Machine Learning-Based Evaluation of Statistical Metrics for Image Encryption

Sanjana Sanjana[1]*, Gaurav Gaurav[2], and Manju Khari[2]

[1] Department of Statistics, Amity University, Noida, India
sanjanasaini115@gmail.com*
[2] School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi 110067, India
gauravmoney26@gmail.com,
manjukhari@yahoo.com

Abstract. Image encryption protects visual data by converting it into an unreadable format during storage and transmission. Although entropy, correlation, NPCR, and UACI are widely used to evaluate encrypted images, it remains unclear whether these metrics are method-independent or whether they retain information about the underlying encryption scheme. This study examines that question using the Advanced Encryption Standard (AES) and chaos-based encryption, applied to 73 images of 512 × 512 resolution and 53 images of 1024 × 1024 resolution. For each encrypted image, entropy, horizontal, vertical and diagonal correlation, NPCR, and UACI were computed and used as input for three classifiers: logistic regression, random forest, and support vector machine (SVM), trained on 80 percent of the data and tested on the remaining 20 percent. The classifiers found it difficult to distinguish images encrypted with AES from those encrypted with the chaos-based scheme. For 512 × 512 images the highest accuracy was 63.33%, obtained by random forest, while SVM and logistic regression reached 56.67% and 50.00%. For 1024 × 1024 images, random forest and SVM both reached 50.00% and logistic regression 45.45%. The contribution of the individual metrics was also examined: entropy and NPCR contributed most for 512 × 512 images, whereas diagonal correlation dominated for 1024 × 1024 images. The results indicate that the classification models cannot reliably separate the two encryption methods, so these metrics carry only limited discriminative information about the encryption scheme.

Keywords: Image encryption · AES · Chaos-based encryption · Machine learning · Statistical metrics.

1 Introduction

The growing use of images for communication as the digital medium gains momentum has rendered image protection a pressing concern. Many types of images, such as medical images, military images, biometric images, satellite images, and regular personal images, are constantly being exchanged online. This has led to the rising need to protect these images, and one of the effective ways to do so is by encrypting them.

© The Author(s) 2026
A. Shastri et al. (eds.), *Proceedings of the Fourth Workshop on Applications of Computational Intelligence and Interactive Systems (WACIIS 2026)*, Advances in Intelligent Systems Research 217,
https://doi.org/10.2991/978-94-6239-832-0_5

Image encryption transforms a regular image into an unreadable form, which can only be recovered with the help of a decryption key and a specific algorithm.

There are many methods proposed for image encryption in the past several years. Most of them could provide secure communication in practice. The most well-known and widely used encryption method is probably the Advanced Encryption Standard (AES), which is based on extensive experimentation and proven to be secure mathematically. Nevertheless, chaos-based encryption methods have also attracted much attention in recent years due to the characteristics of high sensitivity to initial conditions, regular but random distribution in time, and even complexity and unpredictability [3, 4, 14]. To compare the security of different methods, some statistical measures are inevitably required. Entropy, horizontal correlation, vertical correlation, diagonal correlation, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) are the most commonly used criteria in image encryption. They can describe the randomness of the encrypted image pixels and the relationships of neighbouring pixels, as well as the sensitivity of the encrypted image to the initial conditions [6, 7, 11]. As a rule, higher values of these measures indicate a higher security level of an image encryption method.

But is it sufficient to just look at the statistical measures of the image encryption method under test? Does the fact that some methods give good statistical metrics hide certain patterns related to the method itself? And going deeper, are the outputs of different methods actually distinguishable? If so, then commonly used metrics do not give a complete picture of the encryption strength.

2 Motivation and Objective

This study investigated whether machine learning models can distinguish between different encryption schemes based on evaluation metrics alone. Images of 512 × 512 and 1024 × 1024 resolutions were encrypted using AES and chaos-based encryption [4, 7, 15]. The resulting statistical metrics were used as input features for machine learning classifiers. Logistic regression, the random forest classifier, and the support vector machine were used for classification. This allows the study to check if there are any identifiable patterns in evaluation metrics that tell about the encryption method used. Further, the relative contribution of individual metrics such as entropy, correlation, NPCR, and UACI in distinguishing encryption techniques is also examined. This helps in determining which measures have stronger discriminative information and whether all commonly used evaluation metrics contribute equally to the assessment of encryption performance.

