行政院國家科學委員會專題研究計畫 期末報告

利用渾沌訊號與盲源分析法之多張圖像加密技術

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 101-2221-E-216-010-
執 行 期 間 ：101 年 08 月 01 日至 102 年 07 月 31 日
執 行 單 位 ：中華大學機械工程學系

計 畫 主 持 人 ：許隆結

計畫參與人員：碩士班研究生-兼任助理人員：許健聖

報 告 附 件 ：出席國際會議研究心得報告及發表論文

公 開 資 訊 ：本計畫可公開查詢

中 華 民 國 102 年 11 月 08 日

中 文 摘 要 ： 計畫提出了一個新的多張圖像加密法, 此方法結合混沌與盲源分離法。先將明文圖像以渾沌訊號排序置換，然後與密鑰圖像混合。在接收端，從密文圖像以盲源分離技術將原始圖像資料分離出來。然後混沌信號的再次用於恢復來恢復原始圖像的像素。實驗結果證明，密鑰空間大到足以抵抗暴力攻擊, 同時經加密圖像的灰度值分佈具有隨機的行為。

中文關鍵詞： 渾沌, 盲源分析, 圖像, 加密

英 文 摘 要 ： We propose a new perspective on multiple image encryption using chaotic signal and blind source separation. The original image is permuted by the chaotic signal and then mixed with key images. In the receiver, blind source separation technique is used to separate the components of the original image from the ciphertexts. Then chaotic signal is again used to restore the pixels to recover the original image. The experimental results demonstrate that the key space is large enough to resist the brute force attack and the distribution of gray values of the encrypted image has a random-like behavior.

英文關鍵詞： chaos, blind source separation, image, encryption

行政院國家科學委員會補助專題研究計畫 □期中進度報告 ■期末報告

利用渾沌訊號與盲源分析法之多張圖像加密技術

計畫類別：■個別型計畫　□整合型計畫
計畫編號：NSC　101-2221-E-216-010-
執行期間：2012 年 8 月 1 日至 2013 年 7 月 31　日

執行機構及系所：中華大學機械工程學系

計畫主持人：許隆結
共同主持人：
計畫參與人員：　董子儀、許健聖

本計畫除繳交成果報告外，另含下列出國報告，共 __1_ 份：
□移地研究心得報告
■出席國際學術會議心得報告
□國際合作研究計畫國外研究報告

處理方式：除列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

中　華　民　國 103 年 10 月

Contents

A Combination of Chaos and Blind Source Separation for Multiple Images Encryption

Long Jye Sheu, Juhn Horng Chen, Tzu Yi Tung,

Department of Mechanical Engineering Chung Hua University, HsinChu, Taiwan

ABSTRCT: We propose a new perspective on multiple image encryption using chaotic signal and blind source separation. The original image is permuted by the chaotic signal and then mixed with key images. In the receiver, blind source separation technique is used to separate the components of the original image from the ciphertexts. Then chaotic signal is again used to restore the pixels to recover the original image. The experimental results demonstrate that the key space is large enough to resist the brute force attack and the distribution of gray values of the encrypted image has a random-like behavior.

Key words: image encryption, blind source separation, chaos

I Introduction

With the rapid growth of multimedia production systems, more and more image information has been transmitted over the Internet the Internet. Protection of digital information against illegal copying and distribution has become extremely important. To meet this challenge, a variety of the encryption techniques have been introduced. [1–4]. As for digital image processing, methodology is classified into two categories- pixel value substitution and pixel location scrambling [5]. The first one concentrates on changing the pixel value so that others cannot read the original pixel information in the digital image. The other one concentrates on changing the pixel position for the purpose of encryption. However, both of these methods can be easily decrypted by some ways.

Blind source separation (BSS) techniques are applied to recover unknown signals or sources from their observed mixtures. If the number of the original sources is larger than that of the observed mixtures, there poses a significant difficulty of separation. The problem is called as underdetermined blind source separation (UBSS). However, the intractability of UBSS has motivated researchers to study whether it could replace other intractable problems (e.g. integer factorization) in the construction of cryptographic algorithms. Recently, Lin et al. [6, 7] introduce the concept of UBSS for image and speech encryption. The quality of the decrypted speech/images is excellent. Unfortunately, these schemes have been found to be insecure against known-/chosen-plaintext attack and chosen-ciphertext attack [8].

