Utilizing Quality Measures in Evaluating Image Encryption Methods

Abdelfatah A. Tamimi, Ayman M. Abdalla, and Mohammad M. Abdallah

1 Introduction

Image quality measures are essential in evaluating the efficacy of algorithms used in image processing and computer vision. The quality assessment may be computed objectively and automatically or through subjective user evaluation. Although the users' viewpoint is important for many applications, it is not very useful for applications sensitive to the minor changes invisible to humans. Furthermore, it is infeasible to use a large group of users for testing many cases involving dozens of images. Therefore, most researchers focus on objective metrics rather than relying on subjective metrics obtained from human users. Nonetheless, many researchers, such as [1–5], only used some metrics and overlooked the others.

Image quality measurements are often made by comparing a modified image to the original image. Nonetheless, the goals of making such comparisons differ with different applications. Generally, the changes made onto an image can be categorized into two categories based on the purposes of these changes. One category aims at obtaining an image very similar to the original for applications such as denoising, restoration, steganography, and compression. The other category aims at distorting the image to make it unrecognizable, usually for cryptography applications. Previous work on quality measurement, such as [6–10], mostly focused on the first goal. Alternatively, this paper will focus on the latter, that is, using quality metrics for cryptography. Little previous work focused on image quality from that point of view. Recently, [11] proposed a new metric, called a Contrast Sensitivity Function, to measure the degradation of compressed and encrypted

A. A. Tamimi (✉) · A. M. Abdalla · M. M. Abdallah
Faculty of Science and Information Technology, Al-Zaytoonah University of Jordan, Amman, Jordan
e-mail: drtamimi@zuj.edu.jo

H. R. Arabnia et al. (eds.), *Advances in Computer Vision and Computational Biology*, Transactions on Computational Science and Computational Intelligence,
https://doi.org/10.1007/978-3-030-71051-4_21

image sequences. However, this new metric is more suited for image sequences than individual images. On the other hand, quality measures used for evaluating image encryption can also be used for evaluating audio encryption, as done by [12]. Furthermore, many image encryption algorithms apply to three-dimensional objects [13–15].

Additionally, since cryptography produces images unrecognizable by humans, and their visual analyses require experts to recognize possible patterns, this paper will not consider subjective quality metrics. Nonetheless, it is not practical to rely on a small set of metrics to evaluate any given method. A collection of different quality measurement techniques must be used to cover the encryption strength in resisting different types of attacks.

In lossless encryption methods, the decrypted image must be identical to the original. On the other hand, lossy encryption methods recover an imperfect decrypted image. The quality of this decrypted image can be evaluated with the same tools used for recovered and denoised images because it is desired to be very similar to the original. Therefore, decrypted image quality is not in the focus of this paper.

2 Statistical Analysis Measures

The use of statistical analysis measures for a cryptography technique can help in evaluating its resistance to various attacks, especially statistical attacks. This section will discuss common statistical measures employed in image cryptography.

2.1 Keyspace

The keyspace of an encryption algorithm is the set of all possible keys that can be used to encrypt the data. A sufficiently large keyspace prevents brute-force attacks and increases the difficulty for other attacks that try to guess the secret key used in encryption

2.2 Mean Absolute Error

When Mean Absolute Error (MAE) is used in comparing a plain image with its encrypted image, a high MAE value is desired to indicate more difference between the image and its encryption and thus better encryption. MAE is computed with (1).

$$\text{MAE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} \left| A\,[i,\, j] - B\left[i,\, j\right] \right| \tag{1}$$

2.3 MSE and PSNR

Similar to MAE, the mean squared error (MSE) indicates the difference between two given images. Therefore, large values are desired when MSE is computed for an image and its encryption. MSE for two images, stored in matrices A and B, is computed as in (2):

$$\text{MSE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (A\,[i,\, j] - B\,[i,\, j])^2 \tag{2}$$

For image quality measurement, Peak Signal to Noise Ratio (PSNR) is preferred more than MSE. It is computed based on MSE as in (3):

$$\text{PSNR} = 10 \log_{10} \left(\frac{\text{MAX}^2}{\text{MSE}} \right) \tag{3}$$

where MAX is the maximum pixel value in the image. PSNR, measured in decibels, is focused on the unchanged values in the image rather than on the noise. Therefore, a better encryption technique should produce lower PSNR values to indicate having less unaltered values and, consequently, more resistance to attacks.

