iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43298

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Event Management using End-to-End Image Encryption: A Review

Omkar Sisodia[1], Priyanka Bade[2], Pujari Ashwini[3], Mayuri Ambekar[4], Prof. Shiv Shinde[5]
[1, 2, 3, 4, 5]*Dept of Computer Engineering of Pune University, Shri Chhatrapati Shivaji Maharaj College of Enginnering Ahmednagar,India*

Abstract: ***Encryption-then-Compression (EtC) systems are used to securely transmit images over an untrusted channel provider, and a novel grayscale-based block scrambling image encryption method is developed to improve the security of EtC systems. This approach is intended to make encryption-then-compression (EtC) systems more secure. In comparison to the new encryption technology, the suggested scheme allows for smaller block sizes and a greater number of blocks.Despite the fact that the original image has three colour channels, photos encrypted using the suggested method contain less colour information due to the usage of grayscale images to encrypt the data. These features boost security against threats like jigsaw puzzle solvers and brute-force attacks, among other things. Apart from that, despite the fact that the encrypted photos do not include any colour information, it enables for colour sub-sampling, which can improve the compression speed of the images. In a test, encrypted photographs were posted to and later downloaded from social networking sites, and the findings demonstrated that using advanced compression algorithms, the suggested strategy is successful for ETC systems while still keeping excellent compression performance.***
Keywords: Event Management, image compression, non-local network, attention mechanism.

I. INTRODUCTION

A system of encryption followed by compression (and so on) with JPEG compression has been proposed and is now being tested for use on social networking sites and cloud photo storage services. Color-based image encryption techniques for EtC systems, on the other hand, are unable to provide the same level of resistance against colour sub-sampling as colour sub-sampling utilised for JPEG compression because an encrypted image is a full-color image. The grey scale-based pictures encryption approach, which encrypts a full-color image and converts it to a grey scale image, has been proposed to address this issue. Even if grey scale-based picture encryption can be employed to avoid the impacts of colour sub-sampling, colour sub-sampling procedures cannot be considered since the grey scale-based image is made up of RGB components and thus cannot be considered.

Furthermore, compression performance drops dramatically when compared to color-based picture encryption. It has been proposed that the quantization table for grey scale-based images, as well as the grey scale-based image encryption created from YCbCr components, provide greater compression performance. The operation of colour sub-sampling, on the other hand, has not been considered. The colour sub-sampling operation for grey scale-based picture encryption is discussed and considered in this study as it relates to grey scale-based image encryption. Rather than generating the image from RGB components, the grey scale-based image is formed by first converting a full-color image in RGB colour space to YCbCr colour space. Color subsampling can be used to create greyscale-based images, which can then be printed. We also go over the scenario and requirements that must be met for picture encryption to be effective. The gains in compression performance and robustness to colour sub-sampling that have been gained through this study are evaluated using Rate-Distortion (R-D) curves.

II. LITERATURE REVIEW

Sr No	Paper Title	Authors	Publication Year	Conclusion
1	Intra Block Copy in HEVC Screen Content Coding Extensions	XiaozhongXu, Shan Liu, Tzu-Der Chuang, Yu-Wen Huang, Shaw-Min Lei, KrishnakanthRapaka, Chao Pang, VadimSeregin, Ye-Kui Wang, and Marta Karczewicz	2017	This tool is very efficient for coding of screen content video in that repeated patterns in text and graphics rich content occur frequently within the same picture. Having a previously reconstructed block with equal or similar pattern as a predictor can effectively reduce the prediction error and therefore improve coding efficiency.