In this study, we propose an image encryption using chaos signal and blind source separation techniques. The original image is first permuted using a chaotic signal and then mixed using UBSS technique. The present scheme obtains the advantages of both pixel value substitution and pixel location scrambling. The frame is easy to set up while it is demonstrated that the proposed scheme to be immune against traditional attacks. The design also provides a new perspective toward secure communication.

II Blind Source Separation

The blind source separations are techniques to recover n independent sources, $\mathbf{S}(t) = [s_1(t), s_2(t), .., s_n(t)]^T$, from their mixtures, $\mathbf{X}(t) = [x_1(t), x_2(t), .., x_m(t)]^T$, which are linear combination of the independent sources by an unknown matrix, **A**. For the sake of simplicity, we assume the number of mixed signals is the same as the number of independent sources, i.e. *m=n*. This is a simplifying assumption that is not completely necessary. Then, the mixed vector can be written as

$$\mathbf{X}(t) = \mathbf{A}\mathbf{S}(t) \qquad (1)$$

where

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \qquad (2)$$

is the mixing matrix giving the mixing weights. Matrix **A** is generally assumed to be unknown. The source signals, s_i, are unknown as well. When only mixed signals, $x_i(t)$, are known, the BSS algorithms are designed to separate the estimated independent sources, $\hat{\mathbf{S}}(t) = [\hat{s}_1(t), \hat{s}_2(t), ..., \hat{s}_n(t)]^T$, such that

$$\hat{\mathbf{S}}(t) = \mathbf{B}\mathbf{X}(t) = \mathbf{B}\mathbf{A}\mathbf{S}(t) \approx \mathbf{S}(t) \qquad (3)$$

where **B** is the demixing matrix,

$$\mathbf{B} = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} \approx \mathbf{A}. \qquad (4)$$

Many algorithms exist for calculating the demixing matrix, **B**. Among them, Independent

component analysis (ICA) [9] is a faithful, easy and efficient method. In general, the estimated elements of matrix **B** differ from those of $\mathbf{A}^{-1}$. The components of $\hat{\mathbf{S}}(t)$ separated by the ICA reveal opposite phases and unequal amplitudes with the components of the original source, **S**(t).

III Proposed Scheme

The block diagram of proposed BSS-based images encryption is shown in Fig. 1.

