BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 4 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:4 (2022): 313-324
DOI: 10.2478/bjlp-2022-004033

An Innovative Method to Enhance the Distortion Measure of Image Steganography using Advanced Encryption Standard Technique and Least Significant Bit Algorithm by Comparing with OpenCV Algorithm to Achieve Peak Signal to Noise Ratio.

Aarthi B L
Research Scholar, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India, 602105.

Dr.K.Malathi
Project Guide, Corresponding Author, Department of Computer Science and Engineering,
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences,
Saveetha University, Chennai, Tamil Nadu, India, 602105.

Received: August 8, 2022; reviews: 2; accepted: November 29, 2022.

Abstract

Aim: To enhance the distortion measure of encoded images in the process of Image steganography using Cryptography Algorithm for encrypting the data that is Advanced Encryption Standard(AES) with Least Significant Bit Algorithm by comparison to the OpenCV Algorithm. **Methods and Materials:** The two groups are OpenCV Algorithm(N=10) and Least Significant Bit Algorithm using AES(N=10). G-power is calculated for two different groups, alpha (0.05), power (80%). **Results:** The distortion is measured based on the Peak Signal to Noise Ratio value, where the Advanced Encryption Standard Technique using Least Significant Algorithm has the Peak Signal to Noise Ratio value of 80. The two algorithms Least Significant Bit and OpenCV Algorithms are statistically satisfied with the independent sample T-Test (α = .001) value ($p<0.05$) with a confidence level of 95%. **Conclusion:** The distortion measure seems to be better in the Least Significant Bit Algorithm using the Advanced Encryption Standard technique when compared to the OpenCV algorithm.

Keywords

Advanced Encryption Standard (AES), Distortion Measure, Algorithm, Data, Cryptography, Peak Signal to Noise Ratio, Steganography, OpenCV, Image Steganography, Least Significant Bit(LSB), Innovative Method.

INTRODUCTION

Image Steganography is the process of binding information that is text into a cover image. In a way, it is a type of art where invisible or secret communication will take place (Pradhan et al. 2016). The information hidden in the images is not visible to human eyes. There are four types, Image Steganography, Video Steganography, Audio Steganography, and Text Steganography. In this paper, the major discussion is based on Image Steganography. There are two types of techniques in Image steganography, Transform

Domain Techniques and Spatial Domain techniques. Some of the Spatial domain Techniques are LSB substitution, pixel value differencing(PVD), etc, and Transform Domain Techniques are DCT, DWT, etc. Here, the paper will discuss and compare two methods that are Least Significant Bit and the OpenCV algorithm. Image Steganography allows two parties to communicate secretly and covertly. Some of the reasons why data hiding is important are, personal and private data, sensitive data, confidential data, and trade secrets, to avoid misuse of data, unintentional damage of data, human error and accidental deletion of data, monetary and blackmail purposes and to hide traces of crime (Хорев and Сергеев 2020). Moreover, there are applications like confidential communication and secret data storage (Fridrich 2010). Also, it allows for copyright protection on digital files using the message as a digital watermark. Protection of data alteration, access control system for digital content distribution, and media database systems (Sharma and Madhusudan 2015).

Totally more than 20 related articles were published in IEEE and 25 plus related articles were published in Google Scholar like ResearchGate and Sciencedirect. Some of the most cited articles and their findings are, (Arun and Murugan 2017) the author proposed a design of Image Steganography using Least Significant Bit XOR Substitution method for improving security. Here, a random 8-bit secret key that initially XOR with RGB colors is used. Indeed, the storage capacity in the image for data sharing is also improved. (Jaradat, Taqieddin, and Mowafi 2021) the paper implements an innovative method called Image Steganography using chaotic maps and the PSO algorithm aiming at finding the best pixel location to embed the message. Here, the image is divided into 4 blocks. In this paper, the final result has improved the distortion to a minimal value. Also, the Peak Signal to Noise Ratio value is improved to 64. (Elharrouss, Almaadeed, and Al-Maadeed 2020) the article aimed to propose image Steganography using K-Least Significant Bit. The last three Significant Bits are used to embed a text message into a cover image. A method to improve image quality is added to the process after decoding the messaging from the image. As a result, the Peak Signal to Noise Ratio value is very low, that is 33. (Swain 2014) the author implemented an advanced method called Image steganography using nine-pixel differencing and modified Least Significant Bit technique. Here, the image is divided into 3*3 non-overlapping blocks. The PSNR results as an average value of 42. Among all the papers, in my opinion, the best technique is implementing image steganography using chaotic maps and PSO algorithm as it results in a very high PSNR value, which leads to maximum minimizing distortion.