2	Conditional Probability Models for Deep Image Compression Fabian	FabianMentzer∗EirikurAgustsson∗ Michael TschannenRaduTimofte Luc Van Gool	2018	In this paper, author focus on the latter challenge and propose a new technique to navigate the ratedistortion trade-off for an image compression auto-encoder. The main idea is to directly model the entropy of the latent representation by using a context model: A 3D-CNN which learns a conditional probability model of the latent distribution of the auto-encoder.
3	Efficient Nonlinear Transforms for Lossy Image Compression	Johannes Ballé	2018	Authors assess the performance of two techniques in the context of nonlinear transform coding with artificial neural networks, Sadam and GDN. Both techniques have been successfully used in state-of-the-art image compression methods, but their performance has not been individually assessed to this point. Together, the techniques stabilize the training procedure of nonlinear image transforms and increase their capacity to approximate the (unknown) rate–distortion optimal transform functions. Besides comparing their performance to established alternatives, we detail the implementation of both methods and provide open-source code along with the paper.
4	Interference Reduction by Millimeter Wave Technology for 5G-Based Green Communications	TIN-YU WU AND TSE CHANG	2018	The primary goal of this paper is the optimization of data transmissions and connections between 5G base stations (BSs) as well as the improvement of access technologies and transmission methods in consideration of massive multi-input multi-output, a key technology in 5G networks. In order to reach an access technology supported by multiple BSs and small cells, we use 5G millimeter wave (mmWave), due to its high directivity and sensitivity to blockage, to enhance the connection system.
5	Learning Convolutional Networks for Content-weighted Image Compression	Mu Li,WangmengZuo,Shuhang Gu,Debin Zhao,David Zhang	2019	In this paper, motivated by that the local information content is spatially variant in an image, we suggest that: (i) the bit rate of the different parts of the image is adapted to local content, and (ii) the content aware bit rate is allocated under the guidance of a content weighted Importance map. The sum of the importance map can thus serve as a continuous alternative of discrete entropy estimation to control compression rate.

III. PROPOSED SYSTEM

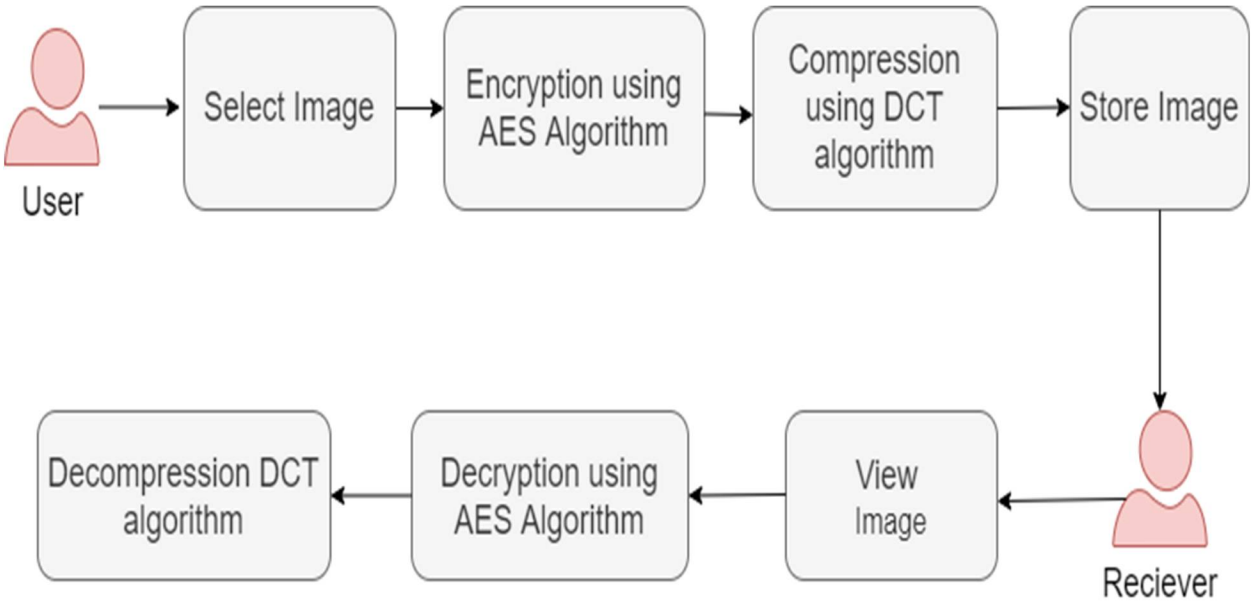


Figure 1. System Architecture

A. Advantages

1) Increases security using advanced compression algorithm.
2) Increases the sharing efficiency.
3) Increasingly adaptable access structures and high security.
4) Processing cost is less.

