Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(7), 127-141
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Comparative Analysis of Impact of Steganography and Crypto-Stego on Network Performance

Chinwe Chizoba Eromosele

School of Computing, Engineering, and Built Environment, Glasgow Caledonian University (GCU), Glasgow, United Kingdom
Email: chikatchy@yahoo.com

How to cite this paper: Eromosele, C.C. (2025) Comparative Analysis of Impact of Steganography and Crypto-Stego on Network Performance. *Journal of Computer and Communications*, **13**, 127-141.
https://doi.org/10.4236/jcc.2025.137006

Received: June 11, 2025
Accepted: July 15, 2025
Published: July 18, 2025

Abstract

Backgrounds: The impact of digital image steganography (stego) and crypto-steganography (crypto-stego) on network performance has not been adequately examined. The major objective of this research is to compare the impacts of both on latency, transfer time, and throughput. Minor objectives include determination of the relationship between payload ratio and data size, latency, and throughput, as well as effect of AES-256 encryption on size of plaintext data. Materials and methods: A virtual network was set up using EVE-NG. OpenStego was used for encryption and embedding of data. Two sets of data, each ranging from 100 to 900 kilobytes in size, were transmitted through the network. The data sets were classified into digital image steganography (stego) and crypto-steganography (crypto-stego). The former contained plaintext while the latter had AES-256 encrypted cipher text. The increase in size of plaintext after encryption was noted. Latency, transfer time, and throughput were recorded using Netperf. Pearson correlation and t-test of two independent means were used in statistical analysis. Results: Crypto-stego has a higher latency, transfer time and throughput than digital image steganography. Reasons for the discrepancy have been offered in the write up. However, the size of the embedded data has strong, statistically significant ($p < 0.05$), positive correlation with each of the three network performance matrices. Payload ratio has a perfect linear relationship with data size and strong, highly statistically significant (<0.01), positive correlation with latency and throughput. Both plaintext and cipher text had essentially equal data size. Conclusion: Users of crypto-stego should expect to enjoy enhanced data security but poor network performance. The perfect linear relationship between payload ratio and data size facilitated the estimation of maximum data size with low imperceptibility risk. AES-256 encryption has a negligible effect on plaintext data size.

Keywords

Crypto-Steganography, Digital Image Steganography, Network Performance, Latency, Transfer Time, Throughput, AES-256 Encryption, Payload Ratio, Least Significant Bit (LSB) Embedding

1. Introduction

Digitalization of global economy, use of remote workforce, increasing reliance on internet for communication, and emergence of telemedicine and electronic health records have made protection of sensitive digital information extremely important for organizations and individuals [1]. On the flip side the increasing sophistication of cybercriminals, some of whom have included artificial intelligence tools in their arsenal, has resulted in a rising trend in security data breaches over the years. Thus, the number of reported incidents of data security compromises in the US has risen from 157 in 2005 to 3205 in 2023 [2]. There was a 1% drop in 2024 according to the annual report of Identity Theft Resource Center [3]. These compromises are associated with significant financial costs for organizations. As an example, the average cost of data breaches globally has jumped from 4.35 million US dollars in 2023 to 4.88 million in 2024 [4].

The objectives of data security are hinged on three cardinal principles-maintenance of confidentiality, integrity, and availability of sensitive information. The techniques available for achievement of these are varied but can be categorized into three, namely cryptography(crypto), steganography (stego), and cryptography-steganography (crypto-stego).

Cryptography, the oldest and most widely used, functions on the principle of scrambling normal comprehensible text into a format (cipher text) which is unintelligible to unauthorized parties. It requires keys for coding and decoding.

Through innovations and adaptations, cryptography has evolved over the ages from Caesar Cipher of Julius Caesar to modern cryptography whose origin is traced to the 1970s [5]. Caesar Cipher applied rudimentary techniques, comprising shifting of alphabets. By today's standards, the degree of security it offered would have been considered weak as it can be easily breached. Contrarily, modern cryptography, which uses complex mathematical algorithms, offers stronger data protection. However, it is not foolproof, and it is vulnerable to brute force and quantum attacks. Currently, AES-256 algorithm is considered the most robust as it has not yet been cracked [6]-[9].

Digital steganography, introduced by Simmons in 1983 [10] works on the principles of imperceptibility and deception. Sensitive information is hidden within an innocuous carrier medium. The latter may be digital image, video, audio, text, or network. Digital image is the most widely used. The flip side of steganography is that it provides a covert channel of communication for criminals, which can be used in the distribution of malware and ransomware and is vulnerable to steganal-

ysis.