Previously our team has a rich experience in working on various research projects across multiple disciplines (Venu and Appavu 2021; Gudipaneni et al. 2020; Sivasamy, Venugopal, and Espinoza-González 2020; Sathish et al. 2020; Reddy et al. 2020; Sathish and Karthick 2020; Benin et al. 2020; Nalini, Selvaraj, and Kumar 2020).Communicating through a secret path must always be confidential with a good efficiency process. The problems that have to be improved are minimal distortion, high quality, and embedding capacity of encoded images. Now, the growing trend in this area has motivated us to enhance the existing system. Steganography is different from Cryptography where the aim is to hide the data in Steganography whereas in Cryptography the data will be converted to an encrypted form with a key. The advantages of using Steganography over Cryptography are that the hidden data is hard to detect and it is not susceptible to attacks such as rotation and translation. The value of the Peak Signal to Noise Ratio value must be high to improve the image quality using distortion measure as a parameter. The study aims to improve distortion measures using the parameters Peak Signal to Noise Ratio and Mean Square Error(MSE).

METHODS AND MATERIALS

The innovative work is done in the Object Oriented Analysis and Design laboratory, Department of Computer Science and Engineering, Saveetha School of Engineering,

SIMATS. There were two groups. The first group is the Least Significant Bit algorithm(N=10) and the second group is the OpenCV algorithm(N=10). Among the two groups, group 1 is the innovative model, and group 2 is an existing model. The results were calculated (Kang 2021) using G* power software and the minimum power of the analysis is fixed as 0.8 and the maximum accepted error is fixed as 0.5 with a threshold value of 0.05% and the Confidence Interval is 95%.

In this analysis, since the major parameter is the number of pixels of each image, different images get the different Peak Signal to Noise Ratio values. Also, different formats of images like jpg, png, jpeg, bmp, etc can be used with different resolutions to check for a change in image capacity, distortion, and image quality using Peak Signal to Noise Ratio value.

OpenCV

(Singh 2019) OpenCV algorithm is the easiest and simplest method to perform Image Steganography. Here, the existing method uses encrypted data to include other data, which significantly impairs the visual representation of the image. The hidden message is transmitted by increasing the bandwidth of the original message or by manipulating the file format. Also, using OpenCV the Image Steganography is difficult to detect.

Pseudo Code for OpenCV

The algorithm steps in OpenCV Algorithm are:

1. Here, the Tkinter dialog box is used.
2. Use the Tkinter file dialog library to open the file using the dialog box.
3. Obtain the image of the path.
4. Load the image into the GUI using the thumbnail function from Tkinter.
5. Load the image as a NumPy array for efficient computation and change the type of unsigned int.
6. Break the image into character level.
7. Represent character in ASCII.
8. Encode the text.
9. Then, Decode it.
10. Join all the bits to form letters.
11. Also, Join all the letters to form messages.
12. Then, along with the encrypted image, print the Peak Signal to Noise Ratio value after calculating it.

Least Significant Bit(LSB)

(Kodar 2017) image steganography is the process in which hides the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is the LSB embedding algorithm. It is the process of adjusting the Least Significant Bit pixels of the carrier image. It is a simpler approach for embedding a message into an image. The LSB insertion varies according to the number of bits in an image.

In a grayscale image, each pixel is represented in 8 bits. The last bit in a pixel is called the Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. If anyone has considered the last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which the least significant bit of the image is replaced with a data bit. Fig. 1, represents the general block diagram of Image Steganography.

Pseudo Code for LSB

The algorithm steps for Least Significant Bit are:

1. Firstly, read the image.

2. Check the maximum bytes to encode.
3. Convert to binary.
4. Modify LSB only if there is still data to store.
5. Decode it.
6. Split by 8-bits.
7. Convert from bits to Character.
8. Decode the secret data from the image.
9. Print the output.
10. Also, Calculate Peak Signal to Noise Ratio and Mean Square Error-values then print it to analyze.

Advanced Encryption Standard(AES)

The Advanced Encryption Standard (AES) is an advanced innovative approach which has a symmetric block cipher selected via way of means of the U.S. authorities to defend labeled information. AES is applied in software programs and hardware at some point in the arena to encrypt touchy statistics. It is crucial for authorities' laptop security, cybersecurity, and digital statistics protection. Fig. 2, represents the overall process of Advanced Encryption Standard for a 128-bit encryption key.