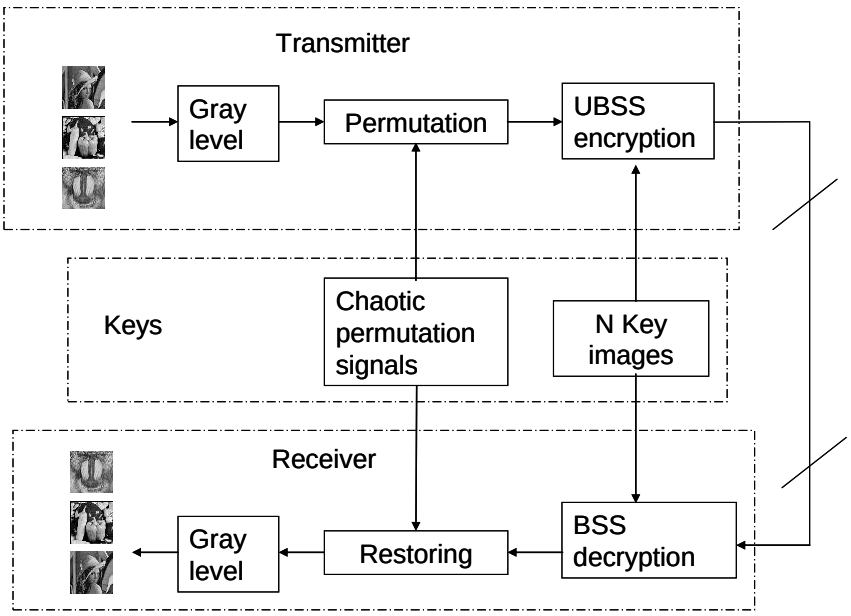

Figure 1 Block diagram chaos+BSS for image encryption

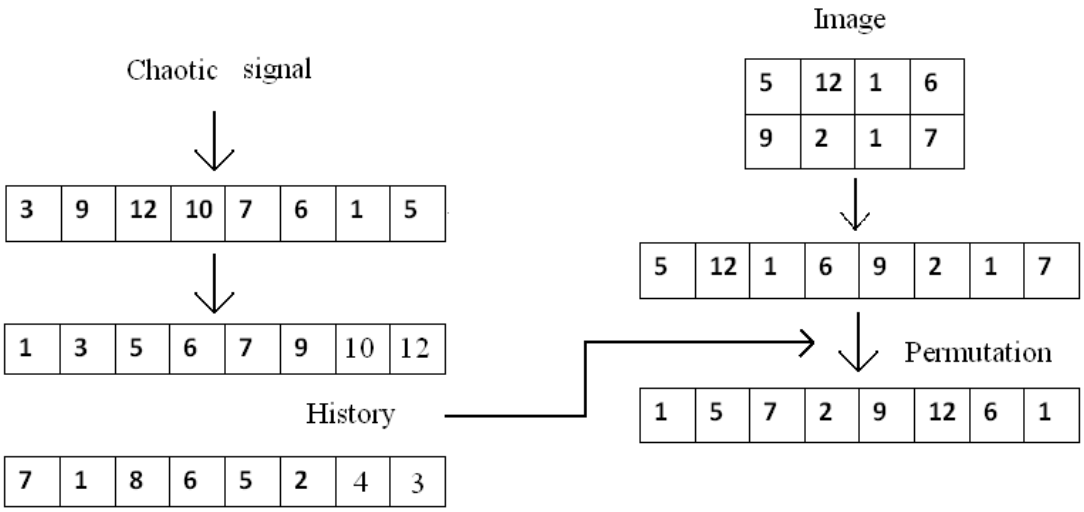

Figure 2 Permutation process

Transmitter: The transmitter consists of two parts: permutation and underdetermined mixing.

a. Permutation

Figure 2 shows the rule of permutation. First we obtain the gray levels of the original images. Then, one-dimensional vectors are formed from the gray levels of the original images. Chaotic signals are then generated to permute the vectors. Each of the chaotic signals is sorted from minimum to maximum. The corresponding position between the sorted and original chaotic signal is recorded in other vectors called history vectors. The one-dimensional vectors from the original images are then permuted according the history vectors and reshaped to form the permuted images.

b. Underdetermined mixing

The *m* permuted images $\mathbf{s} = [s_1(n), s_2(n), ..., s_m(n)]^T$ are mixed with *N* key signals $\mathbf{k} = [k_1(n), ..., k_N(n)]^T$ into the ciphertexts $\mathbf{x} = [x_1(n), x_2(n), ..., x_m(n)]^T$ by using an underdetermined mixing matrix $\mathbf{A_e}$. Specifically, given source matrix $\mathbf{S} = [\mathbf{s}^T, \mathbf{k}^T]^T$, the encryption can be represented by the following equation:

$$\mathbf{x} = \mathbf{A_e S} = [\mathbf{a_s}\ \mathbf{a_k}]\mathbf{S} \qquad (5)$$

where the $\mathbf{a_s}$ $\mathbf{a_k}$ represent the weightings of permutated images and key images in the ciphertexts, respectively. Obviously, Eq. (5) constructs an UBSS problem since there are (*m*+*N*) signals in the ciphertexts. Then the ciphertexts are transmitted to the receiver through the public channel.

Receiver: The receiver consists of two parts: ICA separation and restoring

a. ICA separation

In the receiver end, the ciphertexts are first decrypted by BSS technique and then restored the corresponding pixels to the original position. To recover the original image, at least (*m*+*N*) signals

are required as inputs of the BSS in the decryption. Once the *m* ciphertexts are received from the public channel, the *N* key signals are regenerated by the secret seed I_0 to provide the rest of the *N* inputs of the BSS. Hence, the inputs of the BSS can be written as

$$\mathbf{x_d} = \begin{bmatrix} \mathbf{x} \\ \mathbf{k} \end{bmatrix} = \mathbf{A_d S} \qquad (6)$$

where

$$\mathbf{A_d} = \begin{bmatrix} \mathbf{A_e} \\ \mathbf{0\ I} \end{bmatrix} \qquad (7)$$

In Eq. (7), $\mathbf{0}$ is a $N \times m$ zero matrix, $\mathbf{I}$ is a $N \times N$ identity matrix. It is noted that $\mathbf{A_d}$ is a square matrix of full rank. When $\mathbf{x_d}$ is feed into the BSS, the independent component analysis technique is used to recover the estimate of the permuted images $\hat{\mathbf{s}}$ as shown in Fig. 1.

b. Restoring

After the permuted images are decrypted by BSS, a restoring process which is opposite to the permutation process described in the previous is performed to shuffle the corresponding pixel to its original position. The restoring process is the inverse of the permutation process shown in Fig. 2.

