IT Independent Journal
Vol. 13 No. 4, April (2025), pp. 399-407

ISSN 2301-8984 (Print), 2809-1884 (Online)
Published by Institute of Computer Science

# Facial image protection with visual cryptography and random least significant bit (LSB) steganography

**Panser Karo Karo[1], Simon Simarmata[2], Novianti Madhona Faizah[3], Luky Fabrianto[4]**
[1,3]Computer Science Department, Universitas Tama Jagakarsa, Indonesia
[2]Information Technology Department, Universitas Pamulang, Indonesia
[4]Digital Business Department, Universitas Nusa Mandiri, Indonesia

**A R T I C L E I N F O**

***Article history:***

Received Apr 9, 2025
Revised Apr 15, 2025
Accepted Apr 30, 2025

***Keywords:***

Cryptography;
Photographs;
PSNR;
Random LSB;
Steganography.

**ABSTRACT**

The confidentiality of sensitive data—such as personal information of individuals who may pose security threats to client assets—must be strictly maintained. This data includes personal details such as name, ID number, address, date of birth, occupation, and photographs (images). The data protection process involves combining textual data (ID number, name, date of birth) with a photo into a single image, which is then processed using visual cryptography. The visual cryptography technique applied is the (*k, n*) scheme with a *2-out-of-k* configuration. To enhance data security and confidentiality through dual-layer protection, the output from the visual cryptography process is further secured using steganography with the random LSB (Least Significant Bit) method, applied to one of the shares obtained from the previous step. The best result achieved during testing was a PSNR of 71.9977 and an MSE of 0.0041. It is expected that the combination of visual cryptography and steganography methods will significantly enhance the security of data storage to protecting it from unauthorized access.



***Corresponding Author:***

Luky Fabrianto,
Digital Business Department,
Universitas Nusa Mandiri,
Jl. Margonda No.545, RT.1/RW.7, Pondok Cina, Kecamatan Beji, Kota Depok, Jawa Barat 16424, Indonesia
luky.lfb@nusamandiri.ac.id

## 1. INTRODUCTION

In the rapid development of information technology, the internet now connects almost every computer around the world, allowing the exchange of data in the form of text, images, video, and audio (Dutta & Zisserman, 2019). As a result, protecting sensitive information has become increasingly important. One way to ensure data confidentiality is through information hiding and cryptography (Sharma et al., 2019).

A company specializing in security and safety services, often receives critical data from stakeholders—such as personal information about individuals who may pose security threats to their clients. To safeguard this information, a prototype application has been developed to encrypt images using visual cryptography. For added security, the encrypted image is then hidden inside another image using steganography with a random LSB (Least Significant Bit) method (Ehsan Ali et al., 2021). This combination of visual cryptography and steganography is expected to enhance data protection, ensuring that sensitive documents can only be accessed by authorized parties. Steganography has been used even before the digital era. One famous example happened during World War II, when a satellite image of a Soviet bomber base was secretly hidden inside a painting called The Renoir (Şahin et al., 2021).

Visual Cryptography Secret Sharing (VCSS) and Enhanced LSB steganography to protect grayscale images, the results effective in hiding secret information by high PSNR and low MSE values (Al Ghifary Sujono et al., 2024). Visual cryptography scheme using a random grid method

and adds a master share to improve security, this approach is more secure than traditional VCSS and provides good visual quality in the reconstructed image (Francis & Monoth, 2023). A three-layer security system combining AES encryption, visual cryptography, and LSB steganography, results show that this system effectively protects sensitive data while maintaining high image quality and a high success rate in message extraction (Bhawna & Malik, 2023). A web-based system for hiding data using a hybrid approach that combines LSB steganography and visual cryptography, the system proved to be efficient, easy to use online, and effective in keeping data secure with good visual quality and easy reconstruction (Ediriweera et al., 2023). Steganography method called CRoSS, based on diffusion models, to improve security, robustness, and control over hidden messages, experiments show that CRoSS produces high-quality images that are hard to distinguish from regular ones, making it highly resistant to detection and visual forensic attacks (Yu et al., 2023).

