

色彩科學導論與應用

Encryption Metrics-3 Correlation of Two Adjacent Pixels, v6

授課教師：王宗銘

2021/06/01

Assignment 13

量測原始影像或加密影像兩相鄰像素間之相關性(Correlation of Two Adjacent Pixels, CTAP)，可以得知加密演算法之成效。考慮某一色彩頻道，兩相鄰像素有三種模式，分別為 Horizontal Direction (HD), Vertical Direction (VD), and Diagonal Direction (DD)。

一般我們在量測 CTAP 時，可以取 pixel samples，文獻上有取 1000 點，2000 點，如此可加速計算。此次練習，我們盡可能的求出最多的 pixel samples，故我們並非對整張 image 做敘述統計(descriptive statistics)，而是對影像取非常多的 samples 來做推理統計(inferential statistics)。

假設一張 $M \times N$ 影像， M 代表水平像素量(Width)，其索引為 $0 \sim (M-1)$ ， N 代表垂直像素量(Height)，索引為 $0 \sim (N-1)$ 。令 $V(p, q)$ 代表某個位置 (p, q) 之像素值。三種模式分別敘述如下：

1. 水平模式，Horizontal Direction (HD):

$V(p, q)$ 之相鄰像素為 $V(p+1, q)$ ，如圖 1 所示。對於 HD，因為我們只看 (p, q) 的 **右方**，故我們限制 p 即可， q 無需限制，故 $0 \leq p \leq (M-2)$, $0 \leq q \leq (N-1)$ 。此代表 p 不能在影像的最右側的 column，因為在此情況， $p=M-1$ 導致我們無法找到對應的水平像素 $(p+1, q)$ 。

令 X 代表 $V(p, q)$ 在 HD 之所有像素， Y 代表對應 $V(p, q)$ 在 HD 之相鄰像素，則集合 X 、 Y 都內含 $(M-1) \times N$ 個像素。

X	X	X	X
X	(p, q)	(p+1, q)	X
X	(p, q+1)	(p+1, q+1)	X
X	X	X	X

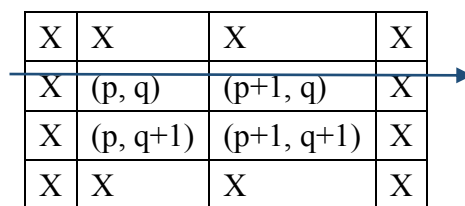


圖 1. 水平模式

2. 垂直模式，Vertical Direction (VD):

$V(p, q)$ 之相鄰像素為 $V(p, q+1)$ ，如圖 2 所示。因為我們只看 (p, q) 的 **下方**，我們限制 q 即可， p 無需限制，故 $0 \leq p \leq (M-1)$, $0 \leq q \leq (N-2)$ 。此代表 q 不能在影像的最下方的 row，因為這樣我們無法找到對應的垂直像素 $(p, q+1)$ 。

令 X 代表 $V(p, q)$ 在 VD 之所有像素， Y 代表對應 $V(p, q)$ 在 VD 之相鄰像素，則集合 X 、 Y 都內含 $M \times (N-1)$ 個像素。

X	X	X	X
X	(p, q)	(p+1, q)	X
X	(p, q+1)	(p+1, q+1)	X
X	X	X	X

圖 2. 垂直模式

3. 對角模式，Diagonal Direction (DD):

$V(p, q)$ 之相鄰像素為 $V(p+1, q+1)$ ，如圖 3 所示。因為我們只看 (p, q) 的右方與下方，我們同時要限制 p, q ，故 $0 \leq p \leq (M-2), 0 \leq q \leq (N-2)$ 。此代表 (p, q) 不能在影像的最右側 column 且也不能在最下方的 row，因為這樣我們無法找到對應的垂直像素 $(p+1, q+1)$ 。令 X 代表 $V(p, q)$ 在 DD 之所有像素， Y 代表對應 $V(p, q)$ 在 DD 之相鄰像素，則集合 X 、 Y 都內含 $(M-1)*(N-1)$ 個像素。