IV Experimental Results

The next step is the evaluation of the scheme to encrypt and decrypt an image. We make a simulation to encrypt three well-known images "Lena.jpg", "Peppers.jpg" and "Baboon.jpg". Figure 3 shows the original images and their histograms with 256 gray levels, the size of each image is 128×128. In this study, the key consists of two parts- the chaotic signal for permutation and noisy key images to UBSS. Here, the chaotic signals to permute the original images are also used as key signals. It is known that the chaotic signals are very sensitive to parameters and initial conditions. The random-like behavior of chaotic signals provides potential to mask the original signals.

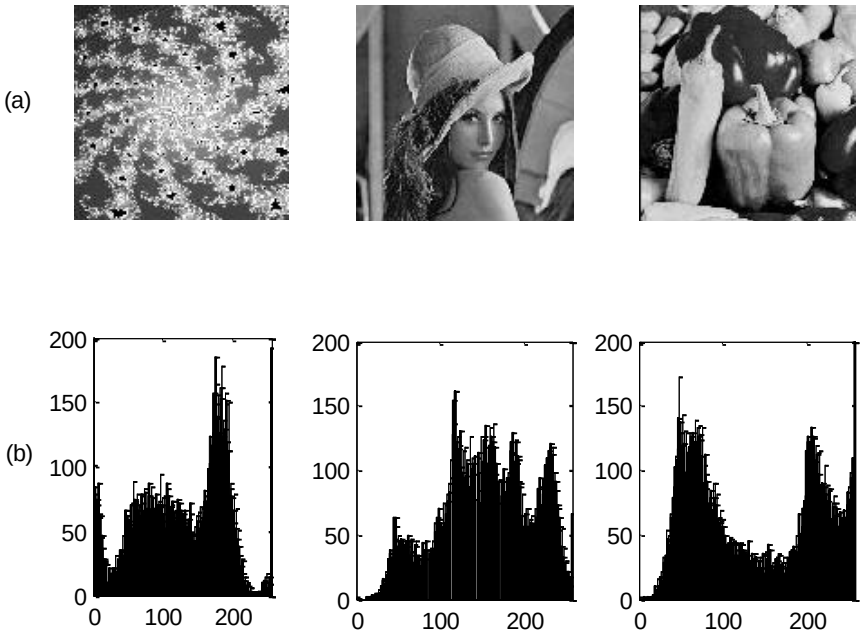

Figure 3 (a) Original images and (b) histrograms of the original images

We choose the chaotic signal from the the Chen-Lee system [10]:

$$\text{Chen-Lee system} \qquad \begin{aligned} \dot{z}_1 &= -z_2 z_3 + \alpha z_1 \\ \dot{z}_2 &= z_1 z_3 + \beta z_2 \\ \dot{z}_3 &= (1/3) z_1 z_2 + \gamma z_3 \end{aligned} \qquad (8)$$

The parameters and initial conditions are chosen to be, $(\alpha, \beta, \gamma) = (5, -10, -3.8)$, and $[z_1(0), z_2(0), z_3(0)] = [0.2, 0.2, 0.2]$. We generate z_1, z_2 and z_3 with time intervals 0.1sec as key signals. The chaotic signals z_1, z_2 and z_3 are then sorted to permute "Baboon.jpg", "Lenna.jpg" and "Peppers.jpg", respectively.

Six random noises n(t) are generated by Marsaglia's Ziggurat pseudorandom number generator (PRNG) [11] to form the key images for UBSS. It is known that Marsaglia's Ziggurat PRNG generates floating-point values with a very huge period, good statistical performance and fast speed. The underdetermined mixing $\mathbf{A_e}$ used in this simulation is random generated as

$$\mathbf{A} = \begin{bmatrix} 0.8257 & 0.9844 & 0.3463 & 8.3012 & 6.6249 & 4.6956 & 0.3023 & 4.2694 & 1.1618 \\ 0.6256 & 0.6201 & 0.1387 & 3.5165 & 4.3960 & 7.9601 & 1.4431 & 6.6141 & 3.5175 \\ 0.1420 & 0.0847 & 0.5831 & 8.1142 & 0.4606 & 8.6777 & 3.0321 & 0.1090 & 9.6535 \end{bmatrix}$$