For encryption, each round consists of the following four steps:

1. Substitute bytes
2. Shift rows
3. Mix columns
4. Add round key.

For decryption, each round consists of the following four steps:

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key
4. Inverse mix columns.

Fig. 3, represents the steps in a single round of encryption and decryption.

Pseudo Code for AES

The algorithm steps for Advanced Encryption Standard(Encryption) are:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

The algorithm steps for Advanced Encryption Standard(Decryption) are:

1. Perform initial decryption rounds.
2. Perform nine full decryption rounds.
3. Perform final XorRoundKey.

For comparing both the models, different images like a set of 10 images for each algorithm are used for calculating MSE, PSNR values. Finally, choose the algorithm which has higher values of PSNR and lower error of MSE. The Peak Signal to Noise Ratio value is inversely proportional to the Mean Square Error.

The system configuration is used for the algorithm to run in a 64-bit Operating System, 4GB RAM PC, Python 3.8, Windows 10, Google Colab, SPSS tool, and Microsoft Office for software specification.

To estimate which algorithm gives the best performance the paper compares Peak Signal to Noise Ratio and Mean Square Error values. The Peak Signal to Noise Ratio value is inversely proportional to the Mean Square Error. This also tells us the image quality with the capacity that can be embedded in the image.

RESULTS

The change in images and their formats will result in a change in Peak Signal to Noise Ratio value. From Table 1, the Peak Signal to Noise Ratio values have been calculated for the data collection of sample size(N=10). From the results, the paper concludes that the Least Significant Bit using AES Algorithm has More Peak Signal to Noise Ratio value compared to the OpenCV algorithm. Moreover, this could also be concluded as Least significant Bit Algorithm has higher image quality and embedding capacity as it has got better values than OpenCV. Also, the distortion is minimal in the least Significant Bit Algorithm. Table 1 represents the data collection from the N=10 sample of images to gain Peak Signal to Noise Ratio and reduce Mean Square Root for increase(%) of image quality and embedding capacity(%). ("Peak Signal-to-Noise Ratio" n.d.) here, the formula is used to calculate Mean Square Root which gives us a lead to calculate the Peak Signal to Noise Ratio value. Also, there is a formula to calculate PSNR from MSE. The lower the Mean Square Error, the higher the Peak Signal to Noise Ratio value will result. The IBM SPSS version 21 statistical software is used for the study. The independent variables are the pixel values and the dependent variables are PSNR, MSE, image quality, and embedding capacity in the study, Image Steganography. In SPSS, the data is collected of sample size N=10 for both OpenCV and Least Significant bit Algorithm. GroupID is given as a grouping variable and PSNR is given as a testing variable. GroupID is given as 1 for OpenCV and 2 for the Least Significant Bit Algorithm. Group Statistics is applied for the Statistical Package for the Social Sciences (SPSS) collected data and shown in Table 2. By performing the statistical analysis group statistics represents the comparison of the PSNR of OpenCV and Least Significant Bit Algorithm. The Least Significant Bit Algorithm using AES has the highest value of PSNR as 82.65 and the lowest is 78.72 in Table 2. This concludes that image quality and embedding capacity is better in the Least Significant Bit Algorithm using AES when compared to the OpenCV algorithm. Fig. 4, represents the comparison chart for the Least Significant Bit(LSB) using AES and OpenCV algorithm using Peak Signal to Noise Ratio value for different sets of 10 images. Table 3 represents the Independent Sample T-Test is applied for the sample collections by fixing the level of significance as 0.005 with a confidence interval of 95%. After applying the SPSS calculation, the Least Significant Bit Algorithm using AES has accepted a statistically significant value($p<0.05$). Fig. 5, represents a simple graph where the X-axis is OpenCV vs Least Significant Bit(LSB) using AES and the Y-axis is the Mean of Peak Signal to Noise Ratio value detection which results in +/- 1SD.

DISCUSSION

The overall results show that there are some variations observed in the Peak Signal to Noise Ratio values which improved the image quality and embedding capacity. That proves that the Least Significant Bit using AES, with a Peak Signal to Noise Ratio value of 80 is better than the OpenCV algorithm with a Peak Signal to Noise Ratio value of 46. There is a statistically significant difference in Image Steganography PSNR values of the two algorithms having a significant accuracy value of 0.001($p<0.005$ Independent sample T-Test).

