**數位影像處理期末報告**

**研究主題: 改良式LSB取代法用於彩色影像資訊隱藏之研究**

姓 名：許OO 學 號：MXXX4016

**Abstract**

資訊隱藏(Steganography)是透過多媒體的影像處理方式，讓數位資訊可以安全的在網路上傳遞以保全機密資料。在數位影像裡，每個像素點最低有效位元(Least Siginificant Bit，LSB)的改變在人類視覺系統較不易察覺，可透過修改影像像素最後幾個位元這種對影像的影響最小的方式達到嵌入資料的目的。本篇研究將以Neamah等人在2020提出的LSB演算法為基礎，嘗試改良傳統LSB取代法，將需要隱藏的文字訊息透過加密方式嵌入原始彩色影像，以期在維持影像品質與增加資料藏量之間取得平衡。

***Keywords:*** *LSB Substitution, Steganography*

1. **Introduction**
   1. 資訊隱藏（Steganography）

在網路時代訊息傳遞與溝通需求大增，如何將機密資料安全且快速的傳送是重要的議題。資訊隱藏技術是將各種形式的重要資料加密後傳遞，讓人不易察覺機密資訊的存在，可達到資訊隱藏、保護的作用。

數位影像資訊隱藏的過程可分為嵌入（embedding）與取出（extracting）兩個階段：第一階段為秘密資料的嵌入，在承載影像（cover image）利用未公開的加密方法將秘密資料（secret data）嵌入後，產生偽裝影像（stego image）；第二階段為秘密資料的取出，利用解密的方法將偽裝影像裡的秘密資料取出，還原成原本的秘密資料，如圖1。

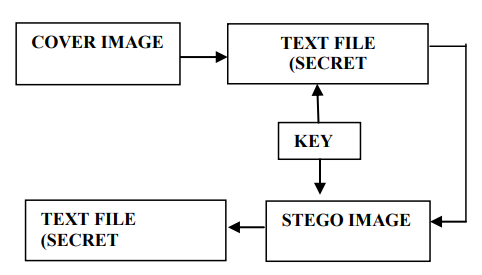


圖1：資訊隱藏過程 [1]

* 1. 最低有效位元取代法(Least Significant Bit Substitution，LSB)
     1. LSB 取代法

在點陣圖中，每張圖是由像素所組成，每個像素的色彩由RGB三原色所組成，每個顏色介於0-255之間，轉成二進位數字後，每個色彩各自使用 8-bit 來儲存顏色數值，故色彩的總長度為24bits，共有 224=16777216種顏色，通常稱為真實色彩（True-Color）的數位影像[3]。

最高有效位 (Most Significance Bit，MSB)是一個二進位數字中最左側的位元(即最高位)，最低有效位元(Least Siginificant Bit，LSB)是一個二進位數字中最右側(即最低位)的位元，MSB數值的改變具有明顯的影響，LSB數值的改變影響極小。

LSB取代法是將一個需要隱藏的資訊取代承載影像（cover-image）的最低有效位，由於最低有效位元的變化對於影像像素值的大小影響有限，用秘密資料取代產生的stego-image讓人類肉眼不足以辨識出兩者之間的差異，具有較高的隱蔽性。在彩色影像RGB三個通道中，利用LSB取代法通常以3-3-2的方式將一個8bits的資料取代彩色影像某一個像素的RGB最低有效位[2]。舉例來說，一個原始彩色影像某一個像素值為(225,100,100)=(11100001,01100100,01100100)，要藏入的資料是“a” = 011000012(ASCII value 97)，用LSB取代法藏完的像素值是(11100011, 01100000, 01100101)= (227, 96,101)。可發現原始影像與偽裝影像之像素值差異不大，不容易看出區別 [3]。

* + 1. 改變嵌入順序的LSB演算法

Rawat等人在2013提出的改良式LSB演算法，是把秘密資料加上資料長度的訊息轉成二進位值後，將嵌入的位元數控制在每個像素的最後一個位元(1st LSB)，秘密資料嵌入順序為：第1個像素R通道的1st LSB →第2個像素R通道的1st LSB →第一個像素G通道的1st LSB →第二個像素G通道的1st LSB →第三個像素G通道的1st LSB →第一個像素B通道的1st LSB →第二個像素B通道的1st LSB →第三個像素B通道的1st LSB [1]。