The scope of this study is defined as follows. First, the main focus is on designing a visual cryptography construction that allows each participant to possess their own secret image share, which can be reconstructed, along with the integration of steganography techniques (Pandey et al., 2022) to enhance data security. Second, the image files used as the data carrier are in JPG and PNG formats. Third, the output generated from the encryption and data embedding process will also be in JPG or PNG format. Lastly, the prototype development and implementation are carried out using the MATLAB R2022b programming environment.

## 2. RESEARCH METHOD

Steganography is the science and art of secret communication by hiding messages within seemingly harmless objects (Mahdi et al., 2019). The existence of the steganographic message itself is concealed. The term comes from the Greek words Steganos, meaning “covered,” and Graphia, meaning “writing” (Hasugian & Simangunsong, 2020). A popular description of steganography is "hidden in plain sight," referring to information concealed right before our eyes. In contrast, cryptography transforms messages into unreadable, random-looking data, where the presence of the message is usually known. Steganography mainly requires two criteria: fidelity and recovery (Eze et al., 2019).

To meet the criteria mentioned above, several key components must be considered in the implementation of steganography. First is the cover-image, which refers to the image used as a medium to hide information, making it undetectable to unauthorized parties. Second is the embedded-image, which is the actual data or image that will be concealed within the cover-image. The result of embedding the hidden message into the cover-image is called the stego-image. A stego-key is also essential; it serves as a secret key used both to embed the information and to retrieve it. Lastly, steganalysis is the science and art of detecting hidden messages within media that have undergone steganographic processing. Those who specialize in steganalysis are known as steganalysts.

This method is not significantly different from the classical LSB technique; however, the key distinction lies in its use of randomly selected pixel areas for message embedding (Sansone, 2022). This is further illustrated in Figure1.

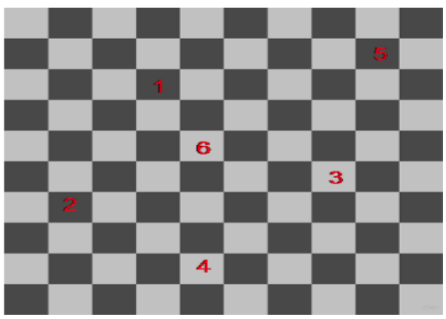


Figure 1. Pixel selection in Pseudo-Random LSB

In the figure 1, it can be seen that with Pseudo Random LSB, data is embedded into the least significant bits of randomly chosen pixels. This approach makes the hidden message more difficult to detect.

Performance measurement of the compression algorithm is needed to measure the distortion that occurs between the original image and the image containing the message (Mahdi et al., 2019)(Sara et al., 2019). There are two calculations that can be done to measure the distortion, namely Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) (Al Najjar, 2024). Mean Squared Error (MSE) is the cumulative root of the error value between the image containing the message and the original image. The MSE equation is given as follows:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||I(i,j) - K((i,j)||^2$$

Where :
*m* and *n* = Dimensions of the image
*I(i,j)* = Pixels of the original image
*K(i,j)* = Pixels of an image containing a message

The values of PSNR and MSE are always inversely related. The Peak Signal-to-Noise Ratio (PSNR) is closely associated with the Mean Squared Error (MSE). As the MSE value decreases, the error becomes smaller, which in turn increases the PSNR value. A higher PSNR indicates better quality, as it reflects a higher signal-to-noise ratio. PSNR is a measure of image similarity by evaluating the pixel differences between the original image and the image containing the hidden message (Biswal et al., 2024). PSNR is expressed in decibels (dB). The PSNR formula is defined as follows:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20.\log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)$$

Where :
$MAX_1$ = The maximum pixel value of the original image (for 8 bit images the $MAX_1$ value is 255)

For RGB images, the MSE value is calculated by summing the MSE values of the Red, Green, and Blue channels, then dividing the total by three. In general, image processing results are considered acceptable to the human eye if the PSNR value is greater than 30 dB (Ryden et al., 2021). The higher the PSNR value, the better the quality of the resulting image.

Visual cryptography is an extension of secret sharing schemes where the data can be visually represented, such as in the form of text or images (Kumar et al., 2022). The secret information is encrypted using a specific method and then divided into several shares, which are printed onto transparent sheets (Vanitha & Mangayarkarasi, 2020). To decrypt the information, one simply needs to stack the required number of shares until the hidden image becomes visible.

