Performance Metrics Analysis for Text and Image Encryption-Decryption

I. System Performance Metrics and Analysis

In this section we define essential metrics for evaluating the efficiency of each multimedia encryption scheme in analyzing the stream cipher performance.

A. Image Encryption Analysis

a) Histogram: A histogram visually represents data distribution, such as pixel intensities in images. Table I shows histograms for red, green, and blue channels of original and encrypted images. Cipher image histograms display equal intensity distribution, indicating random pixel behavior.

TABLE I: Plain and Cipher image histograms

	Red channel	**Green channel**	**Blue channel**
Plain image			
Cipher image			

b) Correlation Coefficient γ and Adjacent Pixel Correlation : The Correlation Coefficient serves as a metric for quantifying the correlation between plain image and cipher image. Correlation coefficient is given by,

$$\gamma = \frac{\sum_{i=0}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=0}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=0}^{n}(y_i - \bar{y})^2}} \tag{1}$$

where, x is the plain image, $\bar{x}$ is the mean of the plain image pixels and y is the cipher image, $\bar{y}$ is the mean of the cipher image pixels. Image encryption aims to reduce correlation between plain and encrypted images, as well as disrupt correlation between adjacent pixels. Original images have high correlation, resulting in linear maps between adjacent pixels, while cipher images show zero correlation.

c) Entropy : The Cipher image randomness measurement involves calculating entropy, typically expressed as bits/pixel.

$$H(x) = -\sum_{i=0}^{n} p(x_i)\log_2 p(x_i) \tag{2}$$

d) Net Pixel Change Rate (NPCR): For robust image encryption, a single bit change in CK (secret key) or IV (Initialization Vector) should cause significant alterations in the cipher image, quantified by ($NPCR$). Let C_1 and C_2 be cipher images encrypted with key streams K_1 and K_2 respectively, differing by a single bit in CK or IV. 'M' and 'N' represent the image's rows and columns, while 'R' denotes its channels.

$$D = \begin{cases} 1; & C_1(i,j) \neq C_2(i,j) \\ 0; & C_1(i,j) = C_2(i,j) \end{cases} \tag{3}$$

$$\text{NPCR} = \sum_{i=0}^{M}\sum_{j=0}^{N}\frac{D}{M \times N \times R} \times 100\% \tag{4}$$

e) Unified Average Change in Intensity (UACI): UACI focuses on Averaged differences between the pixels of C_1 and C_2. Mathematically UACI is calculated using equation (5).

$$\text{UACI} = \sum_{i=0}^{M}\sum_{j=0}^{N}\frac{|C_1(i,j) - C_2(i,j)|}{(\max(C_1) - \min(C_1)) \times M \times N \times R} \times 100\% \tag{5}$$

f) Histogram Deviation (D_H): Histogram deviation is a way to check how well an encryption scheme works by comparing the pixel differences between the original image (O) and encrypted image (E). D_H is calculated by

$$K(i) = |hist_O(i) - hist_E(i)| \tag{6}$$

$$D_H = \frac{K_0 + K_{len(K)-1}}{2} + \sum_{i=1}^{len(K)-2} K_i \tag{7}$$

where, $hist_O$ and $hist_E$ are the histogram of the original and cipher images.

The large value of histogram deviation states a high deviation in the encrypted image from the original one.

g) Irregular Deviation (D_I) : Irregular deviation is a measure used to determine the highest amount of inconsistency in pixel values within an encrypted image resulting from encryption algorithm. Irregular deviation is estimated by

$$D_I = \frac{\sum_{i=0}^{len(K)-1}|K(i) - \overline{(hist_E)}|}{len(E)} \tag{8}$$

where, $\overline{(hist_E)}$ is the mean of cipher image histogram.