(Uruma et al. 2019) this paper proposed a method called novel approach to Image Steganography algorithm through image Colorization. The method embedded data into the null space of the colorization matrix. Using this matrix, a large capacity of data can be embedded into the image. The results of this paper proved that the capacity of image storage for data hiding is improved. (Jaradat, Taqieddin, and Mowafi 2021) the Image Steganography which has been developed in this paper is based on chaotic maps and the PSA algorithm. In this paper, the Peak Signal to Noise Ratio is improved drastically which is appreciable. Using this algorithm, the best pixel location is found and the data is embedded here for data hiding. The main motive of this paper was to improve the PSNR value, image quality, embedding capacity, and minimal distortion. (Darbani,

AlyanNezhadi, and Forghani 2019) an Image Steganography method for embedding text messages specifically in JPEG images. In this paper, the amount of capacity of secret data stored in the image is more. Also, the quality of the image is almost similar to the original image. Here, two adjacent pixels are considered where two less significant bits of each pixel are used for embedding. This is another approach that is used for Image Steganography. (Nandi and Ghanti 2017) image Steganography is implemented with unique steps. The process is that firstly the text is encoded using the steps and then embedded into the image. Similarly, the decoding process is done in the reverse process. So, the three steps are reversing, swapping, and circular right shifting for encoding whereas for decoding the steps are left circular shifting, swapping then reversing.
The paper declares that using this method the data embedded in the image will not be lost. (Jangid and Sharma 2017; Rajput, Adhiya, and Patnaik 2017) audio Steganography is another type of Steganography that is being used to embed data for data hiding. In this paper, the algorithm used is the Least Significant Bit(LSB) algorithm. This paper aimed to increase storage capacity and security. The data embedded in the audio file is not embedded sequentially in a particular place, the data is embedded at specific points of the audio file. The proposed algorithm was better than the existing algorithm. (Velmurugan and Hemavathi 2019) in this paper, Audio Steganography is implemented but here it is implemented with a different algorithm. The algorithm used here is Neural Networks using a hash function to increase security. The main reason for using this algorithm is it is difficult to decode the steg-object. (Jangid and Sharma 2017) this paper implements Video Steganography by MLC(Multi-level clustering) algorithm. In this algorithm, K-means clustering is to cluster the cover frame. As a result, the Peak Signal to Noise Ratio is improved and MSE values are reduced. The main motive of this paper was to improve PSNR value.

The Peak Signal to Noise Ratio is better than the OpenCV algorithm in the Least Significant Bit Algorithm using AES. There is a variation that is significantly high and efficient. This method has brought a drastic change on Peak Signal to Noise Ratio value which is an appreciable value.

It must be able to use all the different types of image formats. An algorithm is said to be best only when it is compatible with types of cases and values. So, it is important and necessary to make sure that the algorithm must be made compatible for all types. Finally, after fulfilling the above criteria there will be an automatic improvement in image quality, embedding capacity, and Peak Signal to Noise Ratio value for all types of images.

CONCLUSION

Therefore, the Least Significant Bit using AES is better than the OpenCV algorithm because the Peak Signal to Noise Ratio value is higher in the Least Significant Bit Algorithm. The Peak Signal to Noise Ratio value is 80 and 46 in the Least Significant Bit using AES Algorithm and OpenCV Algorithm respectively. As the Peak Signal to Noise Ratio value increases, the image quality, and embedding capacity also increase. This will also lead to minimizing distortion.

DECLARATIONS

Conflict of Interests

No conflicts of interest in this manuscript.

Authors Contributions

Author ABL was involved in conceptualization, data collection, data analysis, manuscript writing. Author KM was involved in conceptualization, guidance, and critical review of the manuscript.

Acknowledgments
The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

Funding: We thank the following organizations for providing financial support that enabled us to complete the study.

1. Metricbees Pvt.Ltd, Chennai.
2. Saveetha University.
3. Saveetha Institute of Medical and Technical Sciences.
4. Saveetha School of Engineering.

REFERENCES

Arun, Chandni, and Senthil Murugan. 2017. "Design of Image Steganography Using LSB XOR Substitution Method." In *2017 International Conference on Communication and Signal Processing (ICCSP)*. IEEE. https://doi.org/10.1109/iccsp.2017.8286444.

Benin, S. R., S. Kannan, Renjin J. Bright, and A. Jacob Moses. 2020. "A Review on Mechanical Characterization of Polymer Matrix Composites & Its Effects Reinforced with Various Natural Fibres." *Materials Today: Proceedings* 33 (January): 798–805.