In this study, the FastICA algorithm to perform Independent Component Analysis (ICA) [12, 13] was applied to calculate the demixing matrix, **B** as

$$\mathbf{B} = \begin{bmatrix} 0.3359 & -0.4524 & -0.0948 & -0.4711 & -0.1632 & -0.6242 & 0.7977 & 1.5695 & 2.1262 \\ 0.0004 & 0.0227 & -0.0550 & 3.8419 & -0.0638 & 0.2576 & 0.1379 & -0.1267 & 0.4299 \\ 0.0417 & -0.0610 & -0.0310 & 0.1023 & 0.0395 & 0.5653 & 0.2165 & 0.2163 & 3.9464 \\ 0.0083 & 0.0247 & -0.0204 & 0.0168 & 3.3066 & -0.0523 & 0.0229 & -0.1821 & 0.0982 \\ 0.1962 & -0.2856 & 0.0057 & -0.6756 & -0.0532 & 1.3142 & 0.3234 & -2.4100 & 0.7342 \\ 0.0726 & -0.0792 & -0.0316 & -0.0595 & -0.0986 & 0.5654 & 3.6575 & 0.1997 & 0.4754 \\ 1.7646 & -3.6186 & 5.6102 & -47.4156 & 1.6491 & -28.1639 & -12.3344 & 15.7867 & -43.4778 \\ 26.8326 & -33.7489 & -7.9988 & -39.1945 & -25.7388 & 212.0568 & 64.8183 & 109.5267 & 164.7284 \\ 20.8311 & -32.5184 & -4.5615 & -21.5666 & 7.0351 & 200.5722 & 54.4425 & 126.6156 & 134.2066 \end{bmatrix}$$

Figure 4 shows an example of simulation of secure communication of multiple images. Figure 4a shows three original images and six key images for UBSS. Figure 4b shows the permuted images. It is shown that the permuted images are indistinguishable by human eyes. It should be noted that, the Chen-Lee chaotic signals only shuffle the pixel positions of the images. Hence the histograms of the permuted-images are the same as the original images.

Figure 4c shows the encrypted images. It is easy to see that the encrypted signal has reached the security goal. Figure 4d~4f show the decrypted images are all of good quality. The histograms of the encrypted signal are shown in Fig. 5. From the figure, it can be seen that they are of Gaussian distribution, i.e. similar to white noisy images. The obtained images and their corresponding histograms from the process of decryption algorithm are shown in Fig. 6. It is seen that decrypted images is of good quality where the histogram plots are almost the same as those of the original images as shown in Fig 3.

Figure 4 Example of encryption (a) three original images and six key images (b) permuted images (c) encrypted cipher images (d) decrypted image using z_1 (e) decrypted image using z_2 and (f) decrypted image using z_3

