International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 8, pp. 3010-3026
doi: 10.25147/ijcsr.2017.001.1.200
https://stepacademic.net

Short Paper*

Modified Least Significant Bit Algorithm Applied in Digital Image Signature

Gabriel Nicoh H. Barrios
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
gnhbarrios2020@plm.edu.ph
(corresponding author)

Youzelle Migo F. Gundayao
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
ymfgundayao2020@plm.edu.ph
(corresponding author)

Francis Emanuel E. Santoyo
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
feesantoyo2020@plm.edu.ph
(corresponding author)

Vivien A. Agustin
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
vaagustin@plm.edu.ph

Dan Michael A. Cortez
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
dmacortez@plm.edu.ph

Raymund M. Dioses
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
rmdioses@plm.edu.ph

Jonathan C. Morano
College of Information Systems and Technology Management, Pamantasan ng Lungsod ng Maynila, Philippines
jcmorano@plm.edu.ph

Date received: May 7, 2024
Date received in revised form: July 19, 2024; July 11, 2024
Date accepted: July 15, 2024

Recommended citation:

Barrios, G. N. H., Gundayao, Y. M. F., Santoyo, F. E. E., Agustin, V. A., Cortez, D. M. C., Dioses, R. M., & Morano, J. C. (2024). Modified least significant bit algorithm applied in digital image signature. *International Journal of Computing Sciences Research*, *8*, 3010-3026. https://doi.org/10.25147/ijcsr.2017.001.1.200

**Special Issue on International Research Conference on Computer Engineering and Technology Education (IRCCETE). Guest Associate Editors: Dr. Roben A. Juanatas (National University-Manila) and Dr. Nelson C. Rodelas (University of East).*

Abstract

Purpose – This study aims to improve the embedding process and the integration of an additional layer of security to enhance the overall security of the based Least Significant Bit Algorithm.

Method – The study incorporated the use of NTRUEncrypt for the encryption of the plaintext message, and a randomized embedding technique by generating random pixel locations based on the Lorenz Chaos System. This was assessed using histogram analysis to show the difference between the original and the stego-image, Mean Squared Error (MSE), and Peak signal-to-noise ratio (PSNR).

Results – The modification has been evaluated using a histogram along with the result of its PSNR and MSE, at which the modified least significant bit algorithm obtains the highest PSNR score of 77.078% and the lowest MSE score of 0.0012% for the 512x512 image size, which resulted in a less distorted image and better quality of the image compared to the original base LSB.

Conclusion – The modification of the least significant bit algorithm successfully implemented a randomized embedding process through the Lorenz System and encrypted the secret message through NTRUEncrypt before embedding to further secure the message inside the image. Image distortion was also lessened as tested from the different sizes of images, which were tested through the PSNR and MSE metrics.

Recommendations – The study suggests the implication of machine learning algorithms in generating key pixel locations for data embedding and the use of text compression algorithms to reduce the size of the embedded secret message.

Research Implications – This study is a significant resource for future researchers interested in exploring literature on image steganography and secure communication. Thus, it introduces a novel approach by integrating lattice-based encryption and chaos systems, thereby enhancing secure communication through digital image steganography.

Keywords – digital image signature, image steganography, least significant bit, Lorenz system, NTRUEncrypt

INTRODUCTION

The continuous progression of digital technologies has shown a significant impact on our daily lives, whether for productivity, communications, etc. Computers are now everywhere, and these are utilized to obtain information and move data from different places. However, this growth of digital technology has also had its drawbacks since problems with cybercrimes and data breaches are becoming rampant. With that, necessary measures are needed to ensure that the confidentiality and integrity of data remain intact, especially when it is being transmitted over the Internet. There are two important techniques for providing security, these are cryptography and steganography (Arya & Soni, 2018). Cryptography is the practice of securing information by encryption so that only an authorized person with the right tool can decrypt secret information. On the other hand, Steganography is the technique or practice of hiding a message or information inside a digital medium (Yadahalli et al., 2019).

Steganography works by utilizing unused and redundant parts of a file in a specific format wherein it is embedded in a way that is difficult to notice and since images, videos, and audio digital files contain an excessive amount of redundant data, they are commonly used in steganography techniques (Abed et al., 2015). There are two main domains in image steganography, namely spatial domain, and frequency domain. Cosine, Wavelet, and Fourier transformations are used in the frequency domain. In the spatial domain, Least Significant Bit (LSB) and Pixel Value Differencing (PVD) are the commonly used methods (Setiadi, D., 2019). The Least Significant Bit approach involves concealing a confidential message by modifying the least significant bits of an existing image while avoiding any changes to the most significant bits so that it does not result in unwanted distortion to the image (Jayapandiyan et al., 2017). However, the Least Significant Bit embedding method can generate problems because it only modifies pixel points sequentially, meaning that the first bit of the message will be stored in the least significant bit of the first pixel. Making it simple to identify the hidden message through data analysis. It only occupies a certain part of the pixel of the carrier image and does not utilize the entire pixel space provided in the image (Al-Azzeh et al., 2019; Dong, 2020).