The results obtained make this question quite meaningful. For the 512 × 512 images, the highest classification accuracy was achieved by the random forest classifier at 63.33%, while SVM reached 56.67% and logistic regression reached 50.00%. For the 1024 × 1024 images, random forest and SVM each achieved 50.00% accuracy, while logistic regression achieved 45.45%. These values show that, in a few cases, especially for low-resolution sets, machine learning models were able to extract class-related information from evaluation metrics. This suggests that the standard metrics still contain some separable patterns rather than being a fully neutral indicator of security strength [2, 5].

Therefore, this research does not aim to reject standard image-encryption metrics but rather to examine their limitations more critically. The main idea is simple: if a machine learning model can distinguish between AES-encrypted images and chaos-encrypted images based on standard statistical measures, i.e., entropy, correlation, NPCR, and UACI values, then these metrics should not be the sole measure of the performance of the encryption technique. In other words, strong metric values do not mean that two encryption methods are indistinguishable. This study connects two fields that are often treated separately: image-encryption evaluation and machine learning-based pattern recognition [2, 10].

3 Background

Image encryption has become an important area of research due to the increasing need to secure visual information transmitted over digital networks. Various encryption techniques have been created to protect images from unauthorised access [9]. Traditional cryptographic algorithms like the Advanced Encryption Standard (AES) are commonly used for securing data because of their strong security features and established cryptographic foundations [1].

Besides the widespread use of traditional cryptographic methods like substitution, permutation, and hash functions, their chaos-based counterparts have been the focus of attention of scientists in recent years. Chaotic systems have certain properties, such as sensitivity to initial conditions, pseudo-randomness, and ergodicity, which contribute to their great potential for cryptology and thus inspire a range of chaotic map-based encryption algorithms. These methods improved and generalised traditional cryptographic algorithms based on special characteristics of chaos. An early chaotic image encryption algorithm was proposed by Gao et al. [4] that relied on chaotic sequences for scrambling and modulation of image pixels. Later improvements, including strengthened diffusion and more complex non-linear substitution, have generated even more secure approaches. Zhu et al., for example, gave a secure image encryption scheme which combined the chaotic map and the design of a strong S-box [15]. Liu et al. developed an image encryption scheme that uses a three-dimensional chaotic system to create S-boxes for enhancing the confusion and diffusion properties [8], and Wang and Liu applied a full chaos coupled mapping lattice to privacy image encryption [12].

Kaur and Kumar focus on the implementation of various approaches to image encryption, including a few case studies along with their strengths and weaknesses [6]. Fang et al. investigated the recent progress in chaotic image encryption algorithms and performance evaluation [3]. Zhang and Liu have discussed chaos-based encryption methods and their applications and challenges [14]. Zia et al. surveyed image encryption techniques using chaotic maps in the spatial domain, transform domain, and spatiotemporal domain [16].

Most current image encryption methods are evaluated using entropy, correlation coefficient, NPCR, and UACI. These statistical values indicate randomness, the relationship between adjacent encrypted pixels, and the sensitivity to small changes in the input, and thus can serve as a measures for the encryption quality [7, 11]. High entropy and a low correlation coefficient indicate better encrypted results.

Advances in recent research explore the potential of machine learning techniques to facilitate cryptanalysis and security evaluation. Hou et al. proposed methods for improving classical cryptanalysis based on machine learning to extract hidden patterns in ciphertexts [5]. Benamira et al. also explored the application of machine learning for cryptanalysis to identify structural properties of cryptographic systems [2]. In the context of image encryption, Maniyath and Thanikaiselvan proposed a method based on the combination of chaotic maps and deep neural networks [10].