Crypto-steganography (crypto-stego): Crypto-stego is the most recent technique which was probably introduced in 2014. Its objective is to mitigate the deficiencies of standalone cryptography and steganography [11] [12] By combining the deception principle of steganography with the coding and decoding principle of cryptography it offers double layer of protection to sensitive information. Thus, even if the hidden information is unmasked, the intruder still has the extra task of decoding the message. Despite this advantage its use is not as widespread as cryptography and steganography probably because of the complexity of its effective implementation, associated high overhead costs, and increased vulnerability to steganalysis.

Previous studies on digital image steganography and crypto-steganography have focused mostly on security, robustness, payload capacity, and development of novel embedding techniques with little or no attention to their effects on network performance [13] [14].

Both steganography and crypto- steganography, have a common embedding process with different techniques. Randomized Least significant bit (LSB), a commonly used technique enhances the security of the stego image. As a result of the random replacement of the cover image bits the stego image is resistant to steganalysis [15].

All data security techniques have variable effect on network performance and efficiency because of associated overhead. Network performance has been described as the quality of service a network offers to its users [16]. It is usually reflected in the speed of transmitting information over a network or retrieval of a document. Its metrics include transfer time, latency, throughput, bandwidth, packet loss, Jitter, Error Rate, Utilization, Availability and Mean Opinion Score (MOS).

There is scarcity of information on the impact of digital image steganography and crypto-stego on network performance. The major objective of this research is to compare the impacts of both on network performance. This will enable users who want to change from one to the other know beforehand the expected tradeoff with network performance. Minor objectives include determination of correlation between embedded data and selected network performance metrics, exploration of the relationship between payload ratio and any of these- original data size, latency, throughput, and effect of AES-256 encryption on plain text data size.

2. Materials and Methods

A simulated network was created as shown in **Figure 1**, using EVE-NG, consisting of three Cisco routers configured with Enhanced Interior Gateway Routing Protocol (EIGRP). Two Ubuntu 20.04 systems (server and client) were set up with 2 CPU cores, 4 GB RAM each, and connected via File Transfer Protocol (FTP) for file transfers. The experiment was conducted on a host machine with an Intel Core i7-8700 processor, 64 GB RAM, and a 1 TB Hard Disk Drive (HDD).

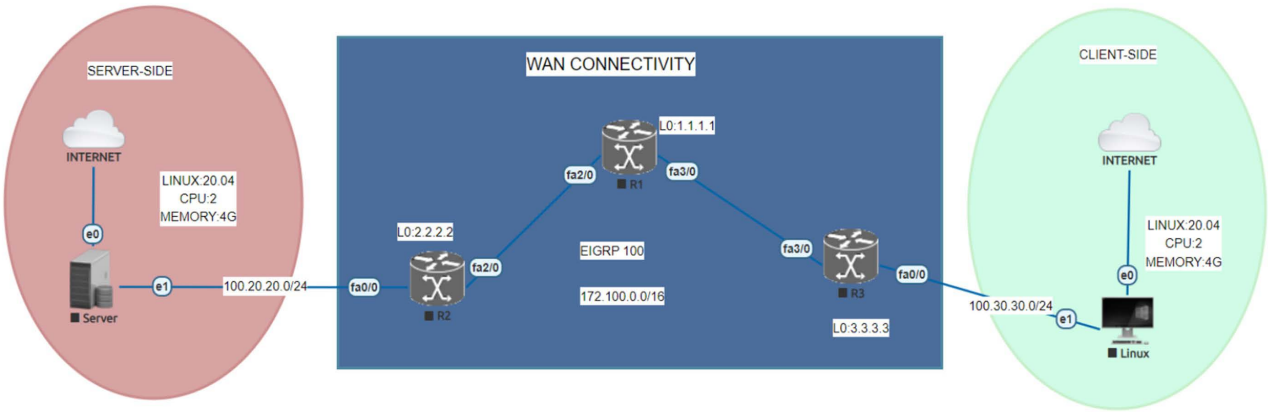


Figure 1. Network topology.

2.1. Software Configuration

1) Encryption: openssl (openssl enc -aes-256-cbc -salt -in "plaintext_file" -out "encrypted_file").

2) Latency Measurement: Netperf (sudo netperf -H server_IP -t TCP_RR -- -o min_latency, max_latency, mean_latency).