B. Algorithms

1) *AES Algorithm for Encryption:* AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.

Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

Input

128_bit /192 bit/256 bit input (0, 1)

Secret key (128_bit) +plain text (128_bit).

Process

10/12/14-rounds for-128_bit /192 bit/256 bit input

Xor state block (i/p)

Final round:10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key.

Output

cipher text(128 bit)

2) *DCT Compression Algorithm*

File compressor is responsible for taking images as input and compresses them using DCT algorithm.

We have used compression threshold factor of t = 0.2

IV. RESULTS AND DISCUSSION

1) *Results 1:* Shows file size on x axis and Uploading Time on Y-axis

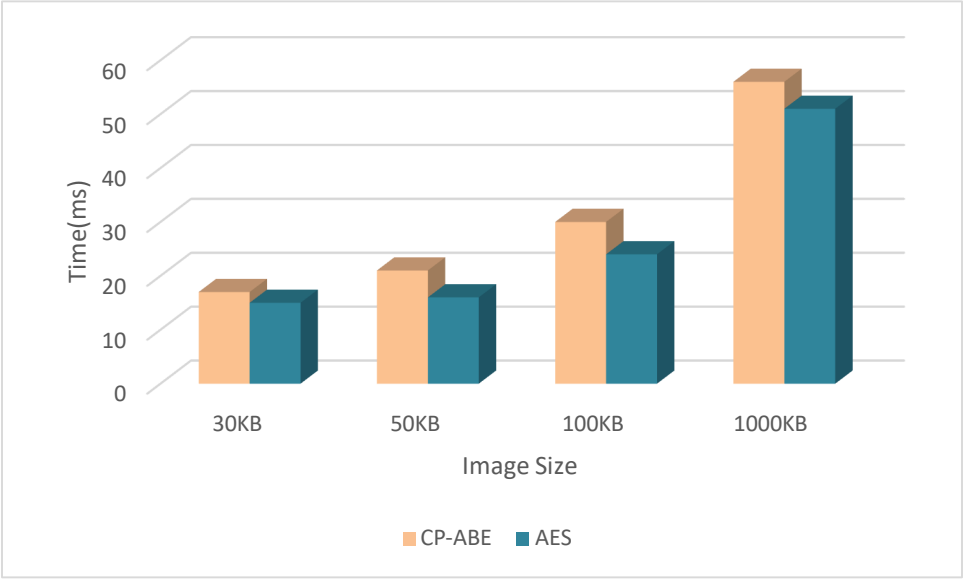


Figure 2: Shows file size on x axis and Uploading Time on Y-axis

Table 3: Show File Size and Uploading Time

Index Number	Image size (KB)	CP-ABE uploading Time	AES uploading Time
1	30	36	32
2	50	42	35
3	100	69	62
4	1000	111	96