Encryption is not used in the least significant bit algorithm, which is generally considered an extra security precaution to guarantee that the hidden message cannot be deciphered in its original form. Meaning, that the traditional LSB is vulnerable to being

retrieved, decoded, and modified by unauthorized persons (Alatawi & Narmatha, 2020). Furthermore, this study is structured with a solution to overcome these drawbacks: initially, to improve data security by integrating NTRUEncrypt which is a Lattice-based Cryptography, an innovative encryption technique that protects against unauthorized access. And a random embedding method based on the Lorenz Chaos System.

LITERATURE REVIEW

Least Significant Bit Algorithm

The Least Significant Bit Algorithm (LSB) approach involves concealing a confidential message by modifying the least significant bits of an existing image and avoiding any changes to the most significant to prevent producing unwanted distortion to the image (Jayapandiyan et al., 2017). The main advantage of LSB compared to other techniques is that it is easier to hide secret message bits directly in the Least Significant Bit plane of the cover image. However, if an individual is aware of a specific hidden message concealed in an image, the traditional LSB technique can be easily extracted using straightforward bit manipulation (Al-Azzeh et al., 2019; Abed et al., 2020). Normally, the Least Significant Bit embedding method occurs by a sequential selection of pixel points, meaning that the first bit of the message will be stored in the least significant bit of the first pixel, making it relatively easy to extract the secret data by simply manipulating a few bits (Abed et al., 2020). Additionally, the least significant bit algorithm lacks encryption, which is regarded as an added security measure to ensure that the concealed message remains indecipherable in its original form. Furthermore, numerous research findings have indicated that incorporating encryption and integrating based LSB with encryption could significantly improve overall security, especially since steganography is not generally standardized and in need of a uniform level of security capability (Gutub & Al-Shaarani, 2020; Tayyeh & Al-Jumaili, 2022).

Lorenz System

There are two kinds of pseudorandom generators. These are the linear PRNG, which utilizes the linear recurrences modulo, and the linear feedback shift register for generating pseudorandom sequences. The chaotic system is determined as a non-linear system with excellent randomness, fast speed, and lower cost. Chaotic systems have been widely used in the design of pseudorandom sequence generators (Yildirim & Tanyildizi, 2023). The Lorenz system possesses numerous characteristics, making it suitable for cryptographic operations (Al-Hazaimeh et al., 2019; Shakir et al., 2023). According to the study by Alshammari, A. (2019), significant requirements are needed to be attained when creating a cryptographic requirement; it should pass the tests for confusion and diffusion, randomness of bit stream sequence, and sensitivity of mismatched key. In the study, they tested the Lorenz randomness Generator by generating 100 binary sequences, each containing 1,000,000 bits. These sequences were subjected to randomness tests to identify

and mitigate any vulnerabilities in the Lorenz system. With that, the cryptosystem was evaluated using the NIST randomness test. Wherein. These tests are essential for determining the quality and dependability of random number generators used in cryptography applications (Rukhin et al., 2010). The used of Lorenz system successfully passed all the NIST 800-22 statistical randomness tests.

NTRUEncrypt

Lattice-based Cryptography is an advancement that contributes to the basic principles of cybersecurity laying the foundations to improve ineffective cryptographic policies (Pradhan et al., 2019). Wherein among the post-quantum cryptography families, Lattice-based Cryptography is constantly accepted due to its provision of a rich set of primitive cryptographic protocols that can be used for dealing with the problems posed by deployment across computing platforms including the capability to perform computational power on encrypted data by providing better foundations for procedures based on asymmetric key cryptography against intruders (Nejatollahi et al., 2019). In the study by Harjito et al (2019), they compared two asymmetric cryptography systems, particularly the Rivest-Shamir-Adleman and Nth-Degree Truncated Polynomial Ring algorithms based on their key generation time, encryption, decryption, and security level. Wherein, the study determined that the NTRUEncrypt algorithm is more resilient and secure than the Rivest-Shamir-Adleman algorithm, making it recommended for security utilization. In addition, RSA, NTRU, and ECC which are all encryption algorithms classified as asymmetric were also compared by (Khalaf et al., 2019) based on three parameters: key size, encryption generation, and time for decoding. The result gathered indicates that ECC produces smaller key sizes compared to RSA and NTRU. However, NTRU has a better performance compared to ECC and RSA for time complexity and the overall security of the encryption algorithms.

METHODOLOGY

This study aims to mitigate the deficiencies associated with the based Least Significant Bit Algorithm that was identified in the study. This includes the base Least Significant Bit algorithm not encrypting the secret message when embedded, which allows unauthorized individuals to read the message, and only embedding the bits inside the image sequentially, making it vulnerable to statistical attacks. With this, the study is focused on developing innovative methods to address these challenges and improve the overall performance of Least Significant Bit Image steganography by enhancing the security of the plaintext through encryption using NTRUEncrypt and randomizing the embedding process of the secret message inside the cover image based on the Lorenz Chaos System.