X	X	X	X
X	(p, q)	(p+1, q)	X
X	(p, q+1)	(p+1, q+1)	X
X	X	X	X

圖 3. 對角模式

整理歸納，我們得知：

水平模式：像素個數共有 $L=(M-1)*N$ 個。

垂直模式：像素個數共有 $L=M*(N-1)$ 個。

對角模式：像素個數共有 $L=(M-1)*(N-1)$ 個。

我們可以根據算式 1-6，計算得出 HD, VD, DD 之 X 與 Y 之相關係數(Correlation Coefficient)。正式的名稱是：皮爾森積動差相關係數 (Pearson product-moment correlation coefficient, PPMCC or PCCs)。詳細的說明，可以參見[1]。相關係數介於-1.0~+1.0 之間。相關係數越接近 0，代表兩像素間無相關。自然界原始影像的特性是：兩像素的相關係數應該較接近 1.0，代表兩像素間具有正相關。然而，我們希望做完影像加密後，兩像素間並無相關，如此才能增加影像的安全性。故其相關係數最好是 0。據此，我們可以藉由求出的相關係數，得知不同加密演算法的效能，進而客觀的比較演算法的優劣。

[1] J. L. Rodger and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," *The American Statistician*, vol. 42, no. 1, pp. 59-66, February 1988.
<https://www.jstor.org/stable/2685263?seq=1>

$\bar{x} = \frac{1}{L} \sum_{i=1}^L x_i$, (sample mean)	(1)
$\bar{y} = \frac{1}{L} \sum_{i=1}^L y_i$, (sample mean)	(2)
$\text{VAR}(X) = \frac{\sum_{i=1}^L (x_i - \bar{x})^2}{L-1}$ (sample variance)	(3)
$\text{VAR}(Y) = \frac{\sum_{i=1}^L (y_i - \bar{y})^2}{L-1}$ (sample variance)	(4)
$\text{COV}(X, Y) = \frac{\sum_{i=1}^L (x_i - \bar{x})(y_i - \bar{y})}{(L-1)}$ (sample covariance)	(5)
$\text{Correlation}(X, Y) = \frac{\sum_{i=1}^L (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^L (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^L (y_i - \bar{y})^2}}$ (correlation coefficient)	(6)

範例：

一張 $M \times N = 3 \times 3$ 影像之綠色通道像素值，可以使用表 1 顯示，此時像素(0,0)位於左上角(Top-Left Corner)。反之，我們也可使用如表 2 所示，此時像素(0,0)位於左下角(Bottom-Left Corner)。我們以 Top-Left 方式來討論。

表 1. $H \times V = 3 \times 3$ 影像				表 2. $H \times V = 3 \times 3$ 影像			
	0	1	2		0	1	2
0	88	27	196	2	183	113	125
1	21	61	12	1	21	61	12
2	183	113	125	0	88	27	196

1. Horizontal Direction (HD)

令 X 代表 $V(p, q)$ 在 HD 之像素，則 X 共有 $L = (M-1) \times N = 2 \times 3 = 6$ pixels

根據表 1， $X = \{88, 27, 21, 61, 183, 113\}$ ，如表 3 所示。

令 Y 代表對應 $V(p, q)$ 在 HD 之像素，則 Y 共有 $L = (M-1) \times N = 2 \times 3 = 6$ pixels

根據表 1， $Y = \{27, 196, 61, 12, 113, 125\}$ ，如表 3 所示。

表 3. 水平模式之 X 與 Y vectors

X vector		Y vector	
88	27	27	196
21	61	61	12
183	113	113	125

根據式 1-5，我們可以得出對應之數值，進而利用式 6 求出 HD 方向之相關係數

$\bar{x} = \frac{1}{6} \sum_{i=1}^6 x_i = 82.17$	(1)
$\bar{y} = \frac{1}{6} \sum_{i=1}^6 y_i = 89.00$	(2)
$\text{VAR}(X) = \frac{\sum_{i=1}^6 x_i^2}{6-1} - \bar{x}^2 = 3676.97$	(3)
$\text{VAR}(Y) = \frac{\sum_{i=1}^6 y_i^2}{6-1} - \bar{y}^2 = 4775.60$	(4)
$\text{COV}(X, Y) = \frac{\sum_{i=1}^6 (x_i - \bar{x})(y_i - \bar{y})}{(6-1)} = 121.60$	(5)