2) *Results 2:* Shows file size on x axis and Downloading Time on Y-axis

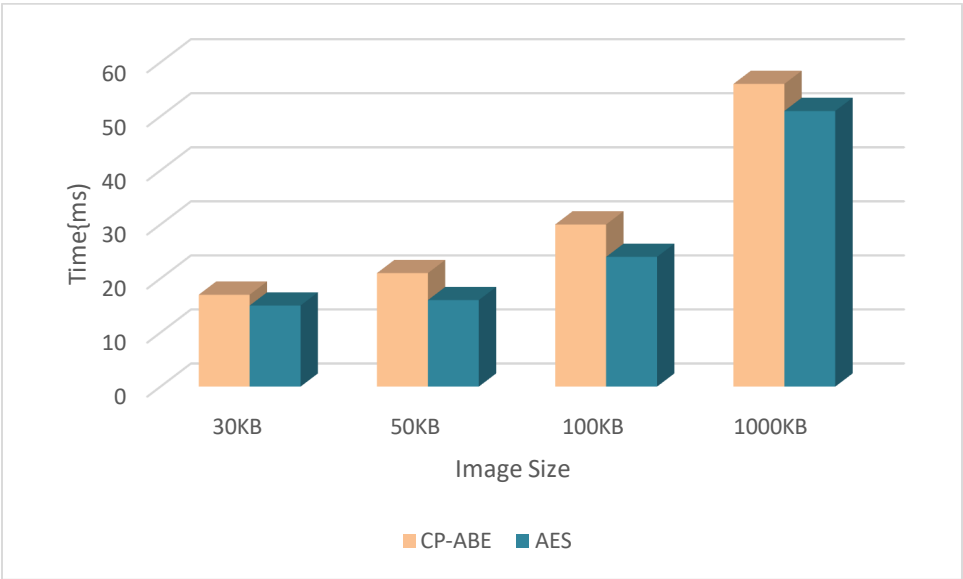


Figure 3: Shows file size on x axis and Downloading Time on Y-axis

Table 4: Show File Size and Downloading Time

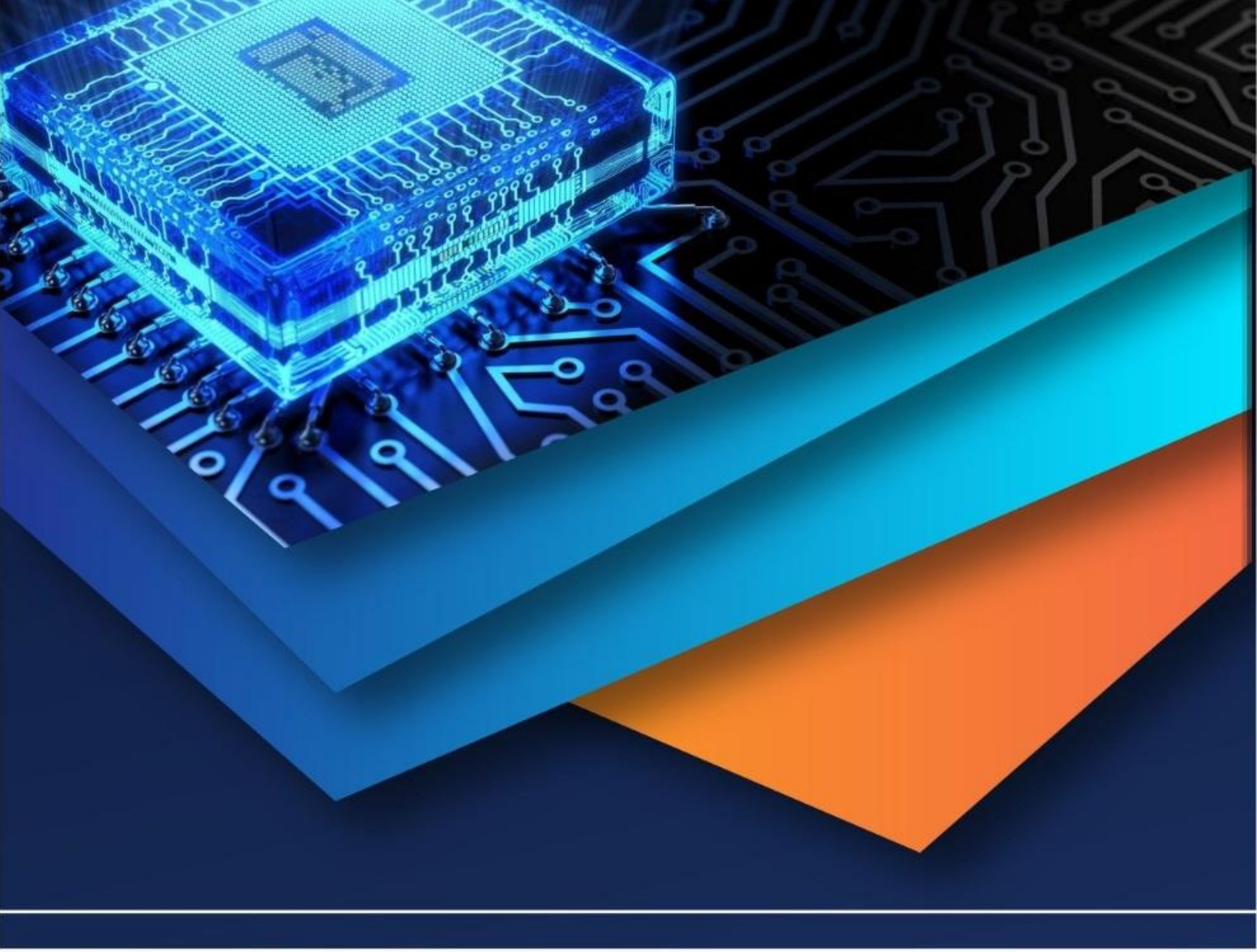
Index Number	Image size (KB)	CP-ABE Downloading Time	AES Downloading Time
1	30	17	15
2	50	21	16
3	100	30	24
4	1000	56	91