Darbani, Abbas, Mohammad M. AlyanNezhadi, and Majid Forghani. 2019. "A New Steganography Method for Embedding Message in JPEG Images." In *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*. IEEE. https://doi.org/10.1109/kbei.2019.8735054.

Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. 2020. "An Image Steganography Approach Based on K-Least Significant Bits (k-LSB)." In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE. https://doi.org/10.1109/iciot48696.2020.9089566.

Fridrich, Jessica. 2010. *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.

Gudipaneni, Ravi Kumar, Mohammad Khursheed Alam, Santosh R. Patil, and Mohmed Isaqali Karobari. 2020. "Measurement of the Maximum Occlusal Bite Force and Its Relation to the Caries Spectrum of First Permanent Molars in Early Permanent Dentition." *The Journal of Clinical Pediatric Dentistry* 44 (6): 423–28.

Jangid, Sachin, and Somesh Sharma. 2017. "High PSNR Based Video Steganography by MLC(multi-Level Clustering) Algorithm." In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE. https://doi.org/10.1109/iccons.2017.8250530.

Jaradat, Aya, Eyad Taqieddin, and Moad Mowafi. 2021. "A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization." *Security and Communication Networks* 2021 (June). https://doi.org/10.1155/2021/6679284.

Kang, Hyun. 2021. "Sample Size Determination and Power Analysis Using the G*Power Software." *Journal of Educational Evaluation for Health Professions* 18 (July): 17.

Kodar, Achmad. 2017. "Implementation of Steganography in Image Media Using Algorithm LSB (Least Significant Bit)." *International Research Journal of Computer Science*. https://doi.org/10.26562/irjcs.2017.aucs10081.

Nalini, Devarajan, Jayaraman Selvaraj, and Ganesan Senthil Kumar. 2020. "Herbal Nutraceuticals: Safe and Potent Therapeutics to Battle Tumor Hypoxia." *Journal of Cancer Research and Clinical Oncology* 146 (1): 1–18.

Nandi, Biswarup, and Mousumi Ghanti. 2017. "Lossless Steganography: An Approach for Hiding Text under Image Cover." In *2017 International Conference on Inventive Computing and Informatics (ICICI)*. IEEE. https://doi.org/10.1109/icici.2017.8365389.

"Peak Signal-to-Noise Ratio." n.d. Accessed October 1, 2021. https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

Pradhan, Anita, Aditya Kumar Sahu, Gandharba Swain, and K. Raja Sekhar. 2016.

"Performance Evaluation Parameters of Image Steganography Techniques." In *2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)*. IEEE. https://doi.org/10.1109/rains.2016.7764399.

Rajput, Shital P., Krishnakant P. Adhiya, and Girish K. Patnaik. 2017. "An Efficient Audio Steganography Technique to Hide Text in Audio." In *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE. https://doi.org/10.1109/iccubea.2017.8463948.

Reddy, Poornima, Jogikalmat Krithikadatta, Valarmathi Srinivasan, Sandhya Raghu, and Natanasabapathy Velumurugan. 2020. "Dental Caries Profile and Associated Risk Factors Among Adolescent School Children in an Urban South-Indian City." *Oral Health & Preventive Dentistry* 18 (1): 379–86.

Sathish, T., and S. Karthick. 2020. "Gravity Die Casting Based Analysis of Aluminum Alloy with AC4B Nano-Composite." *Materials Today: Proceedings* 33 (January): 2555–58.

Sathish, T., D. Bala Subramanian, R. Saravanan, and V. Dhinakaran. 2020. "Experimental Investigation of Temperature Variation on Flat Plate Collector by Using Silicon Carbide as a Nanofluid." In *PROCEEDINGS OF INTERNATIONAL CONFERENCE ON RECENT TRENDS IN MECHANICAL AND MATERIALS ENGINEERING: ICRTMME 2019*. AIP Publishing. https://doi.org/10.1063/5.0024965.

Sharma, Vipul, and Madhusudan. 2015. "Two New Approaches for Image Steganography Using Cryptography." In *2015 Third International Conference on Image Information Processing (ICIIP)*. IEEE. https://doi.org/10.1109/iciip.2015.7414766.

Singh, Himanshu. 2019. "Advanced Image Processing Using OpenCV." *Practical Machine Learning and Image Processing*. https://doi.org/10.1007/978-1-4842-4149-3_4.