Many studies on image encryption and their statistical evaluations have been performed; however, few studies have examined whether commonly used statistical metrics are sufficient to distinguish among different types of image encryption approaches. Most research works have demonstrated the strength of image encryption approaches using the commonly used statistical metrics, such as entropy, without examining whether the metrics are capable of distinguishing between the approaches. In this study, we employed machine learning-based classifiers, including random forest and support vector machine, to investigate the capability of commonly used statistical metrics for distinguishing between encrypted images produced using AES and a chaos-based approach. We examined the individual contribution of the statistical metrics used as features. The results show that the two approaches can be separated only to a limited extent using statistical metrics, and that certain individual metrics contribute more to classification performance than others.

4 Methods and Statement of Contribution

The purpose of this study was to examine whether encryption schemes can be distinguished using the commonly used statistical metrics. Two sets of grayscale images were used: 73 images of 512 × 512 resolution and 53 images of 1024 × 1024 resolution. The images were obtained from the USC-SIPI Image Database [13] and included images from multiple categories. Before encryption, the images were converted to 8-bit grayscale and processed at their respective 512 × 512 or 1024 × 1024 resolutions. Each image was encrypted using AES-based encryption and chaos-based encryption. In the AES method, a 128-bit key in CBC mode is used, while the chaos-based method uses a logistic map with pixel permutation and XOR substitution. After encryption, six statistical metrics were computed for each image. These values were arranged in a separate dataset for each resolution. These six statistical metrics were used as input features for the machine learning models.

Entropy measures the randomness of pixel intensity values in the encrypted image. For an 8-bit grayscale image, the ideal entropy value is close to 8, which shows that all gray levels occur with nearly equal probability [3, 16]. Entropy was calculated using Eq. (1).

$$T = -\sum_{i=0}^{L-1} \quad l(i) log\ _2(l(i)) \tag{1}$$

where T is the entropy of the encrypted image, L is the number of possible gray levels, and l(i) is the probability of occurrence of gray level i.

Correlation coefficients measure the relationship between neighbouring pixels in the encrypted image. The correlation coefficient was calculated using Eq. (2).

$$e_{uv} = \frac{Cov(u,v)}{\sqrt{S(u)}\sqrt{S(v)}} \quad (2)$$

where Cov(u,v) is the covariance between two neighbouring pixel sequences and S(u) and S(v) are their variances. To evaluate this property, correlation coefficients were computed in three directions: horizontal correlation ($corr_H$), vertical correlation ($corr_V$), and diagonal correlation ($corr_D$).

NPCR measures how many pixel values change in an encrypted image if there is a small modification in the original image. It measures the sensitivity of the encryption technique to the initial conditions and evaluates its resistance to different attacks [7, 11, 15].

Suppose two plaintext images differ by only a very small change, and their encrypted outputs are denoted by C_1 and C_2. NPCR is computed using Eq. (3).

$$NPCR = \frac{\sum_{u=1}^{M} \sum_{v=1}^{N} S(u,v)\times 100}{M\times N} \quad (3)$$

The value of $S(u,v)$ was defined using Eq. (4).

$$S(u,v) = \{0, if\ C_1(u,v) = C_2(u,v)\ 1, if\ C_1(u,v) \neq C_2(u,v) \quad (4)$$

Here, M and N represent the number of rows and columns of the image.

While NPCR counts the percentage of changed pixels, UACI measures how large those changes are on average [7, 11, 15]. It is calculated using Eq. (5).

$$UACI = \frac{1}{M\times N}\sum_{u=1}^{M} \sum_{v=1}^{N} \frac{|C_1(u,v)-C_2(u,v)|}{L-1} \times 100 \quad (5)$$

where C1(u,v) and C2(u,v) are the pixel values of the two encrypted images at position (u,v), M and N are the image dimensions, and L is the number of gray levels. For an 8−bit grayscale image, L = 256 and L − 1 = 255.

To test whether these metrics contain any method-specific patterns, three machine learning models were used: logistic regression, random forest, and support vector machine (SVM). An 80:20 train-test split with random_state = 42 was used. The random forest and SVM splits were stratified by class; the logistic regression implementation used the same 80:20 proportion and random state. Logistic regression and SVM features were standardized using StandardScaler. The random forest classifier used 100 trees with random_state = 42. The SVM used an RBF kernel, and its C and gamma hyperparameters were selected on the training data using 5-fold GridSearchCV over C = {0.1, 1, 10, 100} and gamma = {scale, auto, 0.01, 0.1, 1}. Model performance was evaluated on the held-out test data using accuracy, precision, recall, F1-score, and ROC-AUC. Metric contribution was examined using logistic regression coefficients, random forest feature importance, and SVM permutation importance with 10 repetitions.