V. CONCLUSION

The implications of colour subsampling on grayscale-based picture encryption for electronic toner cartridge systems were investigated in this work. Following a description of the scenario and criteria for picture encryption, a demonstration was given. Furthermore, we recommended that the luminance and sub-sampled chrominance components be combined to create a grayscale-based image. To investigate compression performance and robustness against colour subsampling, a large number of images were compressed and decompressed with colour sub-sampling ratios of 4:4:4 and 4:2:0. The results showed that adding colour subsampling to grayscale-based picture encryption does not affect compression performance and that grayscale-based image encryption is robust against colour subsampling.

REFERENCES

[1] J. Vincent, W. Pan, and G. Coatrieux, "Privacy protection and security in eHealth cloud platform for medical image sharing," in Proc. 2nd Int. Conf. Adv. Technol. Signal Image Process. (ATSIP), Mar. 2016, pp. 93–96.
[2] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," Signal Process., Image Commun., vol. 47, pp. 160–169, Sep. 2016.
[3] J. C. Dagadu and J. Li, "Context-based watermarking cum chaotic encryption for medical images in telemedicine applications," Multimedia Tools Appl., vol. 77, no. 18, pp. 24289–24312, Sep. 2018.
[4] Z. Qian, X. Zhang, Y. Ren, and G. Feng, "Block cipher based separable reversible data hiding in encrypted images," Multimedia Tools Appl., vol. 75, no. 21, pp. 13749–13763, Nov. 2016.
[5] C. V. Kumar, V. Natarajan, K. Nirmala, T. Balasubramanian, K. R. Rao, and S. Krishnan, "Encrypted separable reversible watermarking with authentication and error correction," Multimedia Tools Appl., vol. 78, no. 6, pp. 7005–7027, Mar. 2019.
[6] S. Haddad, G. Coatrieux, M. Cozic, and D. Bouslimi, "Joint watermarking and lossless JPEG-LS compression for medical image security," IRBM, vol. 38, no. 4, pp. 198–206, Aug. 2017.
[7] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains,"Comput. Methods Programs Biomed., vol. 159, pp. 11–21, Jun. 2018.
[8] X.-J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," Multimedia Tools Appl., vol. 76, no. 12, pp. 13995–14020, Jun. 2017.
[9] H. Ga and W. Zeng, "Image compression and encryption based on wavelet transform and chaos," Comput. Opt., vol. 43, no. 2, pp. 258–263, Apr. 2019.
[10] Z. Qian, H. Xu, X. Luo, and X. Zhang, "New framework of reversible data hiding in encrypted JPEG bitstreams," IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 351–362, Feb. 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY