Hill Cypher

The Hill cipher algorithm is a symmetric key algorithm which means that we can get the decryption key out of the encryption one with a simple transformation.

The idea behind hill cipher algorithm is actually pretty simple. It takes ***m*** successive plain pixels and substitutes them with ***m*** ciphered pixels. For example, if we have three pixels P_1, P_2, P_3, Hill cipher algorithm will substitute them by C_1, C_2, C_3 according to the following equations:

$C_1 = (K_{11} P_1 + K_{12} P_2 + K_{13} P_3)$ mod range

$C_2 = (K_{21} P_1 + K_{22} P_2 + K_{23} P_3)$ mod range

$C_3 = (K_{31} P_1 + K_{32} P_2 + K_{33} P_3)$ mod range

This can be represented by matrices as following:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}$$

This can simply be written as: **C = K P**

Where **P** is the block of plain pixels that is to be substituted by **C** (block of encrypted pixels). **K** is the key matrix that will do this transformation.

To decrypt the image: $\mathbf{P = K^{-1} C}$

As you have probably noticed, the key matrix must be invertible so that we can decrypt the image back.

The main concept of Hill cipher algorithm is pretty clear. The only thing that we need to work on is how to find the key matrix **K** so that we guarantee that it is invertible. We will discuss this in the next section.

Generation of Involutory Key Matrix

In the algorithm we use, The generated key matrix for Hill cipher algorithm will be involutory, which means that the key matrix is its own inverse e.g. $\mathbf{K^2 = I}$

Let **A** = $\begin{bmatrix} a_{11} & a_{12} & .. & .. & .. & .. & a_{1n} \\ a_{21} & a_{22} & .. & .. & .. & .. & a_{2n} \\ .. & .. & .. & .. & .. & .. & .. \\ a_{n1} & a_{n2} & .. & .. & .. & .. & a_{nn} \end{bmatrix}$ be $n \times n$ involutory matrix

Matrix **A** will be partitioned into 4 smaller matrices each of order $\left(\frac{n}{2}\right) \times \left(\frac{n}{2}\right)$

A = $\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$

Since $\mathbf{A^2 = I}$, then we can deduce the following:

- $A_{12} A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$ (Equation 1)
- $A_{11} + A_{22} = 0$ (Equation 2)

So, to generate an involutory matrix **A**:

- A_{22} can be any $\left(\frac{n}{2}\right) \times \left(\frac{n}{2}\right)$matrix, so we fill it randomly.
- From Equation 2: $\mathbf{A_{11} = -A_{22}}$
- Let $\mathbf{A_{12} = K(I - A_{11})}$ or $\mathbf{K(I + A_{11})}$ (Equation 3)

From Equation 1 and 3: $\mathbf{A_{21}} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$

Results

Figure 1: Original Image (1)

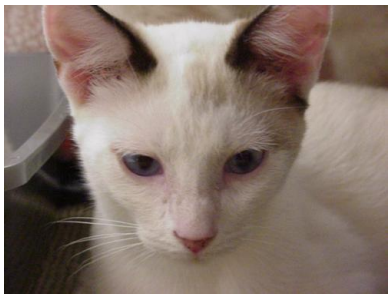

Figure 2: Original Image (2)

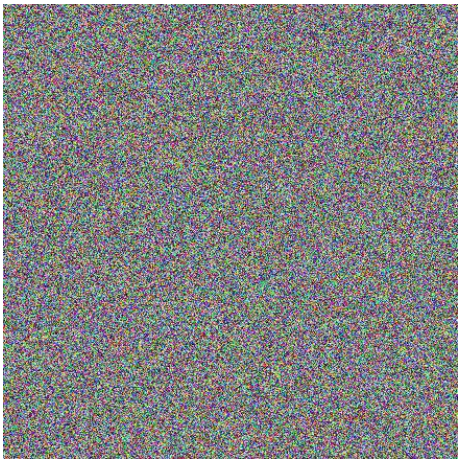

Figure 3: Encrypted Image (1)

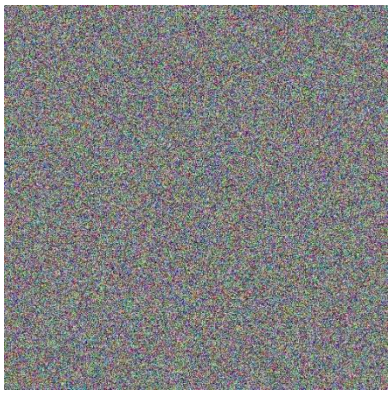

Figure 4: Encrypted Image (2)

Figure5: Decrypted Image (1)

Figure 6: Decrypted Image (2)

We can see that the encrypted image is bigger than the original one as we change the image to have square dimensions, so we can multiply it by our Involutory Key Matrix.
The added pixels have Zero RGB values.