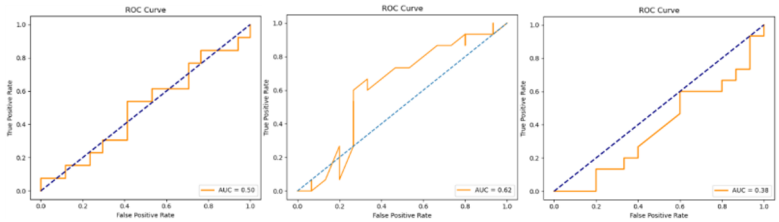
5 Results and Discussion

The classification results indicate that the statistical evaluation metrics contain limited information about the underlying encryption method. In some cases, particularly for the 512 × 512 dataset, machine learning models performed better than random chance. However, this separation was not consistent across different image resolutions. These observations suggest that commonly used statistical metrics are not completely method-independent, although they are not strong enough to produce reliable discrimination between encryption schemes [6, 7, 11].

For the 512 × 512 images, the random forest classifier achieved the highest accuracy of 63.33%, followed by SVM with 56.67%, while logistic regression achieved 50.00% accuracy. In the random forest model, recall for the chaos class was 0.7333, while recall for the AES class was 0.5333, indicating that the model was relatively better at identifying chaos-encrypted images than AES-encrypted images. Similarly, in both the SVM and logistic regression models, recall for identifying the chaos class was higher than the recall for identifying AES. The accuracy of logistic regression (50.00%) indicates that it performs approximately at the level of random guessing. These findings suggest that, for the 512 × 512 dataset, the evaluation metrics contain some structural patterns related to the encryption method, but these patterns are not sufficiently strong to support reliable classification. The classification metrics for the 512 × 512 dataset are shown in Table 1. The ROC curves for the 512 × 512 dataset are shown in Fig. 1.

Table 1. Classification performance for 512 × 512 resolution images

Class	Metric	Random Forest	SVM	Logistic Regression
AES (0)	Precision	0.6667	0.60	0.5833
	Recall	0.5333	0.40	0.4118
	F1-Score	0.5926	0.48	0.4828
Chaos (1)	Precision	0.6111	0.55	0.4444
	Recall	0.7333	0.73	0.6154
	F1-Score	0.6667	0.63	0.5161
Overall	Accuracy	63.33%	56.67%	50.00%



(a) (b) (c)

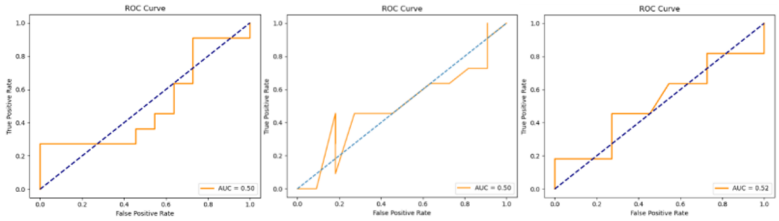
Fig. 1. ROC curves for the 512 × 512 dataset: (a) logistic regression, (b) random forest classifier, (c) SVM

The classification performance for the 1024 × 1024 dataset was lower than that of 512 × 512. Random forest and SVM each achieved 50.00% accuracy, while logistic

regression dropped to 45.45%. These values are at or below the chance-level reference for a two-class problem and therefore do not provide evidence of reliable discrimination between AES and chaos encryption in this dataset. None of the models demonstrated meaningful discrimination between the two schemes. This suggests that at higher image resolutions, statistical metrics contain even less information related to the encryption technique. The classification metrics for the 1024 × 1024 dataset are shown in Table 2. The ROC curves for the 1024 × 1024 dataset are shown in Fig. 2.