Framework of the Modified Least Significant Bit Algorithm

Figure 1 illustrates the implementation of the Modification to the Least Significant Bit Algorithm. The green and yellow colors denote the modifications and tweaks done to the Least Significant Bit Algorithm while the blue color denotes the original least significant bit algorithm. The process is divided into three stages: the input stage, the process stage, and the output stage. For the input stage, the study utilizes a plaintext message and four images obtained from the Image Processing Place; these images were divided into four different sizes which are 64x64, 128x128, 256x256, and 512x512 that would serve as our inputs.

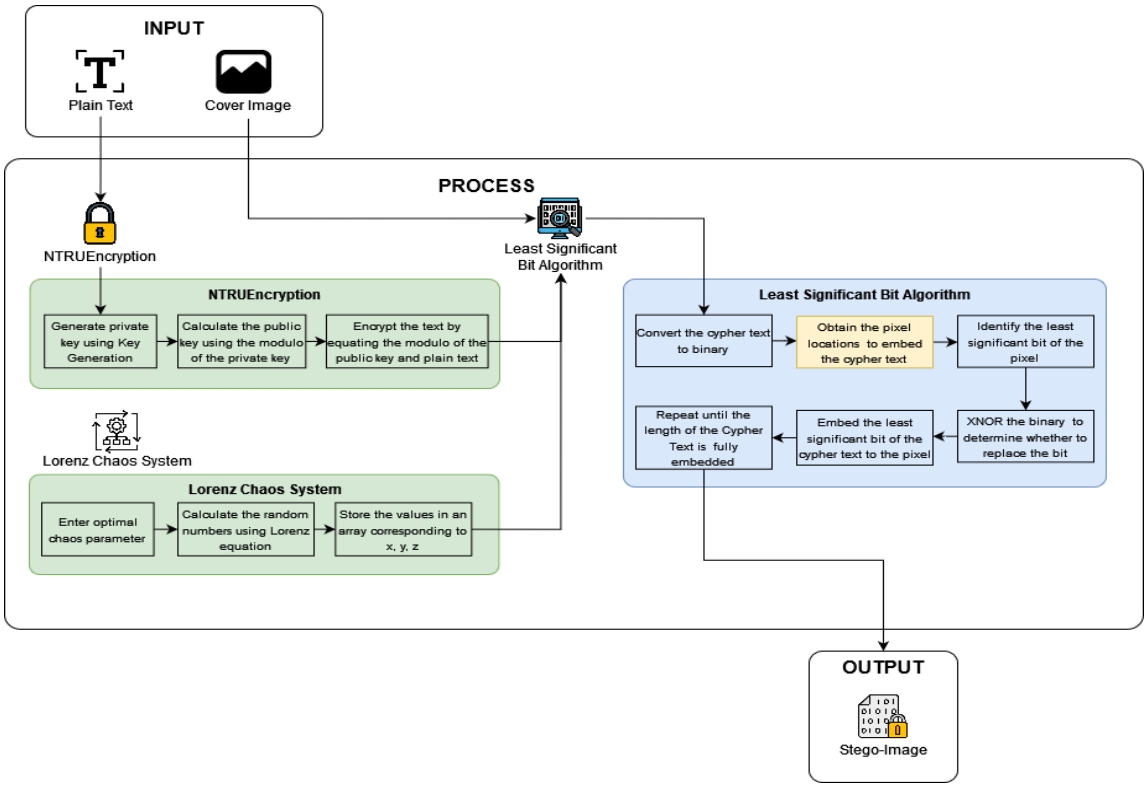

Figure 1. Framework of the Modified Least Significant Bit Algorithm

For the Process stage, the plaintext will be encrypted using NTRUEncrypt, which is an asymmetric encryption that utilizes two different keys for encryption and decryption. The key generation for the public key will occur by using the modulo of the private key, and then encrypting the text by equating the modulo of the public key and the plaintext. On the other hand, the binary form of the cover image is needed to gather each pixel's least significant bit. Next, the ciphertext that is produced will be converted to its binary equivalent, then, the random embedding of the encrypted message will be performed based on the Lorenz Chaos System. The process will repeat until the whole cipher text is embedded inside the image.

For the output stage, after the secret data is embedded, the stego-image will be generated as an output. To verify the message, the stego-image needs to be decrypted by using the proper private key for encryption from the authorized user.

For evaluating the performance of the algorithm enhancement, the most common type of assessment for Image Steganography will be utilized. These include Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR).

These metrics shall determine the quality of the stego-image generated from the modified algorithm. The MSE aims to assess the image distortion and total quadratic mistake between the original image and the stego-image. It can be computed using Equation 1:

Equation 1

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}[I(x,y) - K(x,y)]^2$$

Where m denotes the height and n denotes the width of the cover image along with the stego-image. While I (x, y) and K (x, y) denote the pixel values of the two images (Tayyeh & Al-Jumaili, 2022).

Peak Signal-to-Noise Ratio (PSNR) aims to assess the image quality of the stego-image. As well as test how cohesive the stego-image is to the cover image. It can be computed using Equation 2:

$$PSNR = 10\log_{10}\frac{Max^2}{MSE} \qquad \textit{Equation 2}$$

Where Max is the total number of values inside a pixel, which is 255. A higher Peak Signal-to-Noise Ratio (PSNR) value indicates a better-quality image, and a lower Mean Squared Error (MSE) value implies a smaller discrepancy between the stego-image and original image (Bakhshali et al., 2021; Yadahalli et al., 2019).