3) File Transfer: vsftpd for FTP (sudo apt install vsftpd).

4) Steganography & Crypto-Steganography: OpenStego, a Java written, open source tool, was used for encryption and embedding process.

2.2. Simulation Procedure

1) Data Generation: Plaintext files (100 – 900 KB) were created using dd if = /dev/zero of = file2.txt bs = 1 K count = x.

2) Cover image: 80 kb Joint Photographic Experts Group (JPEG) image was used as cover file.

3) Embedding of Text Files: OpenStego first converted JPEG cover image into BMP format. During embedding the Least Significant Bits (LSB) in pixel channels were replaced with payload bits in a randomised order. Consequently, there is no significant increase in the size of the output file (stego/cryptostego file). This process required 4 steps. Step 1: Extraction of the values of Red, Green, Blue (RGB) colours for each pixel in the cover image by Java's BufferedImage class. Step 2: Conversion of payload data into byte array. Step 3: Transformation of byte array into a stream of bits. Step 4: Randomised replacement of LSB of each RGB channel of a pixel by the payload bitstream. This last step required creation of random numbers by a pseudo-random number generator (PRNG). The numbers determined location of pixels and positions of bits for embedding.

4) Encryption and Embedding of Plain Text Files: Plain text files were encrypted using the AES-256 encryption algorithm before being embedded into digital images with openstego using the Least Significant Bit (LSB) method. This produced a crypto-stego file.

5) File transfer and metrics measurement:

a) The generated digital steganography and crypto-stego files were transferred

using File Transfer Protocol (FTP) which was also used to measure transfer time and throughput across the network.

b) Additionally, Netperf, a performance tool was used to measure the latency for each file transferred.

6) Statistical Analysis: Pearson coefficient of correlation (r) and t-test of two independent means were used in statistical analysis. The level of significance of probability (p) was set at 0.05. Calculations were made at the website of Social Science Statistics [17]. Line graphs and scatter plots were done on the website of statscharts.com [18].

3. Definition of Terms

Latency: The time delay before a packet moves from the source to the destination, representing the time it takes for a packet to travel from the sender to the receiver. It is usually measured in milliseconds (ms).

Transfer Time: The total duration required for a packet or data to move from the source to the destination. It includes the time a packet spends traveling between devices or locations. Transfer time is typically measured in milliseconds (ms) or seconds (s), depending on the data size and network speed.

Throughput: The amount of data successfully transmitted from one point to another within a specific time frame. It is a measure of network performance and efficiency, usually expressed in bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), or gigabits per second (Gbps).

Imperceptibility: The degree of similarity of visual perceptual qualities of stego image and original cover image. It is characterized as high if the stego image cannot be differentiated from the original cover image by visual inspection.

Imperceptibility risk: This refers to the probability of detection of stego image on visual inspection. It is classified as low risk if distortions are not observed on the stego image.

Payload ratio: Percentage of the capacity of a stego file actually utilized in embedding data. It has a relationship with imperceptibility. Payload ratio of 15% is regarded as the threshold. Payload ratio of less than 15% is considered to have low imperceptibility risk. Above this, the risk is high and is associated with image distortion with attendant vulnerability to attacks and data security compromise.

Abbreviations and Acronyms

S = steganography;

CS = cryptography- steganography (crypto-stego).

4. Results

File size

The original 80 kb Joint Photographic Experts Group (JPEG) image was converted before embedding into 2.5 MB Bitmap (BMP) (20971520 bits) by OpenStego. This is the size of the stego file as the embedded data did not significantly increase the file size.

4.1. Payload Ratio

Table 1 represents the embedded data and corresponding payload ratio values, while Figure 2 depicts the line graph showing the relationship between payload ratio and the size of the embedded data. It shows a perfect linear, positive relationship between payload ratio and embedded data size. Pearson correlation (r) is 1. The p-value is <0.01.

Table 1. Embedded data and payload ratio. The sizes of embedded data and payload ratio are presented in Table 1.