舉例來說，一個原始彩色影像：  
像素1 (225,100,100) = (11100001,01100100,01100100)  
像素2 (224,101,102) = (11100000,01100101,01100110)  
像素3 (225,75,80) = (11100001, 01001011, 01010000)，要藏入的資料是“a” = 011000012(ASCII value 97)，用此改良式LSB取代法藏完三個像素值依序是：  
像素1(1110000**0**,0110010**1**,0110010**0**) =(224,101,100)  
像素2(1110000**1**,0110010**0**,0110011**0**) =(225,100,102)  
像素3(11100001,0100101**0**,0101000**1**) =(225,74,81)

* + 1. 使用Xnor判斷的LSB演算法

Neamah等學者在2020提出利用原始影像像素R、G、B右邊第二個位元(2nd LSB)值轉十進位後，取3的餘數來決定嵌入資料至哪一個色彩通道，秘密資料經由某一金鑰做Xnor加密後得到的加密資料依照每個像素的讀取順序，取代該像素RGB獲選通道的最右邊位元(1st LSB)。

此方法在嵌入階段可分為兩大步驟，第一步驟為資料嵌入通道的選擇，舉例來說，原始影像像素1（11011010, 10010101, 10011011）=（218, 149, 155），其RGB的2nd LSB為1012=510，取3的餘數得到2，表示選擇嵌入至B通道(R：餘數0、G：餘數1、B：餘數2)

第二步驟為加密資料的準備，例如一個原始秘密資料10011010，加密金鑰01011100，作Xnor運算後得到的加密資料是00111001，以此加密資料的第一個位元0取代像素1之B通道1st LSB，像素值變更為（11011010, 10010101, 10011010）=（218, 149, 154）。前四個加密資料位元取代的過程如圖 2。

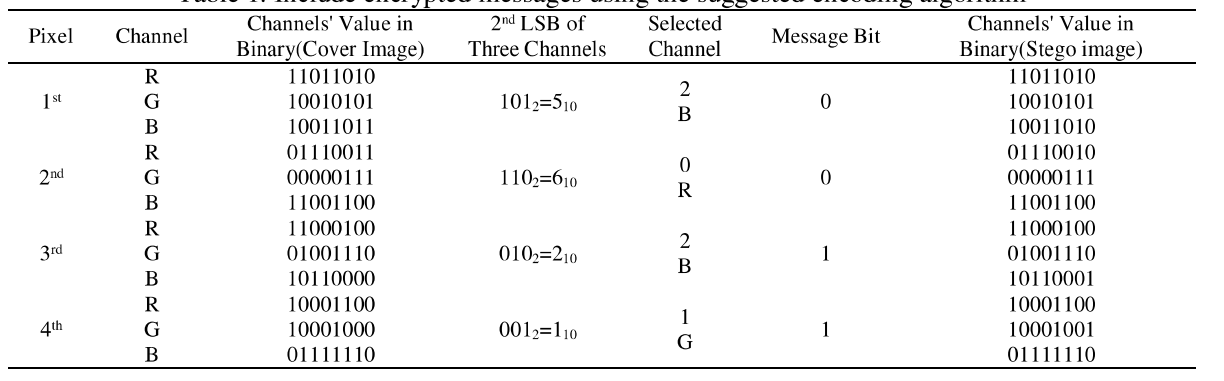


圖 2：加密資料取代過程 [2]

1. Our Propose(需要詳細說明個人所提出的方法)

傳統的LSB方法是在原始影像RGB通道的最右邊位元依序取代為目前需要隱藏的秘密資料，但由於此種方法過於簡單，秘密資料藏入規則極易被識破並取得機密訊息。Neamah等人在2020年提出將資料與秘密金鑰作Xnor運算加密後做為藏入影像的秘密訊息，取出時需要知道當初加密金鑰是甚麼才能正確解密取出原始資料，提升資料傳遞的安全性；另外以原本像素RGB三個通道的2nd LSB取3的餘數計算再決定資料嵌入RGB哪個通道的選擇方法，不需要另外用Location Map紀錄哪些像素值曾被改變、原始藏入的資料長度等訊息，也讓取出資料時更有效率。然而只選擇RGB其中一個通道來取代，每個像素只能藏一個位元資料，藏量固定無法增加為此方法的缺點，以一個512\*512的全彩影像為例，總藏量固定為512\*512\*1=262,144位元。

因此本研究同樣採用Neamah等人提出的Xnor加密法，資料的取代方式改為依序以RGB每兩個通道的2nd LSB作Xor運算，若為True則取代該通道1st LSB位元，False不做改變，期望能增加資料的藏量，並維持一定的影像品質。取出資料時也能以現有像素的2nd LSB得知當初是否有藏入資料，有效地取出原本秘密訊息。