2.4 Entropy

The randomness of the pixel values, indicated by entropy, should increase after encryption to increase the encrypted image resistance against different attacks. The increase in randomness can be measured by computing the entropy ratio, that is, the rate of increase in entropy. Entropy is given by (4):

$$H = -\sum_{i=1}^{\text{MAX}} \left(P(i) \log_2 (P(i)) \right) \tag{4}$$

where:

MAX is the maximum pixel value of the image, and
$P(i)$ is the probability of the occurrence of pixel value i.

2.5 Correlation and Neighbors Correlation

The resemblance of one image to another can be measured with correlation, as given by (5), where $\overline{A}$ and $\overline{B}$are mean values for matrices A and B, respectively:

$$r = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A\left[i,j\right]-\overline{A}\right)\left(B\left[i,j\right]-\overline{B}\right)}{\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\left(A\left[i,j\right]-\overline{A}\right)^{2}\right)\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\left(B\left[i,j\right]-\overline{B}\right)^{2}\right)}} \tag{5}$$

For encryption techniques, it is desirable to have very low correlation values to show stronger encryption.

In addition to the above correlation indicator, the correlation between the neighboring pixels in the encrypted image can be measured and compared with that of the original image. A good indicator of neighbors' correlation is the Value Difference Degree (VDD). To compute VDD, start with computing Value Difference (VD) of each pixel value $P(i, j)$ at position (i, j) as in (6):

$$\mathrm{VD}\left(i,j\right) = \frac{1}{4}\sum i^{'}\,j^{'}\left[P\left(i,j\right)-P\left(i^{'},j^{'}\right)\right]^{2} \tag{6}$$

where the neighborhood of the pixel at position (i, j) is $(i', j') = \{(i - 1, j), (i + 1, j), (i, j - 1), (i, j + 1)\}$. Then, compute the Average Value Difference (AVD) for the whole image. Finally, VDD can be obtained by computing the difference of AVD values for the original image and the encrypted image, divided by their sum, as in (7). The value of VDD should be a number between −1 and 1 where a value near 1 indicates strong encryption.

$$\mathrm{VDD} = \left(\mathrm{AVD}_{\mathrm{original}} - \mathrm{AVD}_{\mathrm{encrypted}}\right) / \left(\mathrm{AVD}_{\mathrm{original}} + \mathrm{AVD}_{\mathrm{encrypted}}\right) \tag{7}$$

2.6 SSIM and MSSIM

As the image is encrypted, structural information should become degraded and distorted. In other words, the structural information of the encrypted image should be sufficiently different from that of the original image. The structural similarity index (SSIM) of an image is given by (8):

$$\mathrm{SSIM} = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{8}$$

where:

μ_x is the average of x,
μ_y is the average of y,
σ_x^2 is the variance of x,
σ_y^2 is the variance of y,
σ_{xy} is the covariance of x and y,
$c_1 = (k_1\ L)^2$ and $c_2 = (k_2\ L)^2$ are two variables to stabilize the division with weak denominator,
L is the dynamic range of the pixel values (typically, this is $2^{\text{bpp}} - 1$, *bpp* is bits per pixel), and
$k_1 = 0.01$ and $k_2 = 0.03$ by default.

To compare the overall structural quality of an encrypted image Y to the original image X, the Mean SSIM (MSSIM) value is computed as in (9):

$$\text{MSSIM}\,(X, Y) = \frac{1}{M}\sum_{j=1}^{M}\text{SSIM}\left(x_j - y_j\right) \tag{9}$$

For encrypted images, a low value of MSSIM is desired since it indicates less structural similarity and better encryption.