Embedded data in kb	Bytes	Bits	Payload ratio in %
100	102,400	819,200	3.9
200	204,800	1,638,400	7.8
300	307,200	2,457,600	11.7
400	409,600	3,276,800	15.6
500	512,000	4,096,000	19.5
600	614,400	4,915,200	23.4
700	716,800	5,734,400	27.3
800	819,200	6,553,600	31.3
900	921,600	7,372,800	35.2

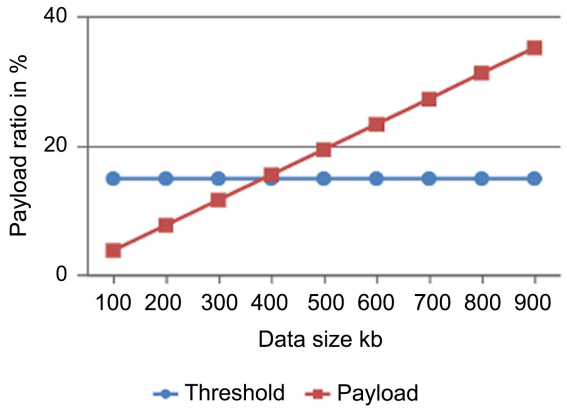


Figure 2. Line graph of payload ratio against embedded data. Horizontal line represents threshold of imperceptibility which occurs at payload of 15%.

The graph line crosses the threshold of imperceptibility at a point slightly below the 400 kb point. The mathematical equation for a straight line is y = mx + c. In this case, it will be R (payload ratio) = m × D (data size) + c (point of intersection on Y-axis. Since both R and D will be zero at intersection, the formula is reduced to R = m × D, where m is a constant obtained by dividing payload ratio by corresponding data size. Data size for 15% payload ratio is 15/0.039 = 384.62 kb.

4.2. Effect of AES-256 Encryption on Embedded Plaintext

32 bytes were added to each embedded data as a result of encryption (Table 2).

This resulted in percentage increase in data size that varied from 0.031% to 0.004% (Figure 3). The values of latency, transfer time, and throughput with corresponding data size are presented in Table 3.

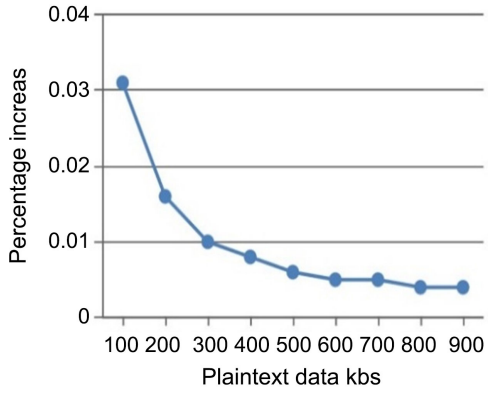


Figure 3. Percentage increase after encryption.

Table 2. Sizes of embedded data and percentage increase after encryption.

Data Size KB	Actual size bytes	Size post-encryption in bytes	% Increase
100	102,400	102,432	0.031
200	204,800	204,832	0.016
300	307,200	307,232	0.01
400	409,600	409,632	0.008
500	512,000	512,032	0.006
600	614,400	614,432	0.005
700	716,800	716,832	0.005
800	819,200	819,232	0.004
900	921,600	921,632	0.004

Table 3. Data size, latency, transfer time, and throughput.

Embedded Data Size KB	Latency (ms)		Transfer Time (sec)		Throughput (MB/s)	
	Latency S	Latency CS	Transfer Time S	Transfer Time CS	Throughput S	Throughput CS
100	44.79	48.25	0.04	0.045	0.36	0.48
200	45.43	48.29	0.04	0.045	0.36	0.5
300	45.87	49.33	0.04	0.045	0.385	0.51
400	47.16	49.5	0.04	0.045	0.425	0.52
500	47.26	49.95	0.04	0.05	0.425	0.53
600	47.74	50.3	0.04	0.055	0.465	0.53
700	48.03	50.37	0.045	0.055	0.475	0.53
800	48.13	50.37	0.045	0.055	0.475	0.53
900	48.15	50.56	0.045	0.06	0.48	0.54

4.3. Latency

Scatter plot demonstrates a linear relationship and a strong correlation between embedded data size and latency of both stego and crypto-stego (Figure 4(a)). Pearson coefficient of correlation (r) is 0.95 and 0.94 for stego and crypto-stego respectively. Each has a p-value of <0.01. These confirm the observation from the scatter plot that there is a statistically highly significant, positive correlation between the size of embedded data and latency.