The lower value of D_I indicates that the pixel distribution is uniform, and the quality of the encrypted image is high.

h) Mean Square Error (MSE): MSE is a metric used to compute the error between the original image A_1 and the decrypted image A_2, taking into account the impact of noise introduced during transmission. Its value is calculated by (9).

$$\text{MSE} = \frac{\|A_1 - A_2\|^2}{M \times N \times R} \tag{9}$$

i) Peak Signal to Noise Ratio (PSNR): PSNR measures the ratio between the maximum possible power of a original image A_1 and the power of the noise that affects the fidelity of the reconstructed A_2 (For theoretical calculations, 0.01 level of salt and pepper noise is added to the encrypted image and transmitted for reconstruction). The formula is,

$$\text{PSNR} = 10\log_{10}\left(\frac{\max(A_1)^2}{MSE}\right) \text{ dB} \tag{10}$$

B. Text Encryption Analysis

a) Histogram: The text histogram illustrates character frequency distribution. In Fig. 1, histograms for original and cipher text using any ciphering algorithm are shown, with similar patterns in other schemes. Fig. 1b depicts a uniform distribution in the cipher text's histogram, indicating randomness.

(a) Original Text (b) Encrypted Text

Fig. 1: Histogram of the text

b) Entropy: In text, entropy, defined similarly to equation (2), is measured in bits per character, differing from the bits per pixel measurement commonly employed for images.

c) Levenshtein Distance and Similarity: Levenshtein Distance is used to measure the similarity between two text words. Higher distance implies low similarity between the text strings. Mathematically, Levenshtein Distance lev(a,b) between two strings a, b (len(a) = $|a|$ and len(b) = $|b|$, head(x)= x[0] and tail(x)= all x other than x[0]) is given by, $\text{lev}(a,b) =$

$$\begin{cases} |a| & \text{if } |b| = 0 \\ |b| & \text{if } |a| = 0 \\ \text{lev}(\text{tail}(a), \text{tail}(b)) & \text{if head}(a) = \text{head}(b) \\ 1 + \min \begin{cases} \text{lev}(\text{tail}(a), b) \\ \text{lev}(a, \text{tail}(b)) \\ \text{lev}(\text{tail}(a), \text{tail}(b)) \end{cases} & \text{otherwise} \end{cases} \tag{11}$$

Levenshtein Similarity (LS) is given by,

$$\text{LS} = 1 - \frac{\text{lev(a,b)}}{\max(|a|, |b|)} \tag{12}$$

d) Net Amplitude Similar Rate (NASR): NASR quantifies the similarity between original (O) and decrypted audio (R).

$$S = \begin{cases} 1; & O(i) = R(i) \\ 0; & O(i) \neq R(i) \end{cases} \tag{13}$$

$$\text{NASR} = \sum_{i=0}^{Len(O)} \frac{S}{Len(O)} \times 100\% \tag{14}$$

e) Net Amplitude Change Rate (NACR): NACR is similar to the NPCR, where difference is calculated within the amplitudes of two encrypted audios A_1 and A_2 with two different keys differing by single bit.

$$D = \begin{cases} 1; & A_1(i) \neq A_2(i) \\ 0; & A_1(i) = A_2(i) \end{cases} \tag{15}$$

$$\text{NACR} = \sum_{i=0}^{Len(A_1)} \frac{D}{Len(A_1)} \times 100\% \tag{16}$$

f) Unified Average Change in Amplitude (UACA): UACA is similar to UACI and is calculated using equation (17).

$$\text{UACA} = \sum_{i=0}^{Len(A_1)} \frac{|A_1(i) - A_2(i)|}{(\max(A_1) - \min(A_1)) \times Len(A_1)} \times 100\% \tag{17}$$

g) Peak Signal to Noise Ratio (PSNR): PSNR is calculated by the formula,

$$\text{PSNR} = 10\log_{10}\left(\frac{\max(M_1)^2}{MSE}\right) \text{ dB} \tag{18}$$

h) Net Character Similar Rate (NCSR): NCSR, Similar to NACR, is calculated as in equations (13) and (14), with the distinction that it measures the similarity between original (O) and decrypted text (R) by considering text characters instead of audio samples.

i) Net Character Change Rate (NCCR): NCCR is similar to the NPCR and NACR, where difference is calculated with in the characters of two encrypted texts T_1 and T_2 with two different keys differing by single bit.

$$D = \begin{cases} 1; & T_1(i) \neq T_2(i) \\ 0; & T_1(i) = T_2(i) \end{cases} \tag{19}$$

$$\text{NCCR} = \sum_{i=0}^{Len(T_1)} \frac{D}{Len(T_1)} \times 100\% \tag{20}$$

1) Encryption Quality Analysis: Histogram deviation and Irregular deviation exhibit similar characteristics for text as they do for images as in equations (6),(7) and (8), albeit in text, the analysis is performed on characters.