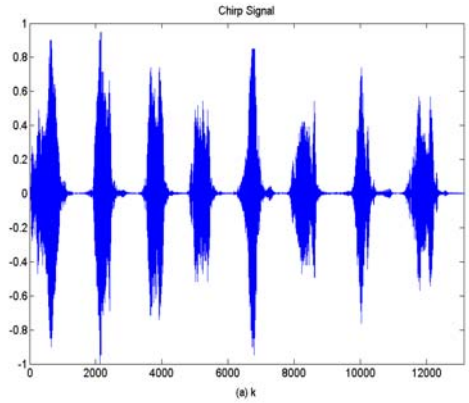
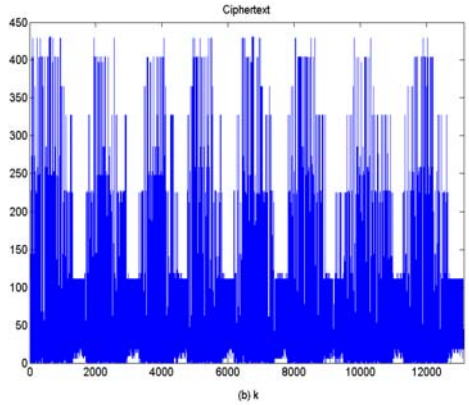
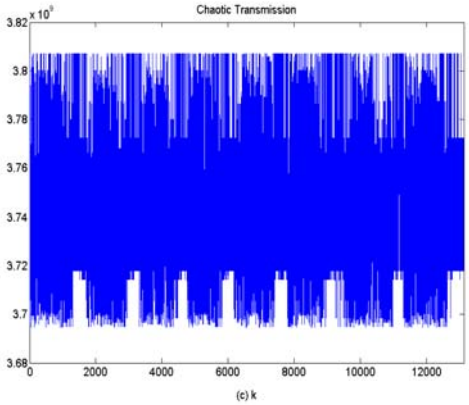


圖 1、後勤映射密碼系統







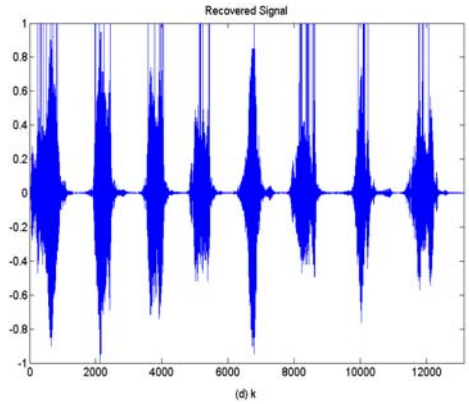
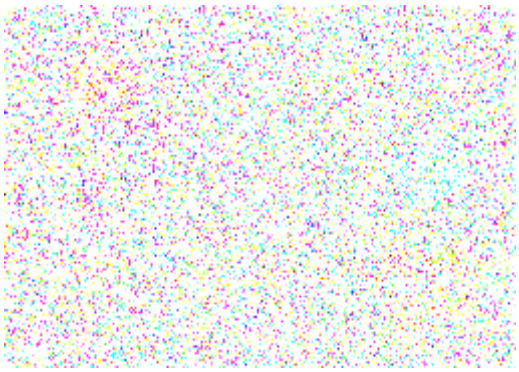


圖 3、鳥鳴部份語音訊號（先以 IDEA 加密再以 Chaotic 遮蔽）(a) 明文訊號 (b) 加密訊號 (c) 混沌傳送訊號 (d) 還原訊號

(a)

(b)



(c)

(d)

圖 4、信用卡影像(先以 Chaotic 遮蔽再以 IDEA 加密)(a) 原始圖像 (b) 混沌遮蔽圖像 (c) 加密圖像 (d) 還原圖像