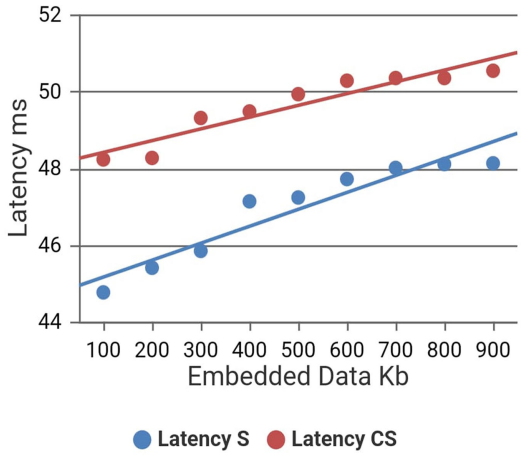
The line graph shows that crypto-stego has a consistently higher latency than stego (Figure 4(b)). The mean latency is 46.95 and 49.66 milliseconds for stego and crypto-stego respectively. The t-value of −5.24 and p-value of <0.01 indicate that the difference of mean latency values is highly significant statistically.

Payload Ratio and Latency

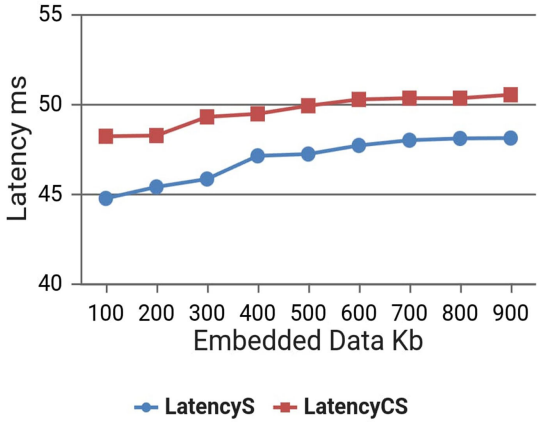
Table 4 represents the payload ratio alongside the corresponding latency for both stego and crypto-stego techniques. The scatter plot illustrates that there is a strong positive linear relationship between payload ratio and latency for both stego and crypto-stego (Figure 4(c)). The r-value is 0.95 and 0.94 for stego and crypto-stego respectively. Each has a p-value of <0.01.

Table 4. Payload ratio and corresponding latency in ms for stego (S) and crypto-stego (CS).

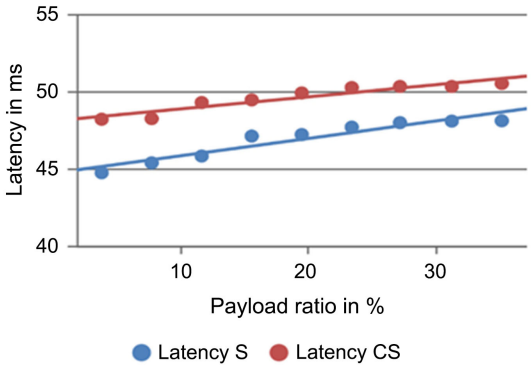
Payload ratio in %	Latency S	Latency CS
3.9	44.79	48.25
7.8	45.43	48.29
11.7	45.87	49.33
15.6	47.16	49.5
19.5	47.26	49.95
23.4	47.74	50.3
27.3	48.03	50.37
31.3	48.13	50.37
35.2	48.15	50.56



(a)



(b)



(c)

Figure 4. (a) Scatter plot of latency against embedded data size; (b) line graph of latency against embedded data size; (c) Scatter plot of latency against payload ratio.

4.4. Transfer Time

The scatter plot shows that embedded data has a linear relationship and strong positive correlation with transfer time (**Figure 5(a)**). R value is 0.82 and 0.94 for stego and crypto-stego respectively. Each has a p-value of <0.01.

The line graph shows that crypto-stego has a consistently higher transfer time than digital image steganography (**Figure 5(b)**). The mean transfer time is 0.04 and 0.05 second for stego and crypto-stego respectively. The t-value of −4.2 and p-value < 0.01 indicate that the difference of mean transfer times is statistically highly significant.

4.5. Throughput

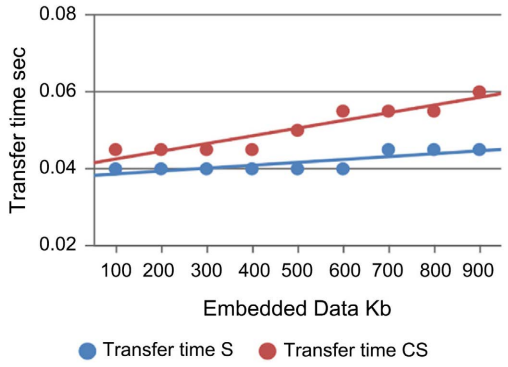
The scatter plot indicates that embedded data has linear relationship and strong correlation with throughput of both stego and crypto-stego (**Figure 6(a)**). R is 0.96 and 0.91 for stego and crypto-stego respectively. Each has a p-value of <0.01. These indicate that there is a strongly positive, statistically highly significant correlation between throughput and embedded data sizes.