RESULTS AND DISCUSSIONS

Secret Message Encryption using NTRUEncrypt

In the Modified Least Significant Bit Algorithm the secret message was modified from plaintext ASCII to a lattice-based encryption format called NTRUEncrypt. The NTRU algorithm requires both a public and private key to encrypt and decrypt a plaintext ASCII. The parameters used for generating the public and private NTRU keys are N=107, p=3, q=64.

```
Private Key Exists
input_image: D:\OLD-sawcon\New-Documents\Github\lsb-test-ntru\RESULTS\peppers-512x512.png
data before: hello world
[*] Maximum bytes to encode: 98304
[*] Encoding data...
secret data:  -3 -21 23 -9 10 -11 9 25 13 -24 -11 28 24 -22 32 17 7 -5 1 26 12 12 28 -22 -4 28 -21 -
9 -2 27 -3 -4 2 29 29 17 -14 32 -24 -16 -15 -11 -16 12 27 25 13 -21 -28 -14 18 -18 31 -9 -1 20 18 -3
0 -31 23 23 -14 19 12 20 17 -7 7 -13 -8 -3 29 0 31 -16 10 25 24 -12 26 -24 -26 -9 3 -20 25 -24 31 32
 30 9 27 -2 -6 -18 -20 16 -23 19 -8 -10 -18 30 -18 22 -28 6 =====
Data about to encode: 2816
Data Encoded, skip this pixel
[+] Saved encoded image.
```

Figure 2. Sample output of encrypting a plain text ASCII using NTRUEncrypt

In figure two (2), after confirming that the private key has already been generated, it counts the maximum number of bytes the image can store. This is calculated using (width * length * 3) / 8. Then the secret message is encrypted using NTRUEncrypt and converted into its binary equivalent.

Image Imperceptibility

The image used in this study was obtained online and has been used as one of the standard test images for digital image processing. The standard pixel dimensions for image processing testing are 512x512, 256x256, 128x128, and 64x64. The original cover image and the stego-image were tested separately for MSE, PSNR, and histogram analysis. The images were chosen as they represented a wide range of red, green, and blue hues which makes the images the perfect candidate for standard image testing.

Figure 3. Cover images (top) and the corresponding stego-images (bottom) from left to right Baboon, Boat, Fruits, and Peppers

Figure three (3) shows the comparison of the initial cover image located at the top row and the modified stego-image located at the bottom row. The figure shows that there is no visible difference between the images. The modified stego-images were embedded with a secret message that when compared with the original image, the naked eye could not see any difference. Regardless of whether the image has RGB values or grayscale, the modified LSB manages to trick the naked eye by making each image have no noticeable difference at a glance. The modified LSB alters the smallest bit of the pixel to embed the image so that even if there is a difference on the image in a technical sense, there is no marginal difference in a visual sense which would alarm any suspicion on the images provided.

Modified Least Significant Bit Secret Message Embedding

The modification of the message embedding is the next step in modifying the Least Significant Bit Algorithm. Initially, the LSB algorithm embeds the data sequentially meaning it embeds from the first row of the image, if the row is already embedded it moves to the next, until the message is fully embedded. In the Modified Least Significant Bit, the researchers utilized the Lorenz Chaos System as a basis for generating random pixel pairs for the image to be embedded. Since the Lorenz Chaos System is sensitive to the initial parameters for its random generation the researchers used the following parameters sigma=10, rho=28, and beta=8/3 which are the optimal parameters for the Lorenz Chaos System.

```
(368,115),(274,321),(332,189),(67,230),(415,86),(289,94),(417,500),(395
,117),(118,313),(236,498),(22,363),(238,50),(161,153),(441,148),(224,67
),(414,471),(159,175),(25,322),(381,131),(221,393),(106,187),(459,116),
(501,436),(477,380),(345,200),(15,16),(438,119),(20,313),(200,258),(186
,499),(167,334),(486,408),(317,313),(69,242),(159,145),(20,260),(213,14
1),(350,11),(425,194),(390,316),(102,299),(241,239),(139,353),(95,145),
(476,0),(278,412),(332,457),(240,179),(427,137),(247,52),(304,496),(283
,344),(210,120),(314,63),(213,496),(434,60),(476,102),(265,176),(12,401
),(474,199),(242,406),(175,83),(164,465),(255,255),(102,79),(166,10),(6
4,101),(359,439),(246,495),(235,77),(101,91),(432,8),(435,376),(123,97)
,(210,109),(55,107),(115,142),(379,101),(126,461),(173,67),(118,41),(38
8,424),(114,64),(78,259),(467,10),(277,463),(147,5),(322,196),(410,397)
,(368,223),(483,497),(134,126),(280,291),(247,456),(397,427),(6,268),(9
7,87),(113,253),(245,86),(389,377)
```