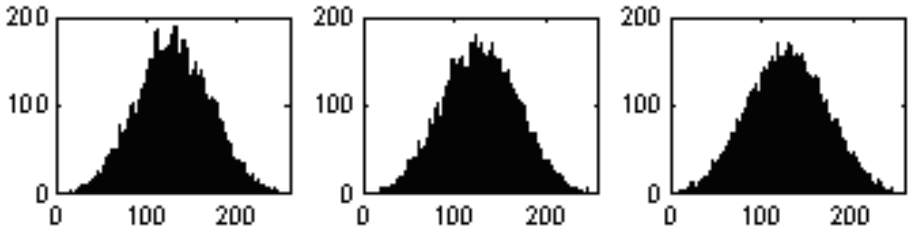

Figure 5 Histrograms of encrypted cipher images

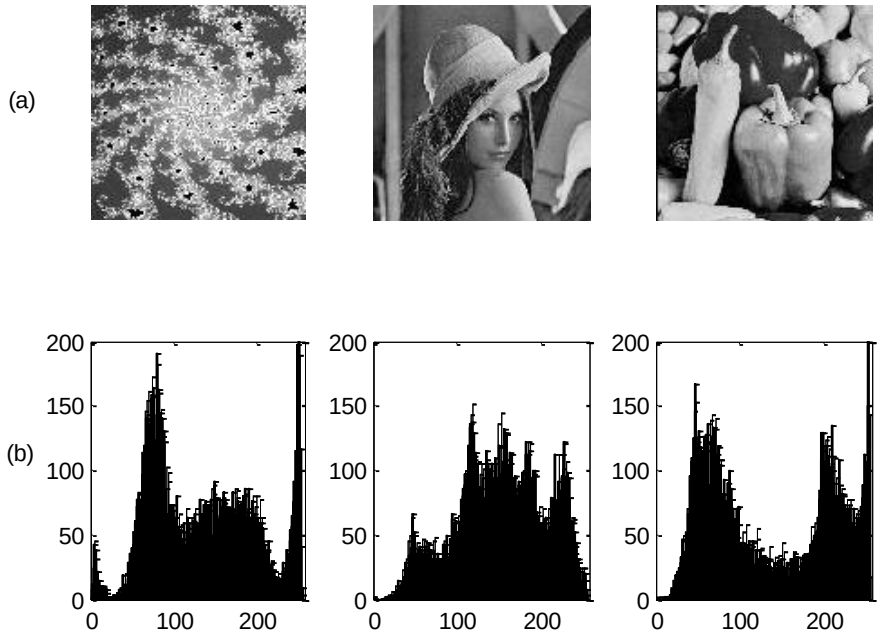

Figure 6 (a) decrypted images and (b) Histograms of the decrypted images

V. Cryptoanalysis

A well-designed encryption scheme should be free at least to resist brute force attack, ciphertexts only attack, known plaintext attack and chosen plaintext/ciphertext attacks. Here we discuss security analysis of this scheme.

Keys and key Space

In the present scheme, the chaotic signals are generated from the chaotic Chen-Lee system with the parameters (α, β, γ) and initial conditions $[z_1(0), z_2(0), z_3(0)]$. The parameters and initial conditions are the secret keys in this scheme. Hence, the secret key consists of six numbers $(\alpha, \beta, \gamma, z_1(0), z_2(0), z_3(0))$. Since these six numbers could be real numbers, the space of the keys will be a 6-dimensional space. The space is nonlinear since all of the keys are not equally strong. In the subspace where the derivative orders or parameters of the Chen-Lee system originate periodic orbits, the sub-key space is degenerative because it is relatively easy to break. Values of $(\alpha, \beta, \gamma, z_1(0), z_2(0), z_3(0))$ which give rise to periodic windows should be avoided since chaotic bands are preferred for encryption. The key space for an encryption scheme should be large

enough to resist the brute force attack. If the precision for each of the six numbers is 10^{-10}, the key space size is 10^{60}.

Another key set is the seed I_0 used to generate the random noisy key images. We use the Marsaglia's PRNG, which uniformly generates floating point values between 0 and 1 with a huge period (almost 2^{1430}), good statistical performance, and fast speed [11]. The total key space size is the product of each sub-key-space which is large enough to resist all kinds of brute force attacks.

VI Conclusions

In this paper, a new perspective on image communication using chaos and blind source separation is proposed. The design of this scheme has many merits: (a) It provides an easy way of both pixel value substitution and pixel location scrambling; (b) The key space is large enough to resist all kinds of brute force attacks.

Acknowledgements

This work was financially supported by the Natural Science Council of ROC under grant number NSC 101-2221-E-216-010.

References

[1] S. S. Maniccam, N. G. Bourbakis, "Image and video encryption using SCAN patterns," Pattern Recognition, Vol. 37, pp. 725-737, 2004.

[2] C. C. Chang, M. S. Hwang and T. S. Chen, "A new encription algorithm for image cryptosystems," Journal of System Software, Vol. 58, pp. 83-91, 2001.

[3] N. Bourbakis and C. Alexopoulos, "Picture data encryption using SCAN patterns," Pattern Recognition, Vol. 25, pp. 567-581, 1992.

[4] H. Cheng and X.B. Li, "Partial encryption of compressed image and videos," IEEE Trans. Signal Processing, Vol. 48, pp. 2439-2451, 2000.

[5] M. Prasad and K. L. Sudha, "Chaos Image Encryption using Pixel shuffling,", Computer Science & Information Technology, DOI: 10.5121/csit.2011.1217.

[6] Q. H. Lin and F. L. Yin, T. M. Mei and H. Liang, "A blind source separation based method for

speech encryption," IEEE Trans. Circuits System, Vol. 53, pp. 1320–1328, 2006.

[7] Q. H. Lin and F. L. Yin, T. M. Mei and H. Liang, "A blind source separation-based method for multiple images encryption," Image and Vision Computing, Vol. 26, pp. 788-798, 2008.

[8] S. Li, C. Li, K. T. Lo and G. Chen, "Cryptanalyzing an encryption scheme based on blind source separation," IEEE Trans. Circuits System, Vol. 55, pp. 1055-1062 2008.