In addition, the line graph shows that crypto-stego has a consistently higher throughput than digital image steganography (**Figure 6(b)**). The mean through-

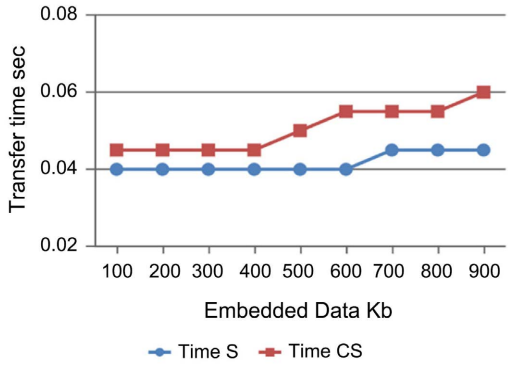
put value is 0.43 mb/sec and 0.52 mb/sec for stego and crypto-stego respectively. The t-value is −5.16 while p-value is <0.01. The difference of the mean throughput values is highly significant statistically.

Payload Ratio and Throughput

Table 5 presents the values of the payload ratio and throughput for both stego and crypto-stego. The scatter plot in Figure 6(c) illustrates a strong positive relationship between payload ratio and throughput. R is 0.96 and 0.91 for stego and crypto-stego respectively. Each has a p-value of <0.01.

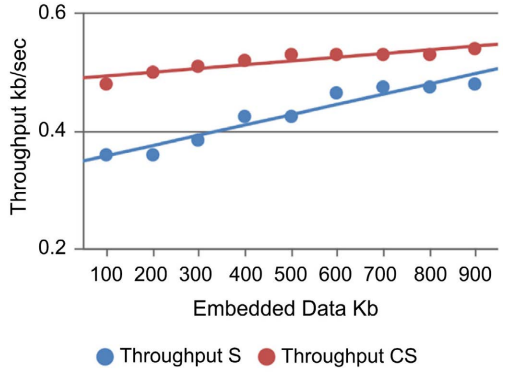


(a)

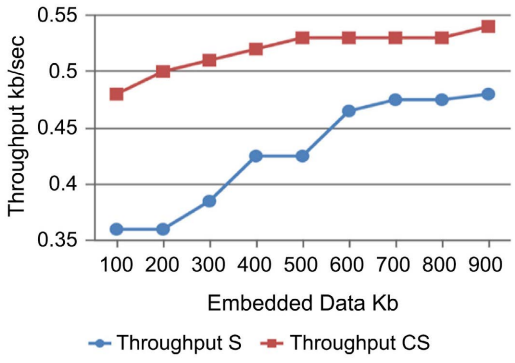


(b)

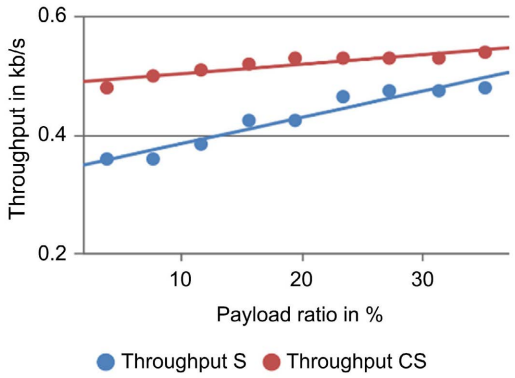
Figure 5. (a) Scatter plot of transfer time against embedded data size; (b) line graph of transfer time against embedded data size.



(a)



(b)



(c)

Figure 6. (a) Scatter plot of throughput against embedded data size; (b) line graph of throughput against embedded data size; (c) Scatter plot of payload against throughput in mb/sec for stego (S) and crypto-stego (CS).

Table 5. Payload ratio and throughput in mb/sec for stego (S) and crypto-stego (CS).