Sivasamy, Ramesh, Potu Venugopal, and Rodrigo Espinoza-González. 2020. "Structure, Electronic Structure, Optical and Magnetic Studies of Double Perovskite Gd2MnFeO6 Nanoparticles: First Principle and Experimental Studies." *Materials Today Communications* 25 (December): 101603.

Swain, Gandharba. 2014. "Digital Image Steganography Using Nine-Pixel Differencing and Modified LSB Substitution." *Indian Journal of Science and Technology*. https://doi.org/10.17485/ijst/2014/v7i9.27.

Uruma, Kazunori, Katsumi Konishi, Tomohiro Takahashi, and Toshihiro Furukawa. 2019. "A Novel Approach to Image Steganography Based on the Image Colorization." *2019 IEEE Visual Communications and Image Processing (VCIP)*. https://doi.org/10.1109/vcip47243.2019.8965732.

Velmurugan, K. Jayasakthi, and S. Hemavathi. 2019. "Video Steganography by Neural Networks Using Hash Function." In *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*. IEEE. https://doi.org/10.1109/iconstem.2019.8918877.

Venu, Harish, and Prabhu Appavu. 2021. "Experimental Studies on the Influence of Zirconium Nanoparticle on Biodiesel–diesel Fuel Blend in CI Engine." *International Journal of Ambient Energy* 42 (14): 1588–94.

Хорев, П. Б., and А. В. Сергеев. 2020. "Application of Steganography in the Corporate Environment." *Информационно-технологический вестник*, no. 4(26) (December): 104–9.

TABLES AND FIGURES

Table 1. Data collection from the N=10 sample of images to gain Peak Signal to Noise Ratio and reduce Mean Square Root for increase(%) of image quality and embedding capacity.

DataSet Sample (Different Images)	PSNR (OpenCV Algorithm)	PSNR (AES-LSB Algorithm)
1	46.5	80.1
2	47.19	82.09

3	48.1	82.65
4	46	78.9
5	47	81.73
6	46	78.72
7	48	81.25
8	48.1	81
9	47.3	79.68
10	46.8	80

Table 2. This is group statistics for both algorithms. Comparison of the Peak Signal to Noise Ratio values of OpenCV and Least Significant Bit using AES. The highest PSNR value of OpenCV is (48.1) and the lowest is (46). The highest PSNR value of the Least significant Bit using AES is (82.65) and the lowest is (78.72)

	Groups	**N**	**Mean**	**Std.Deviation**	**Std.Error Mean**
PSNR	**OpenCV**	10	47.0990	0.79848	0.25250
	AES-LSB	10	80.6120	1.34004	0.42376

Table 3. Independent Samples T-Test is applied for the sample collections by fixing the level of significance as 0.05 with a confidence interval of 95%. After applying the SPSS calculation, the Least Significant Bit using AES Algorithm has accepted a statistically significant value($p<0.05$).

		Levene's Test for Equality of Variances		**T-Test for Equality of Means**						
		F	**Sig.**	**T**	**df**	**Sig. (2-tailed)**	**Mean Difference**	**Std.Error Difference**	**95% Confidence Interval of the Difference**	
									Lower	**Upper**
PSNR	**Equal Variances assumed**	4.373	0.051	-67.939	18	0	-33.513	0.49328	-34.54935	-32.47665
	Equal Variances not assumed			-67.939	14.675	0	-33.513	0.49328	-34.56643	-32.45957