由表1可知，每一個像素RGB通道的2nd LSB有八種可能組合，其中全為0或全為1時不藏入資料，出現的機率為四分之一，另外六種組合皆能藏入2個位元資料，出現的機率為四分之三，以一個512\*512的全彩影像為例，總藏量最佳情況為512\*512\*2=524,288位元，總藏量可能性為512\*512\*1.5=393,216位元。

表1：RGB通道選擇

| R-G-B  (2nd LSB) | Xor (R-G) | Xor (G-B) | Xor (B-R) | Replace  1st LSB | Embedded  bit |
| --- | --- | --- | --- | --- | --- |
| 0-0-0 | 0 | 0 | 0 | － | 0 |
| 0-0-1 | 0 | 1 | 1 | G、B | 2 |
| 0-1-0 | 1 | 1 | 0 | R、G | 2 |
| 0-1-1 | 1 | 0 | 1 | R、B | 2 |
| 1-0-0 | 1 | 0 | 1 | R、B | 2 |
| 1-0-1 | 1 | 1 | 0 | R、G | 2 |
| 1-1-0 | 0 | 1 | 1 | G、B | 2 |
| 1-1-1 | 0 | 0 | 0 | － | 0 |

舉例來說，一個原始秘密資料10011010，加密金鑰01011100，作Xnor運算後得到的加密資料是00111001，原始影像像素1（11011010, 10010101, 10011011）=（218, 149, 155），其R-G的2nd LSB為1-0，Xor(1,0)=1，表示選擇嵌入至R通道，以加密資料的第一個位元0取代像素1之R通道1st LSB；其G-B的2nd LSB為0-1，Xor(0,1)=1，表示選擇嵌入至G通道，以加密資料的第二個位元0取代像素1之G通道1st LSB；其B-G的2nd LSB為1-1，Xor(1,1)=0，表示選擇不嵌入至B通道。第一個像素處理完像素值為（11011010, 10010100, 10011011）=（218, 148, 155）。前四個像素資料嵌入的過程如表 2。

表 2：資料嵌入過程

| Pixel | Channel | Channel’s Value in Binary (Cover Image) | Exclusive OR of Two Channels’ 2nd LSB | Selected Channel | Message Bit | Channels’  Value in Binary (Stego image) |
| --- | --- | --- | --- | --- | --- | --- |
| 1st | R | 11011010 | Xor(1,0)=1 | R | 0 | 1101101**0** |
| G | 10010101 | Xor(0,1)=1 | G | 0 | 1001010**0** |
| B | 10011011 | Xor(1,1)=0 | - | - | 10011011 |
| 2nd | R | 01110011 | Xor(1,1)=0 | - | - | 01110011 |
| G | 00000111 | Xor(1,0)=1 | G | 1 | 0000011**1** |
| B | 11001100 | Xor(0,1)=1 | B | 1 | 1100110**1** |
| 3rd | R | 11000100 | Xor(0,1)=1 | R | 1 | 1100010**1** |
| G | 01001110 | Xor(1,0)=1 | G | 0 | 0100111**0** |
| B | 10110000 | Xor(0,0)=0 | - | - | 10110000 |
| 4th | R | 10001100 | Xor(0,0)=0 | - | - | 10001100 |
| G | 10001000 | Xor(0,1)=1 | G | 0 | 1000100**0** |
| B | 01111110 | Xor(1,0)=1 | B | 1 | 0111111**1** |

取出資料階段，偽裝影像像素1（11011010, 10010100, 10011011）=（218, 148, 155），其R-G的2nd LSB為1-0，Xor(1,0)=1，表示當初在R通道有藏入資料，因此取出像素1之R通道1st LSB，得到加密資料第一個位元0；其G-B的2nd LSB為0-1，Xor(0,1)=1，當初在G通道有藏入資料，因此取出像素1之G通道1st LSB，得到加密資料第二個位元0；其B-R的2nd LSB為1-1，Xor(1,1)=0，表示當初在B通道未藏入資料。前四個像素取出資料的過程如表 3。