Payload ratio in %	Throughput S	Throughput CS
3.9	0.36	0.48
7.8	0.36	0.5
11.7	0.385	0.51
15.6	0.425	0.52
19.5	0.425	0.53
23.4	0.465	0.53
27.3	0.475	0.53
31.3	0.475	0.53
35.2	0.48	0.54

5. Discussion

From the results of this experimental research, it is evident that crypto-stego with AES 256 encryption has higher latency, transfer time, and throughput than digital image steganography. Individually, high throughput is an indicator of good network performance because large amount of data is being transmitted within a

given time. Contrarily, high latency and transfer time portray poor network performance. In combination, the network performance will be adversely affected because the negative impact of high latency and transfer time will override the positive effect of high throughput. Consequently, crypto-stego with high latency, high transfer time, and high throughput will impede network performance more than digital image steganography.

In real time, organizations that use crypto-stego are expected to experience reduced productivity and increased staff frustration. As a corollary, crypto-stego is recommended for organizations and individuals who place a higher premium on data security than on network performance. These include organizations involved in intelligence gathering, military communications, and researchers keen to protect their intellectual property rights.

Encryption and embedding data into digital image are two processes involved collectively or individually in crypto-stego and stego. Their effect on latency and transfer time may explain the differences in the observed values.

Since data size affects latency and transfer time [19] it is expected that encryption algorithms that significantly increase the size of plaintext will indirectly make crypto-stego have a higher latency and transfer time than stego.

AES-256 algorithm has negligible effect on size of plain text in this study. This implies that crypto-stego and stego data were equal in size. Consequently, post-encryption increase in data size has been unequivocally excluded as a causative factor for the observed discrepancies in the values of latency and transfer time.

However, AES-256 algorithm, with its relatively long key, is regarded as computationally intensive [20] [21]. The extra computational overhead associated with the pre-embedding encryption and the complexity of embedding methods result in increased processing time that has been translated into high latency and high transfer time [22].

Additionally, pre-embedding encryption reduces redundancy of the embedded data. This facilitates incorporation of more data within a given space. Thus, it enables handling of relatively large datasets within a given time and a higher throughput [23].

There is a strong positive correlation between embedded data size, latency and throughput in both stego and crypto-stego. This is in contradistinction with the observations in standalone cryptography with AES-256 encryption in which size of data has no significant association with latency and a transient correlation with throughput in the very small data series: 100 - 900 kb [24]. The difference can be attributed to the extra computational overhead and processing time introduced by the steganographic component. The overhead component in very small data series remains constant irrespective of the data size in standalone cryptography with AES-256 encryption. This overhead exerts stronger influence on latency and throughput than data size.

In this experimental environment, the maximum data size for low imperceptibility risk is approximately 385 kb. Larger data will likely cause distortion of image

and compromise security. Furthermore, payload ratio has a perfect linear relationship with data size. This reflects efficiency in the embedding process. Besides, it offers users the ability to reliably predict messages with low imperceptibility risk and the option of splitting large data into smaller units for safe transmission. The flip side of this perfect linearity is that it is vulnerable to steganalysis.

It is noteworthy that both data size and payload ratio have strong positive relationship with latency and throughput. Since they have essentially equal Pearson correlation coefficient (r) it may be assumed that both exert equal impact on latency and throughput.

6. Conclusion

Although crypto-steganography with AES-256 encryption confers double layer of security on data, it has a more adverse effect on network performance than digital image steganography. Data size has a linear relationship and strong positive correlation with latency, transfer time, and throughput of both crypto-steganography with AES 256 encryption and digital image steganography in very small data series (100 - 900 kilobytes). The perfect linear relationship between payload ratio and data size offers predictability and reliability to users but is vulnerable to steganalysis.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Alsaidi, A., Al-lehaibi, K., Alzahrani, H., Al-Ghamdi, M. and Gutub, A. (2018) Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics*, **8**, 33-42. https://doi.org/10.20967/jcscm.2018.03.002

[2] Petrosyan, A. (2024) Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[3] Identity Theft Resource Center (2024) 2024 Annual Data Breach Report. https://www.idtheftcenter.org/

[4] IBM (2024) Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach

[5] Furht, B., Muharemagic, E. and Socek, D. (2005) An Overview of Modern Cryptography. In: Furht, B., Ed., *Multimedia Encryption and Watermarking*, Springer, 135-176.