2.7 Histogram Analysis

An effective image encryption method should perform sufficient confusion and diffusion of the pixels. The encryption method needs confusion to permute the pixels and diffusion to change their values. However, many metrics of encryption could indicate that an encryption method is effective when it has a strong confusion component even when its diffusion component is weak or nonexistent. For an example, see [14, 15]. This problem creates a serious weakness for statistical attacks. Therefore, it is better to use histogram analysis, which is often effective in detecting weaknesses in image diffusion.

A simple and common method of histogram analysis is histogram visualization where the histogram of the original image is compared to the histogram of the encrypted image. The two histograms should appear different to indicate that the distribution of pixel values has changed after encryption. To indicate further resistance against statistical attacks, the histogram of the encrypted image should appear uniform and contain no distinctive peaks that could provide a weakness for the attacks.

For quantitative histogram analysis, the variance of histogram can be computed where a smaller variance value indicates less variation in values and a uniform histogram. The variance Var(V) of the histogram V stored as a one-dimensional array is given by (10) where v_i is the i^{th} element of V and represents the frequency

of gray value i in the image.

$$\mathrm{Var}(V) = \frac{1}{2n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \left(v_i - v_j\right)^2 \tag{10}$$

2.8 Balancedness

In addition to the above measures, encryption systems that employ cellular automata must examine their balancedness. That is, each generation of cellular automata must have nearly an equal number of ones and zeros. Failure to maintain this balance could undermine the efficacy of the whole encryption system. For examples of how this metric is used, see [14, 15].

3 Sensitivity Analysis Measures

The sensitivity of an encryption method to minor changes in the key or the input image makes it more effective, especially against differential attacks. Furthermore, this sensitivity keeps the rest of the secret key or the image secure if part of that information was revealed. Note that the lack of key sensitivity will also undermine the keyspace since many keys would become equivalent and should be excluded.

This sensitivity can be observed visually by making very small changes to the secret key or the input image and observing the result. However, better evaluations could be achieved using UACI and NPCR.

The Unified Averaged Changed Intensity (UACI) and the Number of Pixel Change Rate (NPCR) measure the strength of encryption techniques, especially their resistance against differential attacks. NPCR concentrates on the absolute number of pixels that change their values in differential attacks, while UACI focuses on the averaged difference between two paired encrypted images.

The desired UACI and NPCR values vary with the type and size of the image. A set of benchmark images with tables of theoretically computed upper and lower bounds for UACI and NPCR values have been provided by [16]. They showed through theoretical analysis and practical experiments that their computed theoretical values provide better measures of encryption quality than simple comparisons to other encryption methods.

4 Distortion Robustness Measures

Part of the encrypted image could be lost or distorted with different types of noise during transmission or storage. Therefore, an effective encryption system should be able to recover a meaningful recognizable image after it suffered from added noise or when part of it was occluded. This can be tested with visual observations or with measures of image quality.

To test the robustness of an encryption system with noise, sample encrypted images can be modified by adding noise of different types and intensities. Occlusion can be tested by replacing portions of the image with a single color such as black or white. If the decryption method recovers meaningful images similar to the original, this indicates that the system robustness can tolerate the tested distortion levels. Some of these types of tests were utilized by [14, 15].

5 Complexity Analysis

Space and time efficiency of the encryption system are important factors in determining the suitability of the system implementation for integration into various applications and hardware systems. The time and space requirements of most encryption algorithms are linear functions of the input size. However, the actual running time of these algorithms can vary significantly. Therefore, time and memory space required by the encryption technique should be estimated theoretically and measured empirically. The theoretical analysis should indicate the best, worst, and average cases. The practical experiments should provide the details of the implementation environment, such as the hardware and software specifications, the types and sizes of test data, etc.

6 Conclusion

The goals of image quality measurement differ according to application. This paper focused on image cryptography applications where the quality measurement goal is to ensure having noisy encrypted images with very low visual quality. Different metrics should be used for the encryption technique to ensure its robustness against various types of attacks such as brute-force, statistical, and differential attacks and to demonstrate its suitability for practical applications. Furthermore, these metrics can be used for making comparisons among various encryption techniques.

References

1. A. Yahya, A. Abdalla, *An AES-Based Encryption Algorithm with Shuffling, 2009 International Conference on Security and Management (SAM '09), Las Vegas, NV, USA, in Security and Management* (Eds, CSREA Press, H.R. Arabnia and K. Daimi, 2009), pp. 113–116
2. A. Tamimi, A. Abdalla, A double-shuffle image-encryption algorithm, 2012 international conference on image Processing, computer vision, and pattern recognition (IPCV '12), Las Vegas, NV, USA, in *Image Processing, Computer Vision, and Pattern Recognition*, (CSREA Press, H.R. Arabnia and K. Daimi, 2012), pp. 496–499
3. A. Abdalla, A. Tamimi, Algorithm for image mixing and encryption. Int. J. Multimedia Appl. **5**(2), 15–21 (2013)
4. A. Tamimi, A. Abdalla, An image encryption algorithm with XOR and S-box, in *19th International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV '15), Las Vegas, NV, USA*, (2015), pp. 166–169
5. A. Tamimi, A. Abdalla, A variable circular-shift image-encryption algorithm, in *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV '17)*, (Las Vegas, 2017), pp. 33–37
6. Z. Wang, H.R. Sheikh, E.P. Simoncelli, Image quality assessment: From error visibility to structural similarity, IEEE trans. Image Proc. **13**(4), 1–14 (2004)
7. K.-H. Thung, P. Raveendran, *A survey of image quality measures. 2009 International Conference for Technical Postgraduates (TECHPOS), Kuala Lumpur, Malaysia* (2009). https://doi.org/10.1109/TECHPOS.2009.5412098
8. Z. Wang, A.C. Bovik, *Modern Image Quality Assessment* (Morgan & Claypool, 2006). https://doi.org/10.2200/S00010ED1V01Y2005081VM003
9. B.W. Keelan, *Handbook of Image Quality: Characterization and Prediction* (Marcel Dekker, 2002)
10. R.R. Choudhary, V. Goel, G. Meena, Survey paper: Image quality assessment, proceedings of international conference on sustainable computing in science, technology and management (SUSCOM), Jaipur, India, February 26-28. (2019, 2019). https://doi.org/10.2139/ssrn.3356307
11. N. Khlif, M. Ben Amor, F. Kammoun, N. Masmoudi, A new evaluation of video encryption security with a perceptual metric. J. Test. Eval. **48**. (in press) (2020). https://doi.org/10.1520/JTE20160456
12. A. Tamimi, A. Abdalla, An audio shuffle-encryption algorithm. International Conference on Internet and Multimedia Technologies (ICIMT '14), San Francisco, CA, USA, in *Proceedings of the World Congress on Engineering and Computer Science, vol. I, 2014*, (2014), pp. 409–412
13. M. Mizher, R. Sulaiman, *Robotic Movement Encryption Using Guaranteed Cellular Automata. 2018 Cyber Resilience Conference (CRC), Putrajaya, Malaysia* (2018). https://doi.org/10.1109/CR.2018.8626820
14. M.M. Mizher, R. Sulaiman, A. Abdalla, M.M. Mizher, A simple flexible cryptosystem for meshed 3D objects and images. J. King Saud Univ.-Comp. Inform. Sci.. (in press) (2019). https://doi.org/10.1016/j.jksuci.2019.03.008
15. M.M. Mizher, R. Sulaiman, A. Abdalla, M.M. Mizher, An improved simple flexible cryptosystem for 3D objects with texture maps and 2D images. J. Inform. Secur. Appli. **47C**, 390–409 (2019). https://doi.org/10.1016/j.jisa.2019.06.005
16. Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption. Cyber J.: Multidiscip. J. Sci. Technol., J. Select. Areas Telecommun. (JSAT) **1**(2), 31–38 (2011)