Figure 4. Sample list of randomized x and y pixels generated from the Modified Least Significant Bit Algorithm

Figure four (4) exhibits a sample of the first 100 pixels generated based on the Lorenz Chaos System. After encrypting the plaintext message and converting it to its

binary equivalent, the Modified Least Significant Bit Algorithm generates the randomized pixel locations where the binary secret message will be embedded. The algorithm will go to the randomized pixel location and extract the red, green, and blue values of the pixel. Since a binary consists of eight numbers a total of three pixels will be used to store the 8-bit binary. It will compare the least significant bit of the pixel and embed the binary respectively. If the last bit of the r channel is 1 and the data to be embedded is also 1 then there would be no change. However, if the last bit of b is 1 and the data to be embedded is 0 then the last bit of b will be modified to 0. To check if all the data is embedded the algorithm checks for the initial size of the message and the total size embedded through the loop. After which the loop will end.

Histogram

Comparing the images side by side without using any tools would not show much of a difference between the original and the stego-image. However, if the images were analyzed using a histogram, it can plot the differences between the original cover image and the modified stego image. On the first row where we compare baboon-64x64 and baboon-64x64_ENHLSB. In Figure five (5), the difference in the number of blue pixels around bin 75 increased on baboon-64x64_ENHLSB. This indicates that the modified bits of the blue pixels either increased or decreased by one bit. The smaller the image dimension the more noticeable the difference between the images. Compare this to baboon-512x512 and baboon-512x512_ENHLSB. Where the number of pixels in the bins is not that noticeable on the plot this is the benefit of using a larger image size when utilizing the modified LSB.

Modified LSB Properties and Embedding

Table 1 describes the image “baboon” and its different image sizes. It should be noted that the data embedded across all stego-images is "hello world" equivalent to around 2800 bytes. The size of the original cover image and modified stego image are different as the modified stego image is smaller than the cover image except for the image with the largest dimensions. The size difference of the images is less than the original up until the largest image size of 512x512 where in the size increase is only around 4 KB. As the size of the image increases the number of bytes the modified LSB can embed also increases. The amount of time it takes to embed the data also increases as the size of the image increases.

Histogram of Cover Image and Stego Image (R, G, B)