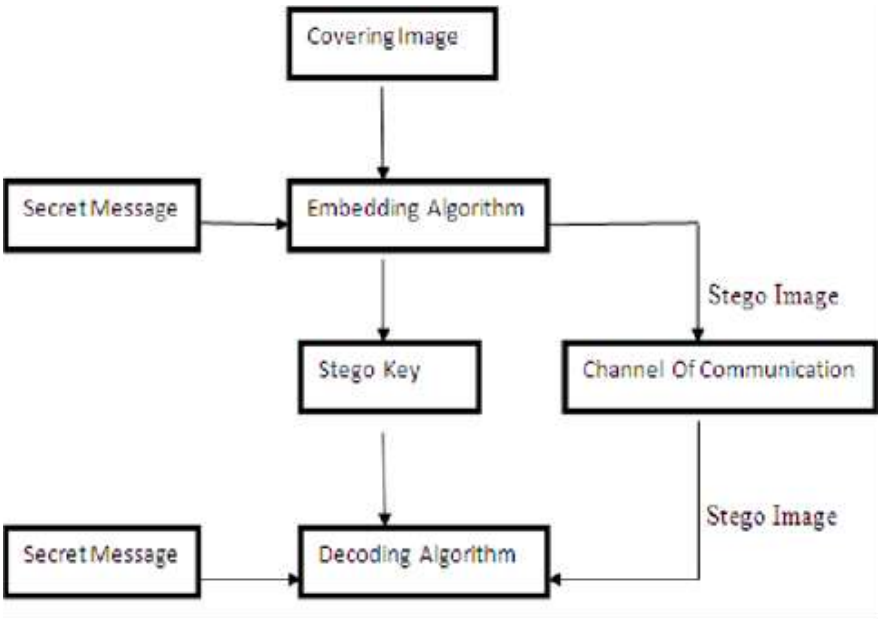

Fig. 1. Block diagram of Image Steganography

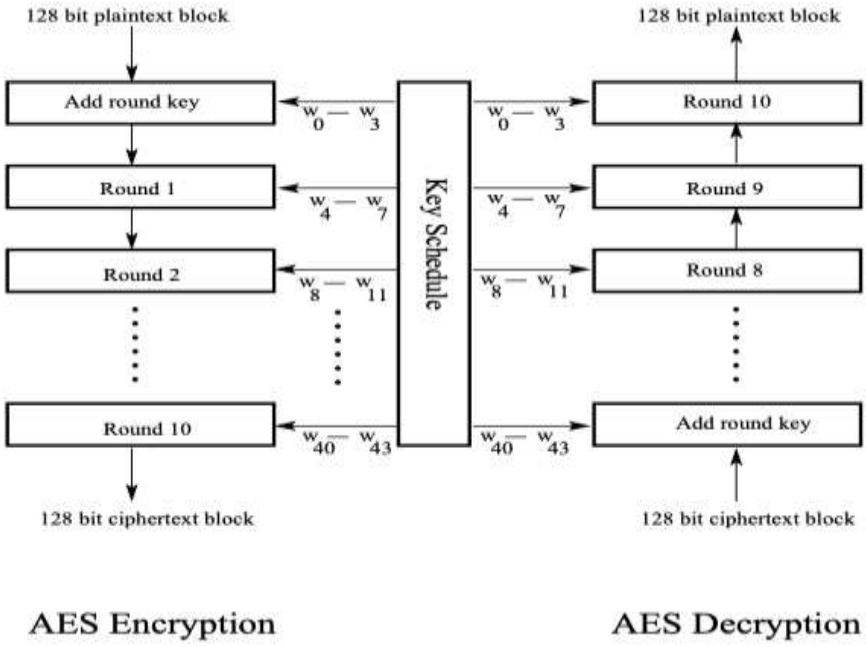

Fig. 2. Overall process of Advanced Encryption Standard for a 128-bit encryption key.

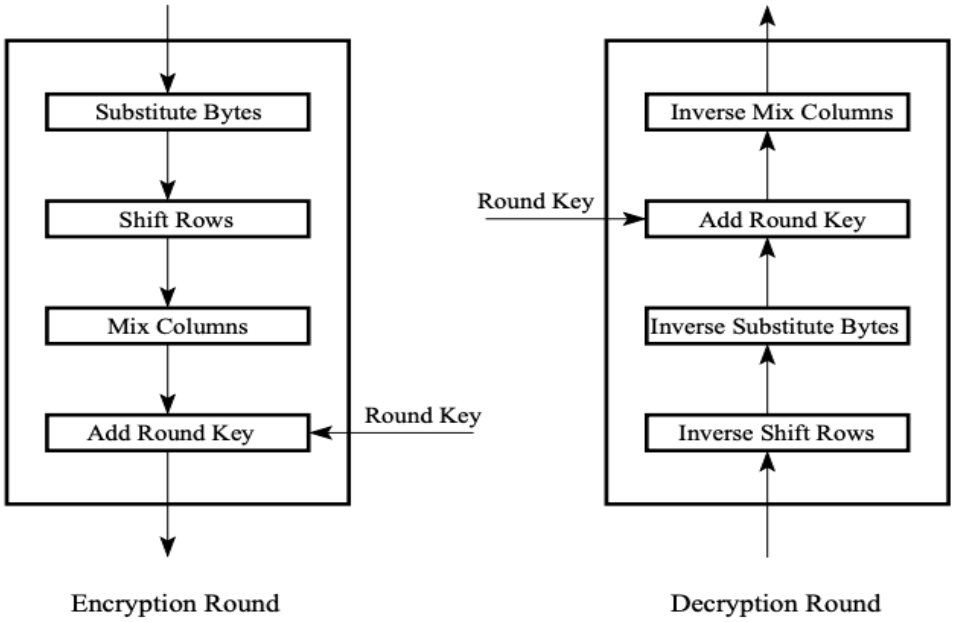

Fig. 3. Steps in a single round of encryption and decryption.