表 3：資料取出過程

| Pixel | Channel | Channel’s Value in Binary (Stego Image) | Exclusive OR of Two Channels’ 2nd LSB | Selected Channel | Message Bit |
| --- | --- | --- | --- | --- | --- |
| 1st | R | 11011010 | Xor(1,0)=1 | R | 0 |
| G | 10010100 | Xor(0,1)=1 | G | 0 |
| B | 10011011 | Xor(1,1)=0 | - | - |
| 2nd | R | 01110011 | Xor(1,1)=0 | - | - |
| G | 00000111 | Xor(1,0)=1 | G | 1 |
| B | 11001101 | Xor(0,1)=1 | B | 1 |
| 3rd | R | 11000101 | Xor(0,1)=1 | R | 1 |
| G | 01001110 | Xor(1,0)=1 | G | 0 |
| B | 10110000 | Xor(0,0)=0 | - | - |
| 4th | R | 10001100 | Xor(0,0)=0 | - | - |
| G | 10001000 | Xor(0,1)=1 | G | 0 |
| B | 01111111 | Xor(1,0)=1 | B | 1 |

1. **實驗結果(一定要有實驗數據佐證你的方法及貢獻)**

　 本次研究以大小512\*512的四張全彩BMP影像作為實驗對象，依序為Lena、Peppers、Baboon和Airplane，如圖3。

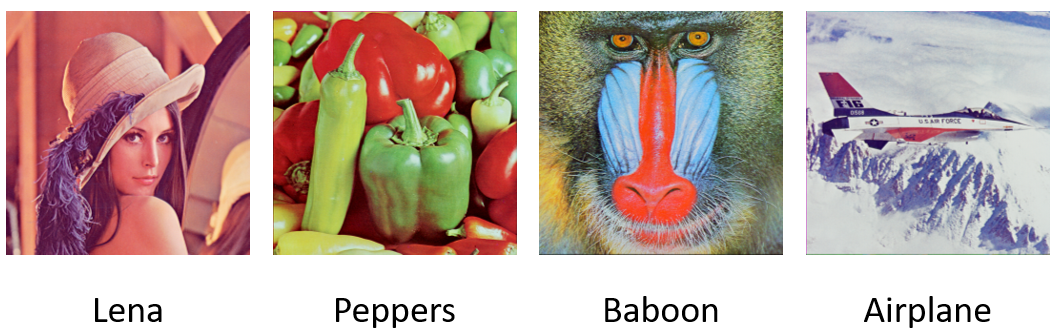


圖 3：Four Cover Images

圖4至圖7為嵌入20萬個位元資料後的偽裝影像與承載影像之像素值分布統計。圖4顯示Lena在藍色通道50-150值的改變較多，圖6顯示Baboon在RGB三個通道50-100值的改變較多，圖5和圖7 Peppers、Airplane兩張圖的變化則不明顯。

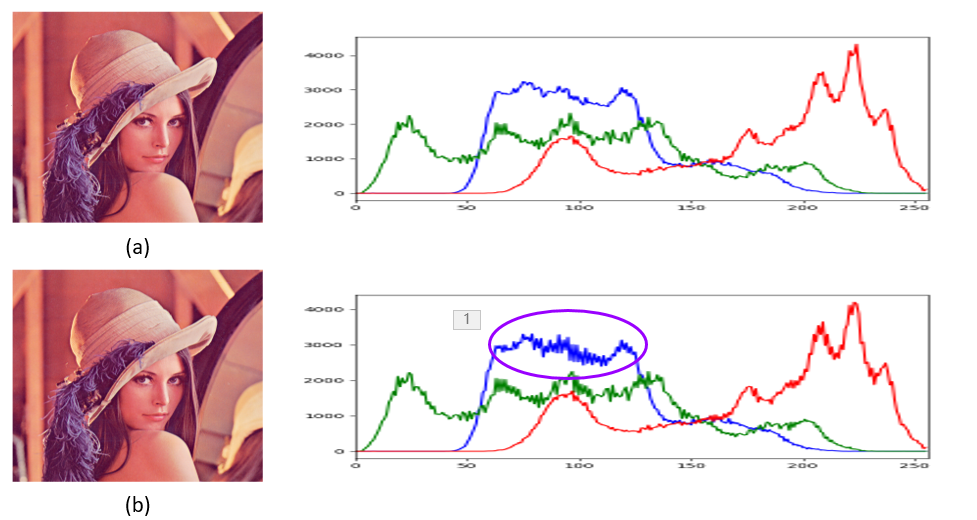


圖 4：(a) The original Lina image and RGB histogram (b) The stego image and RGB histogram(Secret text 200,000 bits)

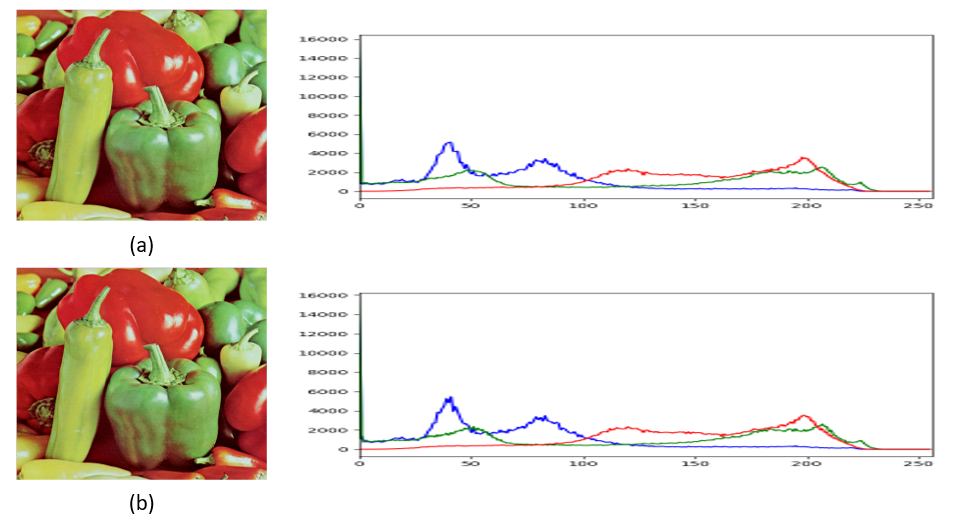


圖 5：(a) The original Peppers image and RGB histogram (b) The stego image and RGB histogram(Secret text 200,000 bits)

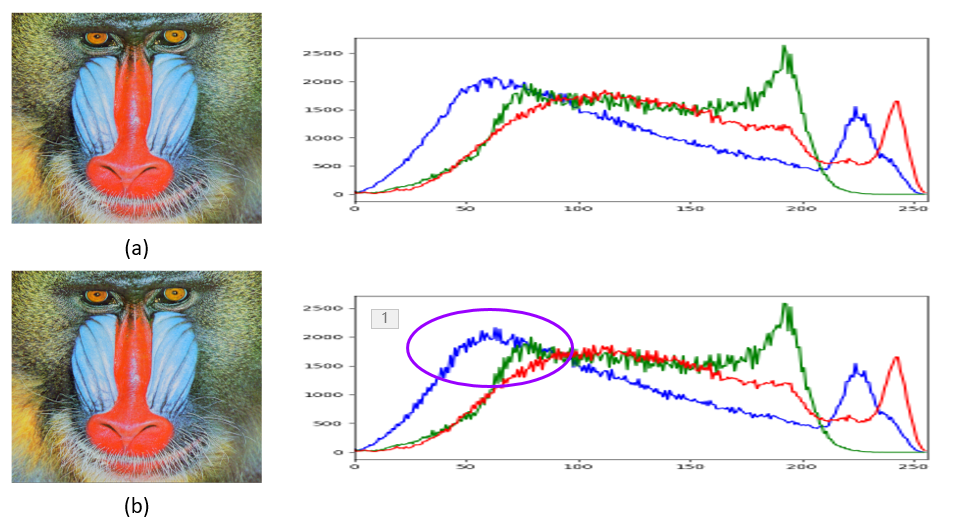


圖 6：(a) The original Baboon image and RGB histogram (b) The stego image and RGB histogram(Secret text 200,000 bits)

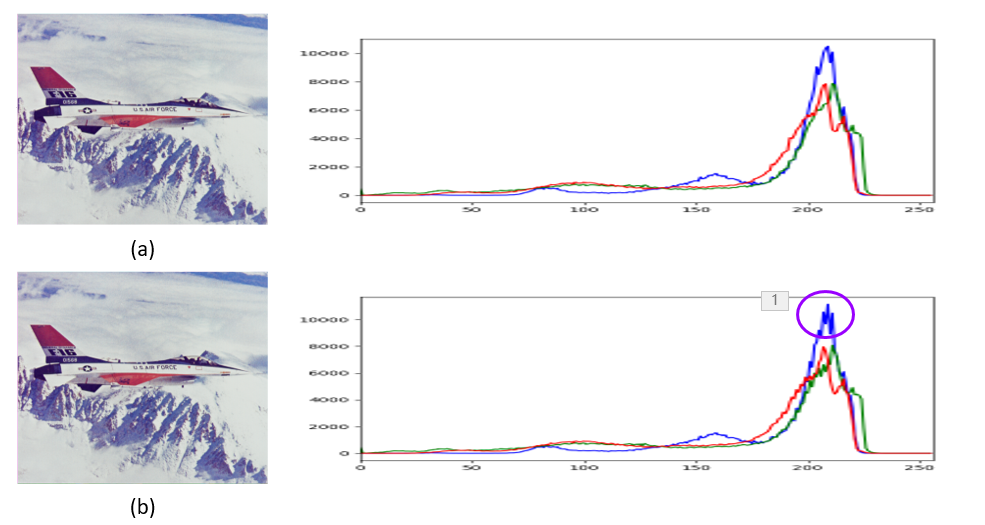


圖 7：(a) The original Airplane image and RGB histogram (b) The stego image and RGB histogram(Secret text 200,000 bits)

在藏入10萬與20萬位元文字資料後，本研究與Neamah等人提出的方法比較如表 4，Lena的影像品質兩個藏量皆佳，Airplane在10萬位元表現較優，Peppers和Baboon在20萬位元的品質為一致。四張圖計算後的平均影像品質與Neamah等人是相同的，顯示本研究的方法能維持一定的影像品質。

表 4：實驗結果－MSE與PSNR比較

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Color image size (512\*512)** | **Secret text 100,000 bits** | | | | **Secret text 200,000 bits** | | | |
| Neamah’s scheme[2] | | Proposed scheme | | Neamah’s scheme[2] | | Proposed scheme | |
| MSE | PSNR | MSE | PSNR | MSE | PSNR | MSE | PSNR |
| Lena | 0.0634 | 60.11 | 0.0629 | 60.14 | 0.1268 | 57.10 | 0.1260 | 57.13 |
| Peppers | 0.0640 | 60.07 | 0.0641 | 60.06 | 0.1278 | 57.07 | 0.1278 | 57.07 |
| Baboon | 0.0633 | 60.12 | 0.0634 | 60.11 | 0.1268 | 57.10 | 0.1269 | 57.10 |
| Airplane | 0.0637 | 60.09 | 0.0635 | 60.10 | 0.1273 | 57.08 | 0.1275 | 57.07 |
| Average | 0.0636 | 60.10 | 0.0635 | 60.10 | 0.1272 | 57.09 | 0.1271 | 57.09 |

在資料最大藏量計算方面，Neamah等人的方法固定最大藏量是262,144位元，以本研究提出的方法實際計算四張圖的藏量，如表5所示，四張圖可藏入的資料量皆優於前者，平均最大藏量為390,700位元，在資料的藏量確實有增加。

表 5：實驗結果－Maximum Embedded Capacity比較

|  |  |  |
| --- | --- | --- |
| **Color image size (512\*512)** | **Neamah’s scheme[2]** | **Proposed scheme** |
| Lena | 262,144 bits | 392,788 bits |
| Peppers | 262,144 bits | 387,394 bits |
| Baboon | 262,144 bits | 393,680 bits |
| Airplane | 262,144 bits | 388,940 bits |
| Average | 262,144 bits | 390,700 bits |

1. Conclusions(簡單的總結本專題研究的具體貢獻)

本研究參考Neamah等人在2020年提出的方法，同樣利用Xnor運算將資料加密，提升資料安全，另外資料藏入的方法仍維持最小位元取代法，利用人類視覺對影像輕微調整不易察覺的特性達到隱藏目的，維持偽裝影像品質。在資料藏入通道的選擇，利用彩色影像有RGB三個通道的特性，改以兩兩通道2nd LSB做Xor運算決定資料是否藏入該通道的方式，在實驗結果可以看出最大藏量明顯多於Neamah等人提出的方法。因此本研究方法可歸納出三個特色：

（1）透過資料加密方法保護資料，提升資料傳遞安全性。

（2）利用LSB取代法使影像像素值變化最少，維持良好影像品質。

（3）改變影像RGB通道藏入資料的選擇方式，提高資料最大藏入量。

**Reference(完整的參考文獻)**

|  |  |
| --- | --- |
| [1] | D.Rawat, V.Bhandari, "Steganography technique for hiding text information in color image using improved LSB method," *International Journal of Computer Applications,* vol. 67, no. 1, 2013. |
| [2] | R. M. Neamah, J. A. Abed, and E. A. Abbood, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," *International Journal of Electrical and Computer Engineering,* vol. 10, no. 1, 2020. |
| [3] | S.Singh, G.Agarwal, "Use of image to secure text message with the help of LSB replacement," *International journal of applied engineering research,* vol. 1, no. 1, 2010. |