[9] C. Jutten and J. Herault, “Blind separation of sources, Part 1: an adaptive algorithm based on neuromimetic architecture,” Signal Processing, Vol. 24, pp. 1-10, 1991

[10] H. K. Chen and C. I. Lee, "Anti-control of chaos in rigid body motion," Chaos, Solitons & Fractals, Vol. 21, pp. 957-965, 2004.

[11] C. Moler, Random thoughts, Matlab News & Notes, pp. 12–13, 1995.

[12] A. Hyvarinen and E. Oja, "A Fast Fixed-Point Algorithm for Independent Component Analysis," Neural Computation, Vol. 9, pp. 1483-1492, 1997.

[13] http://research.ics.tkk.fi/ica/fastica/index.shtml.

[14] Juhn Horng Chen, Long Jye Sheu, Tzu Yi Tung, Hsien Keng Chen, Horng Shing Chiou , Wei Tai Weng, “A Combination of Chaos and Blind Source Separation for Image Encryption”, *Applied Mechanics and Materials Vols. 373-375 (2013) pp 513-516.*

[15] 董子儀, “結合渾沌與盲源分析法之多圖像加密技術”, 中華大學機械系碩士論文, 新竹市, 2012.

計畫成果自評

本計畫進行多圖像加密技術之研究, 計畫完成下面工作:

1. 建立渾沌與盲源分析法結合之多圖像加密技術。
2. 實際測試並實踐本加密方法。
3. 針對本方法討論金鑰空間與破密分析。

部份計畫成果已發表於國際研討會，並受到 EI 資料庫收錄[14]，另外計畫過程培養一位碩士[15]。

行政院國家科學委員會補助國內專家學者出席國際學術會議報告

2013 年 6 月 20 日

附件三

報告人姓名	許隆結	服務機構及職稱	中華大學機械系教授
時間 會議 地點	2013/6/13 至 2013/6/14 大陸廣州	本會核定 補助文號	101-2221-E-216-010
會議名稱	（中文）2013 機電整合、機器人及自動化國際學術會議 （英文）International conference on Mechatronics, Robotics and Automation (ICMRA 2013)		
發表論文題目	（中文）結合渾沌與盲源分析法之圖像加解密技術 （英文）A combination of chaos and blind source separation for image encryption		

報告內容應包括下列各項：

一、參加會議經過

本次會議為 2013 年國際機電、機器人及自動化會議於 6 月 13 日在中國廣州召開。會議由昆士蘭理工大學、韓國海洋大學以及香港工業技術研究中心主辦。本次會議旨在致力於為科研人員和工程師們提供一個高水準的交流平臺,探討機電整合、控制與製造領域的新技術和新應用。

筆者於 12 日從桃園出發飛深圳，由於當天桃園機場大雷雨，以致班機誤點，因此筆者於深圳稍作停留於次日(13 日)早上至會場辦理現場註冊。研討會於在廣東南洋長勝酒店金鑾殿舉辦，參加人數眾多，筆者於 14 日早上聆聽兩場主辦單位舉辦之會議主題演講。筆者發表之論文被安排於當日(14 日)下午之分組發表，時段是 6 月 14 日下午 13:40-17:40，該組共有 24 篇論文發表，筆者論文被安排於第一篇發表，除了宣讀論文，並聆聽其他作者之論文發表，也與其他學者切磋討論。會議程結束後，15 日筆者順道參訪台商在深圳工廠，於 16 日搭機返國。

二、與會心得

對於有機會可以參與此次研討會深感榮幸，除了於台下聆聽各位先進之學術心血結晶之外，又可親見多位大師風采，收穫頗豐。經由這次的研討會，最大的收穫就是對於自動化與人工智慧的論文內容，對其寬度與廣度有更進一步的瞭解，也引發本人對這一方面的靈感，考慮下一步探索此方面為主題與領域研究，也希望在短時間可以有稍許研究成果，如此才不負國科會補助的栽培與用心。

三、考察參觀活動(無是項活動者省略)

筆者並參訪台商機器視覺檢測相關廠商，回國後將推動學校與該廠商之合作。

四、建議

(i) 承蒙國科會補助能夠參與會議，在此特致謝意。能有機會出國參加國際會議，達到學術交流與即時充電目的，感覺收穫很多，未來也計畫每年能出國一至兩次參加國際學術研討會，將有助於筆者在學術領域的研究與學習。

(ii) 本次會議所發表的論文涵蓋機電整合、機器人與自動化等等領域之重要議題。校內相關同仁若能夠更有效的整合將提昇學校在新竹附近區域此領域競爭能力。有助於推展產學合作及學生相關技術之訓練。