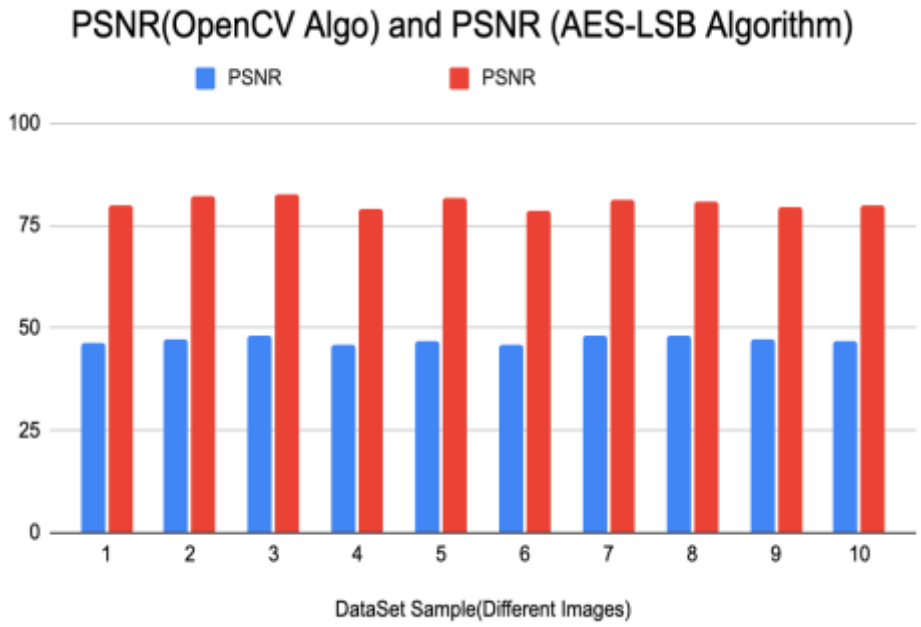

Fig. 4. A comparison chart of Peak Signal to Noise Ratio values for Least significant Bit using AES algorithm and OpenCV algorithm.

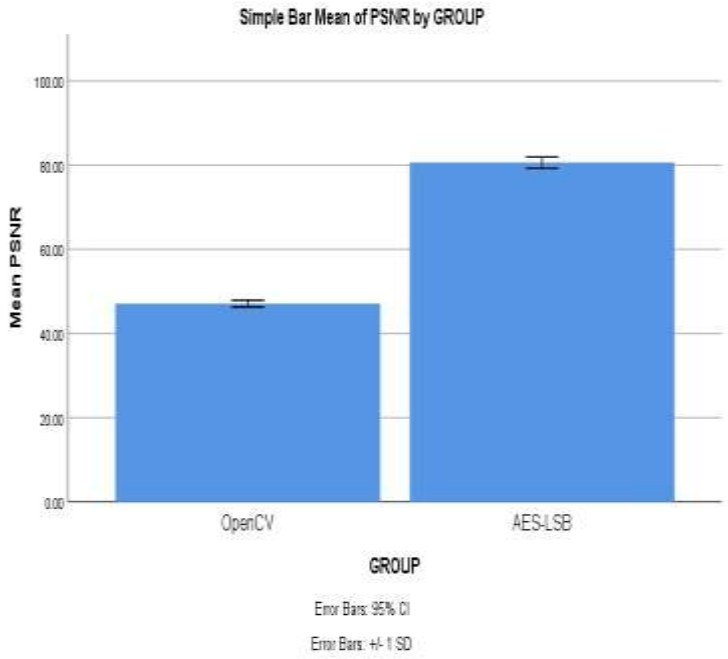

Fig. 5. Bar graph between OpenCV and Least Significant Bit using AES. Comparison of OpenCV and LSB using AES in terms of PSNR values. The PSNR values of LSB using AES are better than OpenCV. X-Axis: OpenCV vs Least Significant Bit using AES Y-Axis: Mean of Peak Signal to Noise Ratio detection is +/- 1SD.