

浮水印加入蜜蜂演算法保護火炮射擊通訊之研究

鄭平守
高雄應用科技大學電子工程系 副教授
pscheng@cc.kuas.edu.tw

林士弘
高雄應用科技大學電子工程系 研究生
pele@mail.lcv.s.kh.edu.tw

黃素慈
高雄應用科技大學電子工程系 研究生
salina.huang@yahoo.com.tw

陳志男
高雄應用科技大學電子工程系 研究生
cheng0728x@giga.net.tw

蔡宗甫
高雄市政府工務局資訊室 管理師
2094620116@cc.kuas.edu.tw

摘要

現今國軍的陸軍步兵火炮射擊所使用的通訊，分為有線通信與無線通信兩種，有線通信必須注意線路是否斷掉，而無線通信需注意通訊保密之安全性，然而火炮射擊必須經由人為的運算將所需的射擊諸元運算出來，若因為有線通信的線路斷路或無線通信加解密有誤，那就無法精確命中目標。

在陸軍步兵的火炮射擊之中有前進觀測人員、射擊陣地、射擊目標區、射擊基準點...等。而這一些跟蜜蜂的某些特性有雷同之處，蜜蜂在尋找花源的時候，有蜜蜂、蜂巢、花源、太陽...等。觀測人員就如同蜜蜂，射擊陣地就如同蜂巢，射擊目標區就如同花源，射擊基準點就如同太陽，我們可以利用蜜蜂傳遞訊息的方法來設計通訊的方法，結合現今最熱門的浮水印隱藏技術，將其演算的方式隱藏傳送通信，達到通訊保密效果，將此蜜蜂演算法與浮水印技術結合設計一 PDA 及主系統，讓陸軍步兵於火炮射擊時，不需經過人員複雜的換算以及對照，使射擊方式更為簡單化，並讓其通訊達到保密的效果。

應用蜜蜂演算法結合浮水印技術於火炮射擊的通訊保密上，可以使射擊的步驟更為精簡，並讓射擊的精確度更為提高，還可以達到通訊的保密，提高了通訊的保密性。

關鍵詞：火炮射擊、通訊、浮水印、蜜蜂演算法。

Abstract

The national army infantry artillery fire used by the communications, can be divided into

two types of wire communications and wireless communications, cable should pay attention to whether the cut off line, wireless communications have joined the secret language, However, the need to send encrypted information, has to be decrypted, artillery fired by the man-made computing needs will be required for the firing data computing, if the cable disconnected lines or wireless communications encryption and decryption error, will not be able to accurately hit the target, if the use of animals in some of the characteristics and of the watermark encryption technology, for encrypted communications, to protect the confidentiality of communications in this paper is to study direction.

Keywords: Firing artillery, Communications, Watermark, the bees algorithm.

1. 前言

為了讓各式各樣的問題可以更有效且最佳化的解決，於是利用了各種動物的習性運用問題的解決，例如：蟻群演算法[1]及蟑螂演算法[2]...等。而陸軍步兵的火炮射擊之中最重要的就是通訊，再來就是火炮射擊的各諸元運算，因此火炮射擊的通訊保密就非常的重要，只要一個不小心就會造成軍事機密外洩，讓火炮射擊的陣地位置暴露，且會使要射擊的目標立即有所防備造成射擊無法精確的命中目標，所以必須要非常的小心才可以。在歷史上因為通訊洩密造成的失敗有許許多多，例如：中途島海戰[3]的失敗，及山本五十六元帥的戰死，都是因為日本海軍的通訊洩密所造成的。由此一戰例之中，我們可以知道通訊保密的重要性，所以對通訊密碼以及通訊工具的使用，都要非常的謹慎且小心，不可以有任何絲毫的疏失，才不會讓敵人有機會能夠乘虛而入。日本元帥山

本五十六的死因就是因為通訊的洩密，那麼也就是說通信洩密是促使日本會戰敗的主因之一，而這一個戰例，我們要永遠記取[4]。為了讓陸軍步兵最重要的火炮射擊之通訊保密可以有效的提升，運用蜜蜂的特性發展出蜜蜂演算法，並結合現今最熱門的浮水印隱藏技術來提升通訊的保密，其重要性是本論文所要探討的。

2. 數位浮水印介紹

在近幾年以來，數位浮水印是相當多學者所關注的重點以及發展的方向之一。而數位浮水印就是將不能看到的標記，隱藏在於一般性的視訊、聲音、影像、文件...等中，並可以禁得起一定程度的影像失真後，仍能將標記抽取出來，做為所有權認證用[10]。

現今所有有關浮水印公開的文獻之中，有很多的浮水印隱藏資料方法也已經先後被提出來；在這一些文獻之中，浮水印有各種不一樣的分類、隱藏以及應用方式。就以視覺的品質來做區分，可以分為可見的浮水印以及不可見的浮水印。而以浮水印本身的特性來做區分，則可以分為以任意影像以及具有統計特性的數值序列。如果以應用來做區別，則可以概略分成兩個廣泛的範圍：以目的為導向和以來源為導向[11]。這些公開的浮水印文獻說明了在不一樣的角度下，浮水印所呈現出的不一樣面貌。

2.1 浮水印的區分

數位浮水印的區分可依照視覺品質及本身特性還有其應用來做區分，分別如下詳述。

2.1.1 依應用來區分浮水印

隱藏浮水印是為了驗明誰才是真正的擁有者，當隱藏浮水印目的是為了要防範購買者做非法及轉賣的使用時，就稱為以目的為導向的浮水印；當隱藏浮水印目的是為了要辨別真正擁有者時，稱為以來源為導向之浮水印[11]。

以目的為導向的浮水印：假如是為了追蹤購買者，或者是使用者違法地把產品移做它用，或者是轉賣因此而加入浮水印者，在每個拷貝版裡面加入獨一無二的浮水印，做為日後辨別這個拷貝版是賣給了哪一個購買者。假如發現了與自己作品的數位媒體資料有類似的時候，只要將所加入的浮水印抽取出來，看看當初是隱藏於哪一個購買者的產品之中。就可以得知是誰把這個數位媒體資料做違法的使

用。

以來源為導向的浮水印：為了所有權之鑑定/辨識的問題而隱藏其浮水印者，在原始影像散佈前，就已經加入了自己的浮水印，這個浮水印能夠具備個人特徵的圖形，以便以後能夠用來驗明影像所有權。這個具備了個人特徵之浮水印，能夠用來鑑定所接收到的數位化媒體資料，是否已經有被修改過了，假如接收到和自己的作品相似影像時，而且從其中取出自己的浮水印，就能夠認定是他人把自己所創作的影像，加以修改過之後所製造出來的，所以就可以達到所有權之鑑定/辨識的能力。

2.1.2 依視覺品質來區分浮水印

隱藏浮水印的方式有將浮水印直接就顯示於被保護的影像上面，而浮水印是清晰而且可以讓人看見的，因此稱之為可見的浮水印；也有將浮水印隱蔽於影像之中而不可以讓人看見的，稱之為不可見的浮水印。可見的浮水印因為浮水印是清晰能夠看見的，所以相對的會破壞影像之品質，而且容易被攻擊者藉著直接的影像處理而去影響到浮水印的品質。不可見的浮水印由於比較不易被攻擊者所以發現，相對地減少了被攻擊的機會。

2.1.3 依本身特性來區分浮水印

利用具有個人特徵的圖形做為浮水印，加到自己的作品中，但在已知的公開文獻中所使用的浮水印，有利用擬亂序列所組成，也有利用高斯分佈的亂數序列所組成，而浮水印並不都是具有其視覺意義。所以，浮水印依據本身特性，可區分為以有統計特性的浮水印及具有意義圖形的浮水印。具有統計特性的數值序列，具有容易以數學描述的特性。例如：浮水印可以是利用高斯所產生擬亂的序列，在偵測浮水印時，只要判斷取回的訊號是否具有一樣之統計特性就行了；有意義的圖為浮水印之優點，在同時兼具訊息的傳遞效益。例如：使用者能在影像中隱藏新型戰車的影像，而當對方取回浮水印的同時，也能曉得新型戰車模樣。這樣的功能可視為資訊隱藏的一種。也就是在視覺無法察覺的原則下，利用對數位影像像素作輕微的改變，來達到隱藏額外資訊的一種編碼方式[12]。

2.2 浮水印的特性

原則上，浮水印必須要具備：強韌性、安全性、不可模糊性、不易察覺性等特性[13]，如下所述：

2.2.1 不可模糊性

抽取出的浮水印，可以清楚的看出和原始的浮水印幾乎一模一樣，能夠做為所有權認證之用。

2.2.2 不易察覺性

本特性是利用人類的視覺和聽覺系統，對於影像以及聲音微小的差異不敏感性，所以對於多媒體的資料，可以嵌入浮水印來取代部分的不重要資料，把浮水印植入原始資料的重複冗餘或高頻信號部分，雖然滿足了不容易察覺的特性，但是放在這些地方之浮水印，也容易因為一般的壓縮技術輕易的去除。

2.2.3 容量大小

至少需能簡單的描述性資料或隱藏商標、識別碼，對於某些需要能夠同時允許多個浮水印，或者要求在有限的頻寬內，可傳送更多的資料，應用上則須要容納更多的資料。

2.2.4 強韌性

為了確保能夠正確的偵測出，及抽取出原先的浮水印，浮水印的技術需能防止各式各樣的攻擊，例如：一般無意者的影像縮小、放大、處理、壓縮、旋轉或是有意者的竄改及移除。

2.2.5 安全性

在早期的技術只有著重於把資料隱藏起來就可以了，並無考慮到駭客能夠藉著逆向工程的反組譯，研究演算法來把浮水印移除，所以浮水印的技術在這裡也必需符合密碼學上重要的：卡卓夫定律，此一定律在定義密碼演算法的安全性，是在密碼鍵上而不是演算法，唯有如此才能夠讓演算法公開為大眾檢驗其安全度，並且不怕逆向工程的攻擊。

2.3 完整的數位浮水印系統架構

一般來說，完整的數位浮水印系統架構可以分成以下浮水印嵌入、浮水印取出、浮水印偵測或驗證三個部份[14]，如下簡述：

2.3.1 浮水印嵌入

目前主要研究如何把原影像混合編碼的方法，與浮水印的資料，以及決定浮水印資料的隱藏位置，有離散小波轉換、離散餘弦轉換...等，這些方法的最終目的是要讓浮水印的資料，在原始影像之中具有不容易察覺性以及強韌性，讓人們沒辦法察覺到影像的差異性，

以及防止各種人為的破壞。

2.3.2 浮水印取出

浮水印的嵌入原影像之中，可以藉由使用者的私密鍵，以及抽取出影像的特徵，做為種子用來嵌入的反向動作把浮水印取出。

2.3.3 浮水印偵測或驗證

可以偵測出影像裡面含有的浮水印，並且可以證明取出的浮水印和原先嵌入的相同或者相似一樣。

2.4 浮水印的應用

數位浮水印的特性需求程度，依應用的領域要求目標不同而有所不一樣，分別舉例如下[15]：

2.4.1 影像資料庫的搜尋

一般來說，要搜尋影像比文字的查詢要困難許多，由於文字的搜尋演算法較簡單，而且條件也較明確，變化的因素較小。而影像則不是，因此對於非文字的檔案，可以將關鍵字或者內容的說明，利用浮水印的形式附加在檔案之中，以利方便而且快速的搜尋。

2.4.2 秘密通訊通道

不同於密碼學的加密，在於把訊息編碼混亂過後，使窺伺者無法知道真正的訊息意義，資訊隱藏的秘密通訊通道，就是在建立讓人無法發覺有保密這回事的通道，假如訊息的本身在隱藏前，先加密後再來傳送，就有雙重的保障。此應用比較要求於有限的頻寬內，可傳送更多的資料，應用於軍事上高度保密的需求。

2.4.3 認證

可使用在信用卡、金融卡上防止被偽造冒用；也可以應用在數位相機把日期嵌入在相片上。

2.4.4 所有權保護

把授權或版權的訊息隱藏於多媒體的內容中，例如：被侵權時，就能從隱藏的授權或者版權的訊息，證明為其所有或者是由何人流出，以採取法律的行動；另外也可以防止拷貝，例如：DVD 的拷貝管理系統機制，會在浮水印裡面含有控制的訊息，標記此一 DVD 為不可以拷貝、可以自由拷貝、或者是只可以拷貝一次。此一應用隱藏的訊息，不會遭受惡意的攻擊或者一般訊號的轉換處理而被破壞；對

於容量的要求也不會很大。

2.4.5 隱藏性標題

病人的身份以及病情的私密資料，隱藏在醫學診斷的影像之中，以避免外加性的標籤記錄，暴露了個人的隱私或者是不小心的張冠李戴而產生了錯誤。此一應用特別要求的隱藏訊息，不會影響到診斷影像的品質，以避免重要的特徵被模糊；另外也可以做為多媒體的索引標誌，以及以內容為主的搜尋存取。