五、攜回資料名稱及內容

筆者攜回會議手冊一本，會後會議論文集將由 Applied Mechanics and Materials 期刊出版，所有被大會收錄的論文並被 EI 檢索。

六、其他

行政院國家科學委員會補助國內專家學者出席國際學術會議報告

2013 年 6 月 20 日

附件三

報告人姓名	許隆結	服務機構及職稱	中華大學機械系教授
時間 會議 地點	2013/6/13 至 2013/6/14 大陸廣州	本會核定 補助文號	101-2221-E-216-010
會議名稱	（中文）2013 機電整合、機器人及自動化國際學術會議 （英文）International conference on Mechatronics, Robotics and Automation (ICMRA 2013)		
發表論文題目	（中文）結合渾沌與盲源分析法之圖像加解密技術 （英文）A combination of chaos and blind source separation for image encryption		

報告內容應包括下列各項：

一、參加會議經過

本次會議為 2013 年國際機電、機器人及自動化會議於 6 月 13 日在中國廣州召開。會議由昆士蘭理工大學、韓國海洋大學以及香港工業技術研究中心主辦。本次會議旨在致力於為科研人員和工程師們提供一個高水準的交流平臺,探討機電整合、控制與製造領域的新技術和新應用。

筆者於 12 日從桃園出發飛深圳，由於當天桃園機場大雷雨，以致班機誤點，因此筆者於深圳稍作停留於次日(13 日)早上至會場辦理現場註冊。研討會於在廣東南洋長勝酒店金鑾殿舉辦，參加人數眾多，筆者於 14 日早上聆聽兩場主辦單位舉辦之會議主題演講。筆者發表之論文被安排於當日(14 日)下午之分組發表，時段是 6 月 14 日下午 13:40-17:40，該組共有 24 篇論文發表，筆者論文被安排於第一篇發表，除了宣讀論文，並聆聽其他作者之論文發表，也與其他學者切磋討論。會議程結束後，15 日筆者順道參訪台商在深圳工廠，於 16 日搭機返國。

二、與會心得

對於有機會可以參與此次研討會深感榮幸，除了於台下聆聽各位先進之學術心血結晶之外，又可親見多位大師風采，收穫頗豐。經由這次的研討會，最大的收穫就是對於自動化與人工智慧的論文內容，對其寬度與廣度有更進一步的瞭解，也引發本人對這一方面的靈感，考慮下一步探索此方面為主題與領域研究，也希望在短時間可以有稍許研究成果，如此才不負國科會補助的栽培與用心。

三、考察參觀活動(無是項活動者省略)

筆者並參訪台商機器視覺檢測相關廠商，回國後將推動學校與該廠商之合作。

四、建議

(i) 承蒙國科會補助能夠參與會議，在此特致謝意。能有機會出國參加國際會議，達到學術交流與即時充電目的，感覺收穫很多，未來也計畫每年能出國一至兩次參加國際學術研討會，將有助於筆者在學術領域的研究與學習。

(ii) 本次會議所發表的論文涵蓋機電整合、機器人與自動化等等領域之重要議題。校內相關同仁若能夠更有效的整合將提昇學校在新竹附近區域此領域競爭能力。有助於推展產學合作及學生相關技術之訓練。

五、攜回資料名稱及內容

筆者攜回會議手冊一本，會後會議論文集將由 Applied Mechanics and Materials 期刊出版，所有被大會收錄的論文並被 EI 檢索。

六、其他

國科會補助計畫衍生研發成果推廣資料表

日期:2013/11/08

國科會補助計畫	計畫名稱: 利用渾沌訊號與盲源分析法之多張圖像加密技術
	計畫主持人: 許隆結
	計畫編號: 101-2221-E-216-010- 學門領域: 動力與控制

無研發成果推廣資料

101 年度專題研究計畫研究成果彙整表

計畫主持人：許隆結	計畫編號：101-2221-E-216-010-
計畫名稱：利用渾沌訊號與盲源分析法之多張圖像加密技術	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	2	2	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	1	1	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：(以 100 字為限)

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）(以 500 字為限)

本計畫進行多圖像加密技術之研究, 計畫完成下面工作:

1. 建立渾沌與盲源分析法結合之多圖像加密技術。
2. 實際測試並實踐本加密方法。
3. 針對本方法討論金鑰空間與破密分析。

本加密方法在網路資訊時代, 大量圖像傳遞之資訊安全應有貢獻