Table 2. Classification performance for 1024 × 1024 resolution images

Class	Metric	Random Forest	SVM	Logistic Regression
AES (0)	Precision	0.5000	0.50	0.4444
	Recall	0.3636	0.55	0.3636
	F1-Score	0.4211	0.52	0.4000
Chaos (1)	Precision	0.5000	0.50	0.4615
	Recall	0.6364	0.45	0.5455
	F1-Score	0.5600	0.48	0.5000
Overall	Accuracy	50.00%	50.00%	45.45%



(a) (b) (c)

Fig. 2. ROC curves for the 1024 × 1024 dataset: (a) logistic regression, (b) random forest classifier, (c) SVM

Overall, the highest accuracy observed in this study was achieved by the random forest classifier for the 512 × 512 dataset, while none of the models exceeded 50.00% accuracy for the 1024 × 1024 dataset. This suggests that the ability of statistical metrics to distinguish encryption schemes is not the same across different image resolutions.

These results show that commonly used evaluation metrics mostly hide the identity of the encryption technique used. However, the above-chance performance of some models, particularly random forest, on the 512 × 512 dataset shows that these metrics are not entirely neutral towards the encryption method. While high entropy or NPCR values may indicate good statistical properties of encrypted images, high values do not guarantee that the encryption schemes will be indistinguishable.

The contribution of each metric in distinguishing the encryption class was also calculated. For the 512 × 512 dataset, the contribution patterns were spread across several features. In logistic regression, entropy and NPCR played the most important role in distinguishing between the two encryption classes. Similarly, in the SVM model, entropy and NPCR had the strongest contributions, while UACI and vertical correlation showed relatively lower contributions. In the random forest model, feature importance values were more evenly distributed; however, diagonal correlation, horizontal

correlation, and entropy ranked relatively high. The metric contribution analysis for 512 × 512 is presented in Table 3.

Table 3. Metrics contribution analysis for 512 × 512 resolution images

Metric	Logistic Regression	Random Forest	SVM
Corr_D	0.056133	0.176360	0.062006
Entropy	0.213676	0.175649	0.496388
Corr_H	0.009428	0.168635	0.012835
Corr_V	0.094476	0.164584	0.156695
NPCR	0.185786	0.162936	0.366048
UACI	0.124224	0.151837	0.160411

For the 1024 × 1024 dataset, diagonal correlation was the most influential feature across all machine learning models. In logistic regression, Corr_D had the largest absolute contribution value (0.426505). A similar pattern was observed in the SVM model, where Corr_D was the strongest contributor with a contribution value of 0.599420. In the random forest model, feature importance values were more evenly distributed; however, Corr_D still ranked first (0.220659) among all features. The metric contribution analysis for 1024 × 1024 is presented in Table 4.

Table 4. Metrics contribution analysis for 1024 × 1024 resolution images

Metric	Logistic Regression	Random Forest	SVM
Corr_D	0.426505	0.220659	0.599420
Entropy	0.145602	0.206721	0.323843
Corr_H	0.117172	0.154094	0.147406
Corr_V	0.094663	0.141700	0.198780
NPCR	0.085958	0.141490	0.208774
UACI	0.020215	0.135337	0.004066

Overall, the findings showed that standard evaluation metrics are not a strong indicator of encryption schemes, but they still contain some traces of the underlying encryption pattern, which can be seen in some cases where machine learning models showed above-chance performance. This also suggests that with an increase in resolution there is a decrease in the accuracy of machine learning models in separating encryption techniques.

6 Conclusion

The goal of this study was to investigate whether the commonly used statistical metrics are sufficient to evaluate and distinguish between image encryption techniques. Images of resolutions 512 × 512 and 1024 × 1024 were taken and encrypted using AES and chaos-based encryption schemes, and statistical measures including entropy, correlation, NPCR, and UACI were computed. These metrics were used as input features for machine learning classifiers. Results showed that the classifiers struggled to distinguish between AES- and chaos-encrypted images, with classification accuracy close to a chance level, especially for high-resolution images. For images of resolution 512 × 512, the random forest model achieved the highest overall accuracy of 63.33%,