3. 陸軍步兵火炮射擊

在陸軍步兵軍事火炮射擊的時候，都會利用到無線的通信以及有線的通信，來做為火炮射擊時連絡射擊指揮及射擊陣地要射擊目標（敵目標）的方向以及方位角...等射擊的相關資訊。

陸軍步兵火炮射擊的時候，其各項諸元的相關位置分別區分為火炮陣地、觀測所、前進觀測兵、射擊目標區、基準點等，如圖 1 所示。

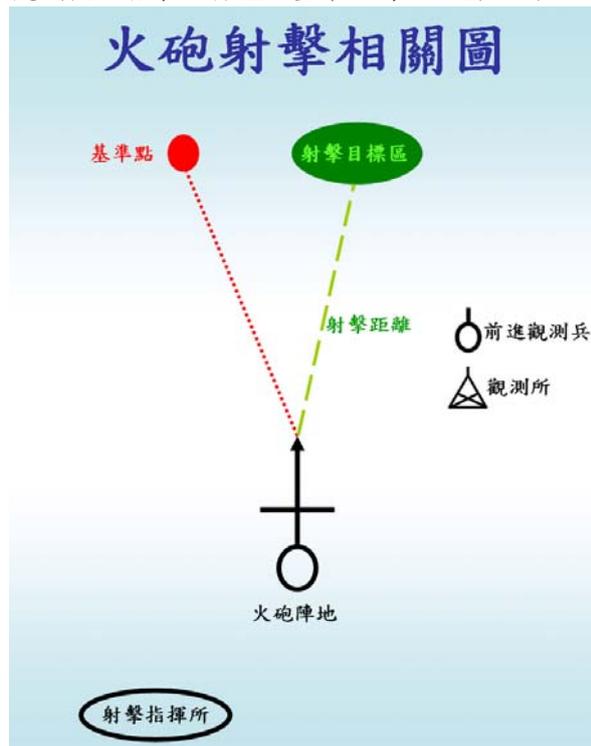


圖 1 火炮射擊相關圖[5]

陸軍步兵火炮射擊之前會選定前方一明顯物做為基準點，當前進觀測人員（前進觀測兵、前進觀測官、觀測所）發現到有敵目標（射擊目標區）的時候，會以基準點為主，回報以基準點為主的相關數據傳回到後方的射擊指揮所，射擊指揮所的人員則計算火炮陣地射擊的相關數據並下達射擊命令。

4. 蜜蜂的特性介紹

4.1 蜜蜂與花的關係

蜜蜂長大轉變為成蟲的時候可區分成三個種類：雄蜂、工蜂及后蜂[6]，如圖 2 所示。



圖 2 蜜蜂成蟲[7]

而蜜蜂和花的關係非常的密切。蜜蜂從花的身上得到蜜蜂所有的營養補給。當蜜蜂由花朵採集淡味花汁時，也同時將雄蕊花朵的花粉，沾於蜜蜂胸腹部的短毛上面。蜜蜂會將這一些花粉，刷到後腿的長毛上面，積成花粉袋籃。當蜜蜂飛至另一朵花採集花汁的時候，身上的花粉就會有一些花粉就自然地，黏到花朵雌蕊的子宮上面，使這一些花朵產生新的種子而達到花朵的傳宗接代。蜜蜂並沒有聰明到製造一把刷子，將所攜帶的花粉刷在花朵雌蕊上面。但是蜜蜂卻曉得在採了一種花朵的花汁和花粉後，會盡量飛到同一種的另一朵花，去做相同的事情。當蜜蜂在這樣毛手毛腳刷花粉的時候，也同時的替這一種花來做媒合。

當然，蜜蜂並不是專門要幫忙這一些花朵相親，蜜蜂主要的目地是要為了自己以及家族的溫飽而著想。自然界配合得如此巧妙，蜜蜂是花朵的恩人，而花朵也是蜜蜂的恩人，彼此互惠。但是，蜜蜂也必須要有相當的能耐才能夠完成此一任務。環境好、氣候好的時候，蜜蜂可以知道要如何運用最節省體力的最短程路線，採集最高數目花朵的花汁以及花粉。但是，當天氣慢慢變冷、花源缺乏的時候，蜜蜂也能夠飛到約十公里外去覓食，假如用體重大小為比例，這相當於人類跑到大概一千三百公里外去找食物，實在令人佩服。

4.2 蜜蜂間通信的方法

根據 Von Frisch 教授[8]獲諾貝爾獎的研究報告，蜜蜂的「大家告訴大家」告知花源的位置所在主要是利用跳舞的方式來表達的，如圖 3 所示。如果「好花」就位於蜂巢的附近（約 100 公尺以內時），蜜蜂就會跳起圓圈舞，就是繞順時針方向的小圓圈，再來繞逆時針方向的小圓圈，一圈又一圈。讓其他的蜜蜂同伴知道，花源大概在 100 公尺以內，一定能夠找得到。假如花源在比較遠的地方，蜜蜂就會跳起搖擺舞，蜜蜂的頭朝著花朵的方向急速搖擺肚

腹部，每秒鐘大約 13 次，搖擺之後向前幾步，順時針方向繞半圈，又朝著花朵的方向跳肚皮舞，再向前幾步，再以逆時針的方向繞半圈，回到開始的方位又跳起肚皮舞。這樣子的舞步就形成了一個阿拉伯數字 8 字形的圖案，兩個半圓圈之間的直線方向就是花源的方向，而這個直線的方向，與蜜蜂蜂巢出口和太陽相連的直線方向之間的角度，就是其他蜜蜂同伴出巢之後，根據太陽定位而必須要採用的飛行角度。這一種 8 字形的搖擺舞一再重複，直到蜜蜂覺得該看的蜜蜂同伴都看到了，蜜蜂就去將攜回的花汁勝利品交給其他的蜜蜂，或者自己找到儲存花粉或者花蜜的蜂窩堆積進去，之後又孜孜不倦地飛出去繼續勞力了，一天大概做 10 次左右[9]。

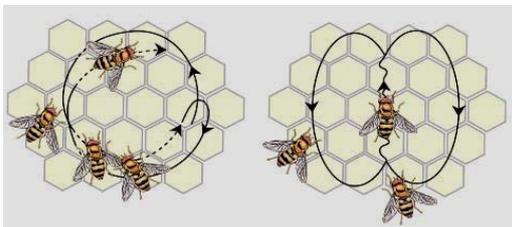
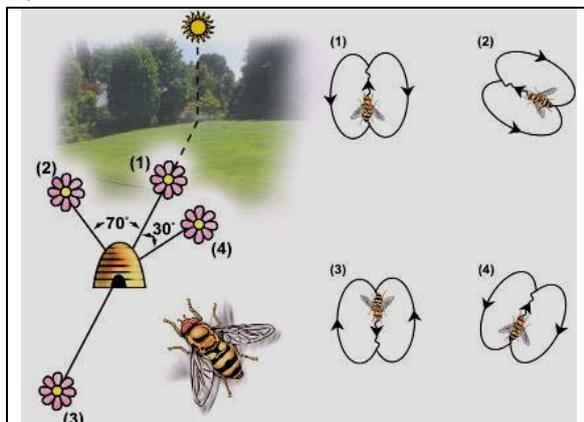


圖 3 左為圓圈舞，右為搖擺舞[9]

4.3 花源目標與蜂巢的關係

蜜蜂發現到花源（目標）之後，就會開始跳舞通知其他的蜜蜂，蜜蜂在蜂房以搖擺舞報告其他蜜蜂同伴花源的地點以及方向，如圖 4 所示。



- (1) 太陽在蜂巢正前方，目標與太陽同方向。
- (2) 目標在太陽及蜂巢連線左邊 70 度方向。
- (3) 目標與太陽反方向。
- (4) 目標在太陽及蜂巢連線右邊 30 度方向。

圖 4 蜜蜂在蜂房以跳舞告知花源地點方向[9]

4.4 花源目標距離蜂巢的關係

通報花源距離信息的蜜蜂利用搖擺肚腹的方式，來告知花源距離蜂巢有多遠。當蜜蜂回到朝花源的方向跳肚皮舞的時候，搖擺肚皮

的次數越多，就是代表花源離蜂巢的距離越遠。當蜜蜂搖擺跳舞的時候，並會同時磨擦雙翅產生大約三十分之一秒長的音響，大概能夠讓太擁擠的觀眾也可以收聽到花源距離的報告。蜜蜂們會在旁邊觀察 5 至 10 秒鐘之後，蜜蜂們就會飛離蜂巢，照著報佳音之蜜蜂的優良溝通，大多很快地就可以找到這一些好花的花朵。

也有不一樣種類的蜜蜂，是利用繞搖擺舞圈子的速度，來告知其他蜜蜂同伴花源離蜂巢的距離，距離越遠的時候就會繞得越慢，距離越近的時候繞得越快，例如：在離蜂巢 180 公尺附近有花源，這樣蜜蜂在 15 秒鐘裡，就繞了 7 圈，但是 6.4 公里外的花源，蜜蜂 15 秒鐘內，才繞了兩個 8 字圈；其他的蜜蜂同伴看到這種無精打采地通報，除非蜂巢家裡面有無米為炊之憂，去的同伴自然就會減少了。所以報信以及收信的蜜蜂都非常聰明。依據科學家仔細研究的結果，蜜蜂跳搖擺舞，通報同一花源之方向和遠近的時候，有時候會因為不同的蜜蜂會有一些少許的差異。這並不是因為有一些蜜蜂的資質太差了，而是由於出去覓食的蜜蜂年齡有差別。蜜蜂們擔任採食任務的年紀大約都在 10 到 60 天大。兩個月大的蜜蜂已經是年邁的老蜜蜂，跳起舞來就不像 10 天大的青春少女充滿了活力。而且加上因為風向以及風力，也會讓不同的蜜蜂作略有不同的報告。所以，在蜂巢的蜜蜂也在觀察了幾隻回家通報使者的跳舞之後，在心裡做了統計學的平均，才會飛出蜂巢去尋花源，又依據太陽的方位與報告蜜蜂指示的角度而定方向，通常很快地就找到了花源的所在位置。蜜蜂返回蜂巢的時候，仍然依據太陽的方位而定出回家的方向。蜜蜂們並沒有拿出一把尺出去測量距離，而是根據返回蜂巢的時候，體力需要消耗多少而估計算出花源距離蜂巢有多遠，回去告訴其他的蜜蜂同伴。

因此，雖然在蜂房跳舞通報的時候，看不到、也嗅不到花源，蜜蜂卻可以依據自己良好的記憶，以及高明的推論，算出太陽與花源之間的角度，並定出在這段時間中太陽在天空已經移動了多遠，並且舞出花源的方向以及距離遠近。

5. 浮水印加入蜜蜂演算法保護通訊

在陸軍步兵軍事火射擊的時候，都會利用到無線通信以及有線通信，來做為射擊時連絡射擊陣地要射擊目標的方向以及方位角...等

射擊資訊，但是有線通信最害怕線路有所斷線或者是被截聽，因為派人員出去查線非常的費時又非常的麻煩，要是於戰時未查到斷線的地方就陣亡了，就必須要再派其他人員出去查線，所以非常的危險，影響個人的生命安全。而無線通信最害怕的是被截聽，雖然於通話的時候，會加有密語在通訊裡面，但是只要被敵方的人員截取到，一定會想出辦法破解的，所以就利用蜜蜂的特性結合浮水印的技術設計出一套好用又能保密的通訊系統。

5.1 蜜蜂演算法運用

陸軍步兵軍事火射擊時，一些相關的位置，就如同蜜蜂尋找花源有點相似，而觀測人員（前進觀測兵、前進觀測官、觀測所）就如同尋找花源的蜜蜂負責回報目標，射擊的火炮陣地就如同蜜蜂的蜂巢一樣，射擊目標區就如同花源目標一樣，火炮的射擊基準點就如同蜜蜂以太陽為基準點一樣，其示意圖如圖 5 所示。

蜜蜂與火炮射擊之相關性

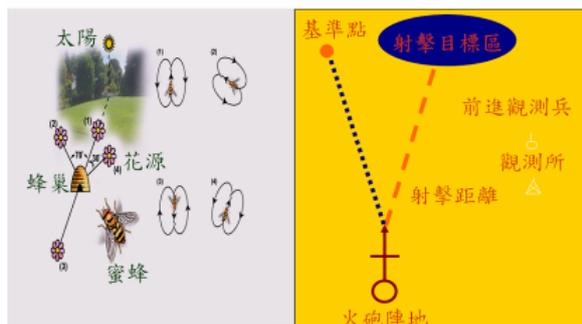


圖 5 蜜蜂與火炮射擊相關性

當前進觀測人員（前進觀測兵、前進觀測官、觀測所）發現到有敵目標的時候，會回報相關的數據傳回到射擊指揮所，而蜜蜂發現花源的時候，也是回報相關的數據回到蜂巢。所以蜜蜂尋找花源與陸軍步兵火炮射擊兩者的關係非常相像，所以利用蜜蜂回報花源時候的特性，設計一 PDA 及主系統，讓前進觀測人員（前進觀測兵、前進觀測官、觀測所）來使用 PDA，射擊指揮所的人員則使用主系統來下達射擊命令。

5.2 結合浮水印技術於通訊保密

當前進觀測人員（前進觀測兵、前進觀測官、觀測所），利用 PDA 回報射擊目標區的相關方位角及距離時，只要於 PDA 上面畫上橢圓的角度以及圈數，橢圓形的角度，就代表火炮陣地和火炮射擊基準點，所連成的假想基準線；和火炮陣地與射擊目標區，所連成的假想目標線，兩線所夾的角度就是橢圓形的角度。

而所畫的橢圓形圓圈的圈數，就代表射擊陣地距離射擊目標區的距離，示意圖如圖 6 所示。



圖 6 PDA 上畫橢圓角度及圈數示意圖

再來點選 PDA 內建的圖片，將剛剛資訊利用浮水印的技術儲存到圖片之中，然後按下發送，示意圖如圖 7 所示。



圖 7 隱藏發送資訊示意圖

當後方的射擊指揮所主機系統收到資訊的時候，必須要有解浮水印的機制，才可將隱藏於圖片之中的火炮射擊資訊抽取出來，示意圖如圖 8 所示。

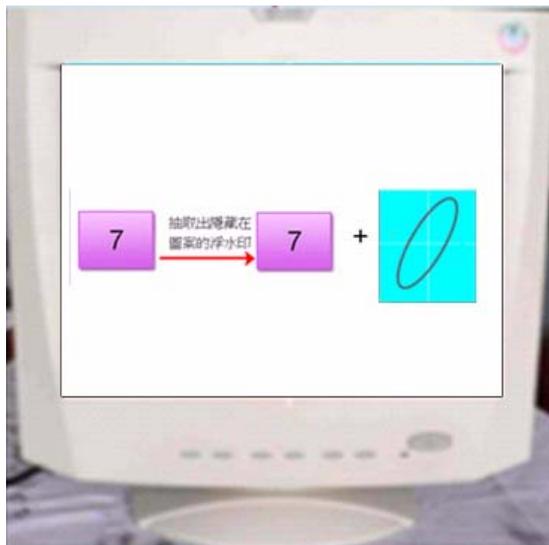


圖 8 將隱藏於圖片中的資訊抽取出來示意圖

如果沒有解浮水印的系統將有用的火炮射擊資訊抽取出來，所獲得的資訊只是一張無意義的圖片而已，另外就算抽取出來之後，沒有蜜蜂演算法系統將火炮射擊資訊加以解密換算，所獲得的資訊只是另一張無用的橢圓形圖片罷了，所以射擊指揮所的主機系統必須要利用有浮水印的系統先將隱藏於圖片之中的火炮射擊資訊抽取出來，再利用蜜蜂演算法的系統將其火炮射擊資訊換算出要射擊的角度以及距離，並自動將火炮要射擊的各項調整諸元圈數計算出來，示意圖如圖 9 所示。

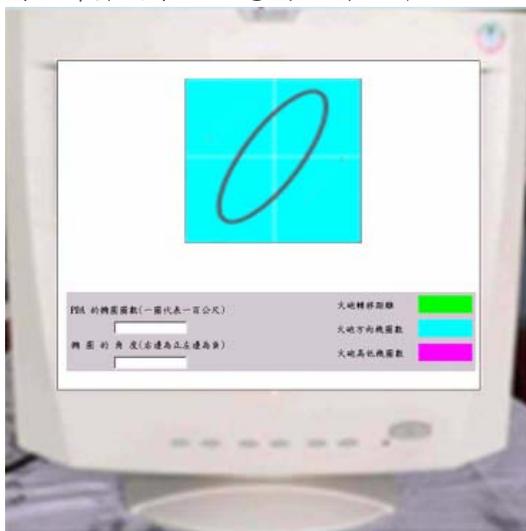


圖 9 自動將射擊各諸元計算出來示意圖

5.3 小結

利用蜜蜂演算法結合浮水印技術來發展出 PDA 與主系統，有兩層的保護，若沒有經過有蜜蜂演算法及浮水印技術結合的主系統解密，只是獲得兩張無用的圖片，就算解的了第一層浮水印隱藏的加密，到了第二層無法再利