$\text{Correlation}(X, Y) = \frac{\sum_{i=1}^L (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^L (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^L (y_i - \bar{y})^2}} = 0.029018$	(6)
---	-----

2. Vertical Direction (VD)

令 X 代表 V(p, q) 在 VD 之像素，則 X 共有 $L=M*(N-1)=3*2=6$ pixels

根據表 1， $X=\{88, 27, 196, 21, 61, 12\}$ ，如表 4 所示。

令 Y 代表對應 V(p, q) 在 VD 之像素，則 Y 共有 $L=M*(N-1)=3*2=6$ pixels

根據表 1， $Y=\{21, 61, 12, 183, 113, 125\}$ ，如表 4 所示。

表 4 垂模式之 X 與 Y vectors

X vector			Y vector		
88	27	196	21	61	12
21	61	12	183	113	125

根據式 1-5，我們可以得出對應之數值，進而利用式 6 求出 VD 方向之相關係數

$\bar{x} = \frac{1}{6} \sum_{i=1}^6 x_i = 67.50$	(1)
$\bar{y} = \frac{1}{6} \sum_{i=1}^6 y_i = 85.83$	(2)
$\text{VAR}(X) = \frac{\sum_{i=1}^6 x_i^2}{6-1} - \bar{x}^2 = 4771.50$	(3)
$\text{VAR}(Y) = \frac{\sum_{i=1}^6 y_i^2}{6-1} - \bar{y}^2 = 4396.97$	(4)
$\text{COV}(X, Y) = \frac{\sum_{i=1}^6 (x_i - \bar{x})(y_i - \bar{y})}{(6-1)} = -3335.90$	(5)
$\text{Correlation}(X, Y) = \frac{\sum_{i=1}^L (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^L (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^L (y_i - \bar{y})^2}} = -0.728298$	(6)

3. Diagonal Direction (DD)

令 X 代表 V(p, q) 在 DD 之像素，則 X 共有 $L=(M-1)*(N-1)=2*2=4$ pixels

根據表 1， $X=\{88, 27, 21, 61\}$ ，如表 5 所示。

令 Y 代表對應 V(p, q) 在 D 之像素，則 Y 共有 $L=(M-1)*(N-1)=2*2=4$ pixels

根據表 1， $Y=\{61, 12, 113, 125\}$ ，如表 5 所示。

表 4. 對角模式之 X 與 Y vectors

X vector		Y vector	
88	27	61	12
21	61	113	125

根據式 1-5，我們可以得出對應之數值，進而利用式 6 求出 DD 方向之相關係數

$\bar{x} = \frac{1}{4} \sum_{i=1}^4 x_i = 49.25$	(1)
$\bar{y} = \frac{1}{4} \sum_{i=1}^4 y_i = 77.75$	(2)

$VAR(X) = \frac{\sum_{i=1}^6 x_i^2}{4-1} - \bar{x}^2 = 977.58$	(3)
$VAR(Y) = \frac{\sum_{i=1}^6 y_i^2}{4-1} - \bar{y}^2 = 2692.92$	(4)
$COV(X, Y) = \frac{\sum_{i=1}^4 (x_i - \bar{x})(y_i - \bar{y})}{(4-1)} = 124.42$	(5)
$Correlation(X, Y) = \frac{\sum_{i=1}^L (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^L (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^L (y_i - \bar{y})^2}} = 0.076681$	(6)

假設 Origi_image 目錄儲存原始影像 N 張，不失一般情況下，令 N=6，並以 bmp 影像格式為例。Encry_image 目錄儲存對應的加密影像。Decry_image 目錄儲存對應的解密影像，如表 2 所示。

表 2：以 3 個目錄分別儲存原始影像、加密影像、解密影像與目錄內對應之影像名稱

編號	Origi_image directory	Encry_image directory	Decry_image directory
1	01_Airplane.bmp	01_Airplane_en.bmp	01_Airplane_de.bmp
2	02_Baboon.bmp	02_Baboon_en.bmp	02_Baboon_de.bmp
3	03_Lena.bmp	03_Lena_en.bmp	03_Lena_de.bmp
4	04_Peppers.bmp	04_Peppers_en.bmp	04_Peppers_de.bmp
5	05_Sailboat.bmp	05_Sailboat_en.bmp	05_Sailboat_de.bmp
6	06_Splash.bmp	06_Splash_en.bmp	06_Splash_de.bmp

1. 請寫一個 python 程式，分別對每組原始影像與加密影像，依照水平、垂直、對角，分類，求出其 CTAP 相關係數。
2. 假設各目錄之檔案名稱都一一對應，但是程式設計時，請考慮測試之影像數量可能並非固定 6 個。
3. 請將計算後之數值，依照目錄輸出成 1 個 CSV 檔案(output13.csv，以利後續分析與整理。
4. 各 CSV 檔案第 1 行輸出各行之項目名稱，如範例所示。

請注意：

1. 輸出相關係數，Correlation(X, Y)，之精確度為小數 6 位，第 7 位四捨五入。其餘數值為小數 2 位，第 3 位四捨五入。
2. 相關係數之數值一定介於-1.0 與 1.0 之間。 \bar{x} , \bar{y} , VAR(X), VAR(Y)一定為正值。輸出時，請判斷數值介於正確範圍內。
3. 一般而言，原始影像，各頻道之相關係數離離 0.0 較遠，代表原始兩相鄰像素間較相關。反之，加密影像各頻道之相關係數距離 0.0 較近，代表經過加密後，兩相鄰像素間較不相關。

輸出檔案：以 output13.csv 為例

第 1 行為 title

第 1 行 Image Name, Mode, Channel, \bar{x} , \bar{y} , VAR(X), VAR(Y), COV(X, Y), Correlation(X,Y)

第 02-19 行為第一組影像，20-37 行為第二組影像，依此類推

第 02 行，原始影像名稱, HD、R Channel, 各種數據結果為式 1-6 之數據，以下類推

第 03 行，原始影像名稱, HD、G Channel, 各種數據結果

第 04 行，原始影像名稱, HD、B Channel, 各種數據結果

第 05 行，原始影像名稱, VD、R Channel, 各種數據結果

第 06 行，原始影像名稱, VD、G Channel, 各種數據結果

第 07 行，原始影像名稱, VD、B Channel, 各種數據結果

第 08 行，原始影像名稱, DD、R Channel, 各種數據結果

第 09 行，原始影像名稱, DD、G Channel, 各種數據結果

第 10 行，原始影像名稱, DD、B Channel, 各種數據結果

第 11 行，加密影像名稱, HD、R Channel, 各種數據結果

第 12 行，加密影像名稱, HD、G Channel, 各種數據結果

第 13 行，加密影像名稱, HD、B Channel, 各種數據結果

第 14 行，加密影像名稱, VD、R Channel, 各種數據結果

第 15 行，加密影像名稱, VD、G Channel, 各種數據結果

第 16 行，加密影像名稱, VD、B Channel, 各種數據結果

第 17 行，加密影像名稱, DD、R Channel, 各種數據結果

第 18 行，加密影像名稱, DD、G Channel, 各種數據結果

第 19 行，加密影像名稱, DD、B Channel, 各種數據結果

....

....

Program:

The python program, “學號-13-DEC_MAT3.py,” inputs several pairs of original and encrypted images and produces output13.csv。

測資：

1. 提供 Bottom-Left 檔案 Group-1.rar。
2. 提供 Top-Left 檔案 Group-2.rar
3. 提供 01_Airplane.bmp 已分離 R, G, B 之 3 個影像檔案(Images.rar)。

Submission:

Please submit the following **TWO** files.

1. 學號-13-DEC_MAT3.py
2. Output13.csv