followed by SVM and logistic regression with 56.67% and 50.00%, respectively, indicating that the models can distinguish between the two encryption schemes to a limited extent. Class-wise results showed moderate but inconsistent discrimination, with chaos-encrypted images being identified slightly better than AES images across all models. For 1024×1024 resolution images, the classification performance decreased further, with random forest and SVM both achieving an accuracy of 50.00% and logistic regression yielding 45.45%. The class-wise precision, recall, and F1-scores at this resolution were also closely balanced and generally weak, showing that the classifiers were no longer able to capture meaningful differences between AES- and chaos-encrypted images. These results suggest that statistical metrics contain limited but not completely absent method-specific information. Metric contribution analysis showed that no single metric consistently dominates the classification process, suggesting that encryption evaluation may require more comprehensive analysis methods beyond standard statistical measures.

7 Future Research Directions

In the future, this study can be extended by using larger and more varied datasets, including colour, medical, and satellite images, to determine whether the current findings hold true across different image types. Other encryption methods such as hybrid, DNA-based, and transform-domain techniques could also be used for comparison. More advanced features, such as frequency-domain and complexity-based image features, should be explored. Other future directions include applying deep learning methods to identify hidden patterns in encrypted images. A comprehensive framework for evaluating image encryption methods should include attack-based assessment on a larger dataset and improved statistical testing methods.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Artuğer, F.: Innovative image encryption approach based on bitwise XOR high nonlinear S-boxes and random permutation. Soft Comput. 29, 2891–2903 (2025)
2. Benamira, A., Gerault, D., Peyrin, T., Tan, Q.Q.: A deeper look at machine learning based cryptanalysis. In: Canteaut, A., Standaert, F.-X. (eds.) EUROCRYPT 2021. LNCS, vol. 12696, pp. 287–317. Springer, Cham (2021)
3. Fang, P., Liu, H., Wu, C., Liu, M.: A survey of image encryption algorithms based on chaotic system. Vis. Comput. 39, 1975–2003 (2023)
4. Gao, H., Zhang, Y., Liang, S., Li, D.: A new chaotic algorithm for image encryption. Chaos Solitons Fractals 29(2), 393–399 (2006)
5. Hou, Z., Ren, J., Chen, S.: Improved machine learning-aided linear cryptanalysis: application to DES. Cybersecurity 8, 22 (2025)
6. Kaur, M., Kumar, V.: A comprehensive review on image encryption techniques. Arch. Comput. Methods Eng. 27, 15–43 (2020)

7. Lai, Q., Hu, G., Erkan, U., Toktas, A.: High-efficiency medical image encryption method based on 2D logistic-Gaussian hyperchaotic map. Appl. Math. Comput. 442, 127738 (2023)
8. Liu, H., Liu, J., Ma, C.: Constructing dynamic strong S-box using 3D chaotic map and application to image encryption. Multimed. Tools Appl. 82, 23899–23914 (2023)
9. Mahalakshmi, K., Nagarajan, S.: Comprehensive review and analysis of image encryption techniques. IEEE Access 13, 109783–109813 (2025)
10. Maniyath, S.R., Thanikaiselvan, V.: An efficient image encryption using deep neural network and chaotic map. Microprocess. Microsyst. 77, 103134 (2020)
11. Masood, F., Driss, M., Boulila, W., Ahmad, J.: A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wirel. Pers. Commun. 127, 1405–1432 (2022)
12. Wang, X., Liu, P.: A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans. Circuits Syst. I Regul. Pap. 69(3), 1291–1301 (2022)
13. Weber, A.: The USC-SIPI image database: version 6. Technical Report USC-SIPI-432, Signal and Image Processing Institute, University of Southern California (2018)
14. Zhang, B., Liu, L.: Chaos-based image encryption: review, application, and challenges. Mathematics 11(11), 2585 (2023)
15. Zhu, S., Deng, X., Zhang, W., Zhu, C.: Secure image encryption scheme based on a new robust chaotic map and strong S-box. Math. Comput. Simul. 207, 322–346 (2023)
16. Zia, U., McCartney, M., Scotney, B., Martinez, J.: Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. Int. J. Inf. Secur. 21, 917–935 (2022)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