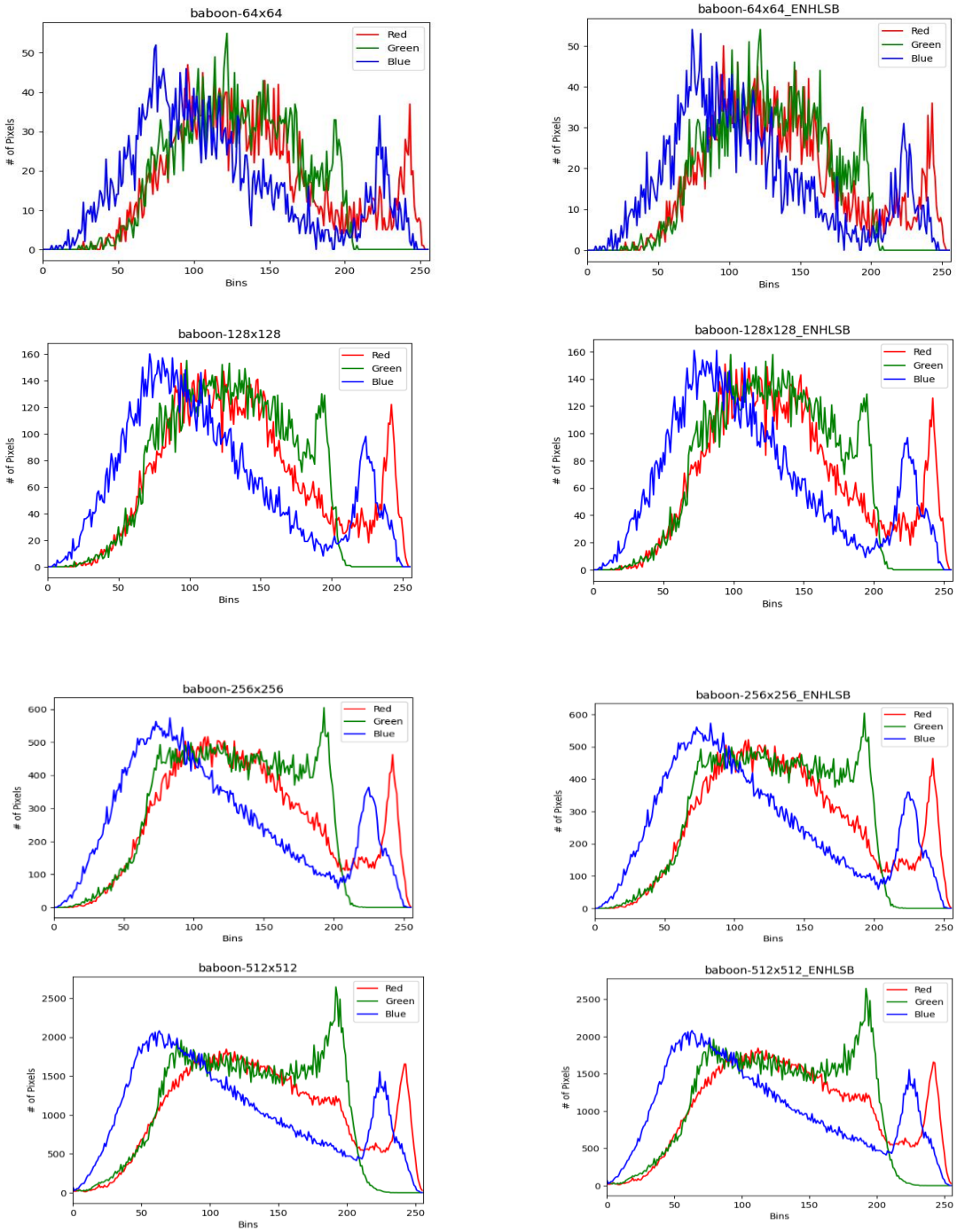

Figure 5. The histogram images of the original cover image (left) and the stego image with the embedded secret message (right).

Table 1. Image Size, Cover Image File Size, Stego Image File Size, Size of byte embedded, Elapsed time.

Image Name	Image Size	Cover Image File Size	Stego Image File Size	Max bytes to encode	Elapsed Time for embedding
baboon-64x64.png	64x64	11471 bytes	10205 bytes	3536 bytes	0.30 seconds
baboon-128x128.png	128x128	45803 bytes	39859 bytes	6144 bytes	0.37 seconds
baboon-256x256.png	256x256	186122 bytes	160035 bytes	24576 bytes	0.64 seconds
baboon-512x512.png	512x512	637192 bytes	643164 bytes	98304 bytes	1.75 seconds

Image Quality Assessment

Making changes to the original cover image can distort the quality of the image. These metrics are used by comparing the original image and the modified stego-image. To evaluate the image quality of the modified stego-image the study shall make use of the metrics of MSE and PSNR.

Table 2. Comparison between the base LSB stego-image and Modified LSB stego image using MSE and PSNR

Base LSB Image	Modified LSB Image	MSE		PSNR	
		Base LSB	Modified LSB	Base LSB	Modified LSB
baboon64base.png	baboon-64x64.png	0.1326	0.0823	56.906	58.978
baboon128base.png	baboon-128x128.png	0.0333	0.0205	62.903	65.011
baboon256base.png	baboon-256x256.png	0.0081	0.0052	69.036	70.955
baboon512base.png	baboon-512x512.png	0.0020	0.0013	75.040	76.777
boat64base.png	boat-64x64.png	0.1210	0.112	57.290	57.636
boat128base.png	boat-128x128.png	0.0317	0.0281	63.106	63.638
boat256base.png	boat-256x256.png	0.0077	0.0071	69.245	69.602
boat512base.png	boat-512x512.png	0.0019	0.0016	75.223	75.862
fruits64base.png	fruits-64x64.png	0.1240	0.0879	57.178	58.691
fruits128base.png	fruits-128x128.png	0.0318	0.0211	63.098	64.871
fruits256base.png	fruits-256x256.png	0.0074	0.0057	69.402	70.567
fruits512base.png	fruits-512x512.png	0.0017	0.0013	75.822	76.669
peppers64base.png	peppers-64x64.png	0.1220	0.0974	57.264	58.244
peppers128base.png	peppers-128x128.png	0.0306	0.0214	63.267	64.822
peppers256base.png	peppers-256x256.png	0.0080	0.0052	69.086	70.968
peppers512base.png	peppers-512x512.png	0.0016	0.0012	76.0837	77.078

The findings in Table 2 indicate that the modified LSB produces satisfactory PSNR results and the MSE confirms that there is no marginal difference visually between the original cover image and the modified stego image. Large image sizes have a better PSNR score as the amount of data the modified LSB can embed inside the images is vastly larger than the other image sizes. When comparing the stego-images generated by the base LSB method and the Modified LSB technique, the Modified LSB shows a better PSNR and MSE score than that of the base LSB. The biggest factor for these scores is the length of the secret message as well as the pixel location for the data embedding. The modified LSB

scored lower in MSE indicating it has less distortion and quadratic error than the LSB. PSNR score for the modified LSB is also higher which means that the output stego-image is more cohesive and has less noise than the base LSB.

CONCLUSION AND RECOMMENDATIONS

Conclusion

Image steganography using the Least Significant Bit Algorithm integrated with NTRUEncrypt and Lorenz Chaos was successfully tested and implemented in this study. The modification satisfied all the evaluations such as histogram, PSNR, and MSE required by the researchers. The findings indicated that the Modified LSB is an enhancement to the base least significant bit algorithm in terms of image distortion, encryption, and image embedding process. Graphical metrics from the histogram showed that there is no marginal difference between the original cover image and the modified stego image. The findings from the PSNR and MSE tests indicate that the Modified LSB performed positively on the generated stego-image. With the highest PSNR score of 77.078 and an MSE score of 0.0012 for the 512x512 image size generating a less distorted image. This signifies that the modified LSB yields a better stego-image, exhibiting a closer resemblance to the original cover image. The plaintext message's encryption using NTRUEncrypt resulted in a more secure secret message increasing the algorithm's confidentiality. NTRUEncrypt lattice nature makes it harder to acquire the secret message without the proper private and public keys in place. The embedding process of the Least Significant Bit algorithm was further modified via a randomized embedding process utilizing the Lorenz Chaos System. This improvement resulted in the NTRUEncrypt encrypted plain text being embedded randomly throughout the image requiring a key to decipher the location.

Recommendations

For future suggestions, it can be experimented with different image formats, particularly those with lossless compression characteristics, and embedding audio or video files inside an image. Text compression algorithms also help to reduce the image's file size immensely, as encrypted text requires more bytes to encode compared to plaintext format. Furthermore, the use of machine learning algorithms to generate key pixel locations was also suggested for data embedding.

ACKNOWLEDGEMENT

The researchers would like to express their sincere gratitude to their instructors, thesis advisers, and everyone else who helped them immensely during their research journey. The researchers are grateful to their professors for their expert knowledge, mentorship, and continuous encouragement, which greatly contributed to the success of their work.

DECLARATIONS

Funding

The study did not receive funding from any institution.

Conflict of Interest

The researcher declares no conflict of interest in this study.

Informed Consent

Not applicable.

Ethics Approval

Not applicable.

REFERENCES

Abed, S., Al-Huwais, N. H., Atiyah, Y. A., Parvin, S., & Gawanmeh, A. (2020). (2020, October). An Improved Least Significant Bit Image Steganography Method. In *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)* (pp. 90-96). IEEE.https://ieeexplore.ieee.org/document/9264299

Al-Azzeh, J., Alqadi, Z., Ayyoub, B., & Sharadqh, A. (2019). Improving the security of LSB image steganography. *JOIV: International Journal on Informatics Visualization*, *3*(4), 384-387.

Al-Hazaimeh, O., Al-Jamal, M., Alhindawi, N., Omari, A., (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing and Applications*, *31,* 2395–24051.

Alatawi, H., & Narmatha, C. (2020, September). The Secret image hiding schemes using Steganography-Survey. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-5). IEEE. doi: 10.1109/ICCIT-144147971.2020.9213764.

Alshammari, A. (2020). Comparison of a Chaotic Cryptosystem with Other Cryptography Systems. *Engineering, Technology & Applied Science Research, 10,* 6187-6190. 10.48084/etasr.3745.

Arya, A., & Soni, S. (2018). Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method. *International Journal of Computer Science Trends and Technology (IJCST)*, *6*(2), 160-165. https://www.ijcstjournal.org/volume-6/issue-2/IJCST-V6I2P30.pdf

Bakhshali, M. A., Gholizadeh, M., Layegh, P., Nahidi, Y., Memarzadeh, Z., Meybodi, N. T., & Eslami, S. (2021). Evaluation of High-Efficiency Image Coding algorithm for dermatology images in teledermatology. *Skin Research and Technology*, *27*(6), 1162-1168. https://pubmed.ncbi.nlm.nih.gov/34251058/

Dong, W. (2019, November). Research on Least Significant Bits (LSB) Image Information Hiding Based on Random Bit Selection Embedding Algorithm. In *Proceedings of the 4th International Conference on Intelligent Information Processing* (pp. 41-43). https://doi.org/10.1145/3378065.3378073

Gutub, A., & Al-Shaarani, F. (2020). Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. *Arabian Journal for Science and Engineering*, *45*(4), 2631-2644.

Harjito, B., Tyas, H. N., Suryani, E., Wardani, D. W. (2022). Comparative analysis of RSA and NTRU algorithms and implementation in the cloud. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *13*(3), 157- 164. https://tinyurl.com/usjrk4d9

Jayapandiyan, J. R., Kavitha, C., & Sakthivel, K. (2020). Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. *IEEE Access*, *8*, 136537-136545.

Khalaf, A.O., Salah, S.K., Sartep, H.J., & Abdalrdha, Z.K. (2019). Subject Review: Comparison between RSA, ECC & NTRU Algorithms. *International Journal of Engineering Research and Advanced Technology,* 5(11), 11-15. https://ijerat.com/index.php/ijerat/article/view/167

Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-quantum lattice-based cryptography implementations: A survey. *ACM Computing Surveys (CSUR)*, *51*(6), 1-41. https://doi.org/10.1145/3292548

Pradhan, P. K., Rakshit, S., & Datta, S. (2019, March). Lattice-based cryptography: Its applications, areas of interest & future scope. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 988-993). IEEE. https://ieeexplore.ieee.org/document/8819706

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, N., Dray, J., Vo, S., & Bassham, L. (2010). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. CSRC. https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final

Setiadi, D. R. (2019). Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation. *International Journal of Electronics and Telecommunications,* 65(2), 287-292. https://www.ijet.pl/index.php/ijet/article/view/10.24425-ijet.2019.126312/553

Shakir, D.A. Q., Salim, A., Al-Rahman, S. Q., (2023). Image Encryption Using Lorenz Chaotic System. Journal of Techniques, 5, 122–128. https://doi.org/10.51173/jt.v5i1.840

Yadahalli, S. S., Rege, S., & Sonkusare, R. (2020, June). Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)* (pp. 1325-1330). IEEE. doi: 10.1109/ICCES48766.2020.9137887

Tayyeh, H. K., & Al-Jumaili, A. S. A. (2022). A combination of least significant bit and deflate compression for image steganography. *International Journal of Electrical and Computer Engineering*, *12*(1), 358-364.

Yildirim, G., & Tanyildizi, E. (2023, May). Random Number Generator Based on Optimization and Chaotic System. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE. doi: 10.1109/ISDFS58141.2023.10131689.

Authors' Biography

Gabriel Nicoh H. Barrios is a determined researcher in the field of computer science, with a vision to push the boundaries of computing. Born in Kanagawa, Japan but raised in the Philippines, Mr. Barrios' interest in computing technology sparked his fascination with solving problems and helping other people. With flame in his eyes and eagerness to learn new things, Mr. Barrios and his colleagues embarked on a journey to find a way to further the field of computer science. Through hard work and inspiration from his loved ones and colleagues, Mr. Barrios discovered valuable insights into image steganography and general information security. Mr. Barrios' dedication to furthering the field continues as he strives for a more secure and progressive world.

Youzelle Migo F. Gundayao is an optimistic researcher in computer science, who aspires to advance the limits of computing. He is a student at Pamantasan ng Lungsod ng Manila and is driven by his dedication and the support of his loved ones and peers to achieve his goals through diligent effort and inspiration.

Francis Emanuel Santoyo is a Computer Science Student of Pamantasan ng Lungsod ng Maynila. He's been a competitive student and player-athlete. He had won a research contest back then in senior high school before going into college. His research involves innovation, challenges, security, and privacy. He currently works as a Designing and Branding Volunteer in Google Developer Student Club at Pamantasan ng Lungsod ng Maynila.

Ms. Vivien A. Agustin is currently an Assistant Professor at the Pamantasan ng Lungsod ng Maynila. She serves as the Program Chairperson of the Information Technology Department under the College of Information Systems and Technology Management. Before joining Pamantasan ng Lungsod ng Maynila, she was a professor at the Universidad de Manila for 22 years, where she also served as the program coordinator. She earned a bachelor's degree in information technology from St. Paul University in Tuguegarao, Cagayan. Additionally, she holds a master's degree in information technology from Pamantasan ng Lungsod ng Maynila (2021) and a Master of Public Management Governance from Universidad de Manila (2015). Currently, she is pursuing her Doctorate in Information Technology at La Consolacion University Philippines. She is a member of the Philippine Society of Information Technology Educators (PSITE-NCR), Institute of Industry and Academic Research Incorporated, and Aloysian Publication. Having published her research on a global scale in the field of Information Technology, she is currently working on new research that she hopes to publish and present.

Dr. Dan Michael A. Cortez is currently the Vice President for Research Academic and Extension Services at the Pamantasan ng Lungsod ng Maynila. He is also the former Program Chairperson of the Computer Science Department. He has ten (10) years of teaching experience. He graduated with the degree of Bachelor of Science in Information Technology from the Pamantasan ng Lungsod ng Maynila. He also obtained his Master of Science in Information and Communications Technology degree from the same university. He finished his doctorate in Information Technology from the Technological Institute of the Philippines-Quezon City Campus. He is a member of the Philippine Society of Information Technology Educators (PSITE-NCR) and the Computing Society of the Philippines. He is also an author of various books and has already published his research in the field of Information Technology, both locally and internationally.

Raymund M. Dioses is currently Assistant Professor I at Pamantasan Ng Lungsod ng Maynila. He is from the Department of Education Senior High School Department before he entered Pamantasan ng Lungsod ng Maynila he is currently the chairman of the Computer Science Department under the College of Information Systems and Technology Management. His teaching abilities were greatly enhanced by working experience at CORE Gateway College Inc. (CGCI) where he served as one of the College Faculty and Chairperson of the Computer Education Department for eight (8) years and five (5) years in Senior High School as Teacher II at Department of Education. He graduated with the degree of Bachelor of Science in Computer Science at St. Jude College. He finished his master's degree program in Master of Arts in Education majoring in Educational Management at CORE Gateway College, San Jose City Nueva Ecija. He is studying another master's degree program in Master of Information Technology major in Computer Education, ongoing thesis at Nueva Ecija University of Science and Technology, Cabanatuan City, Nueva Ecija.

Jonathan C. Morano is currently lecturer I at Pamantasan ng Lungsod ng Maynila. He has more than 20 years of working and teaching experience in the field of Information Technology. His expertise inspires the next generation of students to get into the field of computer science. Mr. Morano graduated with the degree of Bachelor of Science in Computer Science from the Technological University of the Philippines. He obtained his Master of Arts in Teaching Major in Information Technology from Central College of the Philippines. As well as his Master of Science in Information Technology from La Consolacion University Philippines. He is also an author of various published research in the field of Information Technology, published both locally and internationally.