[6] Kumar, M. (2022) Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis. *Array*, **15**, Article 100242. https://doi.org/10.1016/j.array.2022.100242

[7] Rao, S.K., Mahto, D., Yadav, D.K. and Khan, D.A. (2017) The AES-256 Cryptosystem Resists Quantum Attacks. *International Journal of Advanced Research in Computer Science*, **8**, 404-408. https://www.ijarcs.info/index.php/Ijarcs/article/view/3025/3008

[8] Gorine, A. and Suhaib, M. (2024) Exploring AES Encryption Implementation through Quantum Computing Techniques. *American Journal of Computer Science and Technology*, **7**, 139-155. https://doi.org/10.11648/j.ajcst.20240704.12

[9] Smith, C. (2024) Department of Anti-Hype: No, China Hasn't Broken Military Encryption with Quantum. https://www.forbes.com/sites/craigsmith/2024/10/16/department-of-anti-hype-no-china-hasnt-broken-military-encryption-with-quantum-computers/

[10] Simmons, G.J. (1984) The Prisoner's Problem and the Subliminal Channel. In: Chaum, D., Ed., *Advances in Cryptology*, Springer, 51-57.

[11] Rahmani, M.K.I., Arora, K. and Pal, N. (2014) A Crypto-Steganography: A Survey. *International Journal of Advanced Computer Science and Applications*, **5**, 168-172.

[12] Taha, M.S., Rahim, M.S.M., Lafta, S.M., Hashim, M.M. and Alzuabidi, H.M. (2019) Crypto-Steganography: Enhancing Data Security Using Advanced Embedding Algorithms. *IOP Conference Series*: *Materials Science and Engineering*, **518**, Article 052003.

[13] Wang, D., Yang, G., Chen, J. and Ding, X. (2024) GAN-Based Adaptive Cost Learning for Enhanced Image Steganography Security. *Expert Systems with Applications*, **249**, Article 123471. https://doi.org/10.1016/j.eswa.2024.123471

[14] Kumbhakar, D., Sanyal, K. and Karforma, S. (2023) An Optimal and Efficient Data Security Technique through Crypto-Stegano for E-Commerce. *Multimedia Tools and Applications*, **82**, 21005-21018. https://doi.org/10.1007/s11042-023-14526-7

[15] Yanuar, M., Suryadi, M.T., Apriono, C. and Syawaludin, M.F. (2024) Image-to-Image Steganography with Josephus Permutation and Least Significant Bit (LSB) 3-3-2 Embedding. *Applied Sciences*, **14**, Article 7119. https://doi.org/10.3390/app14167119

[16] Nadenggan, H.R.S. and Riadi, I. (2022) Analysis of Local Area Network Performance Using Quality of Service. *International Journal of Computer Applications*, **183**, 43-51. https://doi.org/10.5120/ijca2022921866

[17] Social Science Statistics. https://www.socscistatistics.com

[18] StatCharts.Com. https://www.statscharts.com

[19] Daoud, L., Hussein, F. and Rafla, N. (2019) High-Level Synthesis Optimization of AES-128/192/256 Encryption Algorithms. *International Journal of Computers and Their Applications*, **26**, 129-136. https://www.researchgate.net/publication/336835049_High-Level_Synthesis_Optimization_of_AES-128192256_Encryption_Algorithms#fullTextFileContent

[20] Abdelrahman, A.A., Fouad, M.M. and Dahshan, H.M. (2017) Analysis on the AES Implementation with Various Granularities on Different GPU Architectures. *Advances in Electrical and Electronic Engineering*, **15**, 526-535. https://doi.org/10.15598/aeee.v15i3.2324

[21] Singh, S. and Attri, V.K. (2015) State-of-the-Art Review on Steganographic Techniques. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, **8**, 161-170. https://doi.org/10.14257/ijsip.2015.8.7.15

[22] Abolade, O., Okandeji, A., Oke, A., Osifeko, M. and Oyedeji, A. (2021) Overhead Effects of Data Encryption on TCP Throughput across IPSEC Secured Network. *Scientific African*, **13**, e00855. https://doi.org/10.1016/j.sciaf.2021.e00855

[23] Zhao, J., Yang, Z., Li, J. and Lee, P.P.C. (2024) Encrypted Data Reduction: Removing Redundancy from Encrypted Data in Outsourced Storage. *ACM Transactions on Storage*, **20**, 1-30. https://doi.org/10.1145/3685278

[24] Eromosele, C.C. (2025) Evaluating the Impact of AES-256 Encryption on Network Performance: An Analysis of Transfer Time, Latency and Throughput. *International Journal of Scientific Research and Modern Technology*, **4**, 49-58.