用蜜蜂演算法解密，還是一張無意義的圖片，所以有雙重保護的蜜蜂演算法結合浮水印技術之主系統，對於陸軍步兵的火炮射擊步驟更為簡化，又能夠確保通訊的安全。

6. 未來展望

現今已經有一些應用動物的特性在某一些地方了，發展出螞蟻演算法及鳥類演算法還有螳螂演算法...等，例如：最佳化就有應用到螞蟻的特性以及鳥類的特性，而軍中也有將動物的特性，應用於體能戰技之中。但是還有更多動物的特性，可以運用在更多的地方，只要多加注意動物的某些特性，相信在未來一定有更多動物的特性，會應用在更多的工程貢獻上。

7. 結果與討論

在陸軍步兵軍事火射擊的時候，都會利用到無線通信以及有線通信，來做為射擊時連絡射擊陣地要射擊目標的方向以及方位角...等射擊資訊，但是有線通信最害怕線路有所斷線或者是被截聽，因為派人員出去查線非常的費時又非常的麻煩，要是於戰時未查到斷線的地方就陣亡了，就必須要再派其他人員出去查線，所以非常的危險，影響個人的生命安全。而無線通信最害怕的是被截聽，雖然於通話的時候，會加有密語在通訊裡面，但是只要被敵方的人員截取到，一定會想出辦法破解。利用浮水印加入蜜蜂演算法來發展出保護通訊的系統，讓陸軍步兵的火炮射擊步驟更為簡化，避免人員的計算錯誤，確保通訊的安全，深信本研究可確保通訊保密的安全。

參考文獻

- [1] Dorigo, M, maniezzo, v., and colornj, A., "the ant system: Optimization by a colony of cooperating agent" IEE Transactions on Systems, Man, and cybernetics-Part B, Vol126-1, PP.29-41.
- [2] 鄭富升、涂嘉勝、陳慶鴻、呂昌鴻、林崇倫,「螳螂演算法的發展與應用」, 行政院國家科學委員會補助專題研究計畫, NSC-95-2221-E-230-037, 95 年 8 月 1 日至 96 年 7 月 31 日。
- [3] <http://e-life.dahan.edu.tw/phpbb2/viewtopic.php?t=881&sid=cae8609042334f566a2c9d5c6200d3b5>。
- [4] 李敏祺,「山本大將的殞落」, 清流月刊, 中華民國 92 年 10 月號。

- [5] 蔡宗甫、鄭平守、趙宜婷、黃榆粧、鄭宇涵、陳慧雯，「應用蜜蜂演算法於軍事射擊之通訊保密」，2006 全國電信研討會，2006 年 12 月 2 日。
- [6] 蘇文博蜂巢之奧秘—蜜蜂、花源與設計 (上) 神奇的蜜蜂 <http://www.teamtc.org.tw/health/LIFE/%E8%9C%82%E5%B7%A2%E4%B9%8B%E5%A5%A7%E7%A7%981.htm>。
- [7] http://episte.math.ntu.edu.tw/articles/sm/sm_27_07_2/page2.html。
- [8] Karl Von Frisch, Dancing Bees: An Account of the Life and Senses of the Honey Bee. The flight paths of honeybees recruited by the waggle dance, Nature 435, May 2005, pp.205-207.
- [9] 蘇文博蜂巢之奧秘—蜜蜂、花源與設計 (中) 明確的示知 <http://www.teamtc.org.tw/health/LIFE/%E8%9C%82%E5%B7%A2%E4%B9%8B%E5%A5%A7%E7%A7%982.htm>。
- [10] 謝欣宏(1999),「以電子浮水印為基礎的數位著作權保護之研究」，中正理工學院電子工程研究所碩士論文。
- [11] Podilchuk, C.I.,Zeng,W., "Image-Adaptive Watermarking Using Visual Models "IEEE Journal on Selected Areas in Communications, vol. 16,No.4, May 1998.
- [12] Bender, W., Gruhl, D., and Morimoto, N., "Techniques for data hiding" . In Proc. Of SPIE, vol.2420, pp.40, Feb, 1995.
- [13] 黃興銘(2001),「高安全性的數位影像浮水印技術研究」，國立高雄第一科技大學電腦與通訊工程系碩士論文。
- [14] 戴敏倫、李素瑛、周義昌，「多媒體資訊安全：數位浮水印」，電子月刊，1999 年 3 月。
- [15] 蔡宗甫、鄭平守、鄭宇涵、趙宜婷、陳慧雯，「水印指紋辨識系統」，TBI 2006 台灣商管與資訊研討會，2006 年 11 月 1 日。