For better illustrate the idea of visual cryptography, the construction and reconstruction processes are explained as follows. Suppose there is a secret image R that needs to be divided into two shares. The construction process is illustrated in Figure 2, where the secret image R is split into Share 1 and Share 2. In the reconstruction process, stacking both shares will reveal the secret image R (Georgi et al., 2021). Terms frequently used in visual cryptography include: pixel, boolean OR, pixel expansion, hamming weight and contrast.

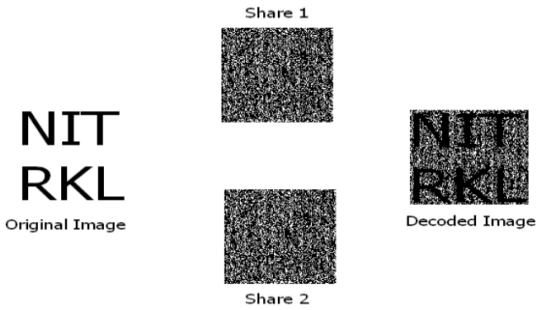


Figure 2. Visual cryptography construction process (Jena & Jena, 2009)

A pixel is the smallest element of a digital image and is defined by a coordinate axis *(x, y)* (Hu et al., 2007), where the x-axis is aligned with the rows and the y-axis with the columns, as illustrated in Figure 3. Each pixel has a value ***f****(x, y)* that represents the color intensity at that specific point. Every digital image can be represented in raster form (Elmurod et al., 2021), where its elements consist of individual pixels.

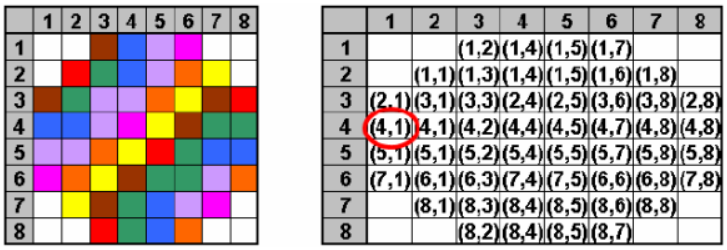


Figure 3. Pixel Ilustration (Hu et al., 2007)

In visual cryptography, an image will be represented as a Boolean matrix, where entry 1 represents the color black, and entry 0 represents the color white (Aszalós, 2021). Figure 4 shows the image representation of a Boolean matrix.

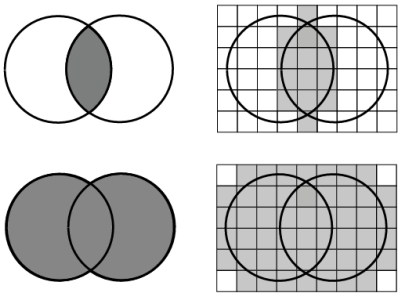

Figure 4. Boolean AND/OR Ilustration (Aszalós, 2021)

The physical model of visual cryptography uses images printed on transparencies. Therefore, the Boolean OR operation occurs when two transparencies are stacked (Wu & Yao, 2023). When stacking two transparencies, the result will appear black if either or both of the transparencies have black pixels.

The research method used in this thesis is an experimental research method. Experimental research involves the direct collection of data by the researcher. The purpose of the experiment in this study is to develop a document security application that secures facial image data using visual cryptography and steganography with the random LSB method. The research data consists of facial images and profile information, which will be implemented using visual cryptography and steganography with the random LSB method.

The analysis of system requirements involves detailing all the components needed for system development and creating a project plan related to the system. In this study, the functional requirements of the system or software being developed are as follows: the system must be capable of securing data, encrypting plaintext, and decrypting the plaintext back to its original form.

The image below illustrates the workflow design and research framework for the system development process. This section presents the reconstruction process of the algorithm that integrates visual cryptography with steganography. The goal is to securely embed sensitive visual information by encrypting it into multiple visual shares and then concealing the result using the random LSB steganography technique. This combined approach enhances both confidentiality and data hiding, making it more resistant to unauthorized access or detection, as present in Figure 5.

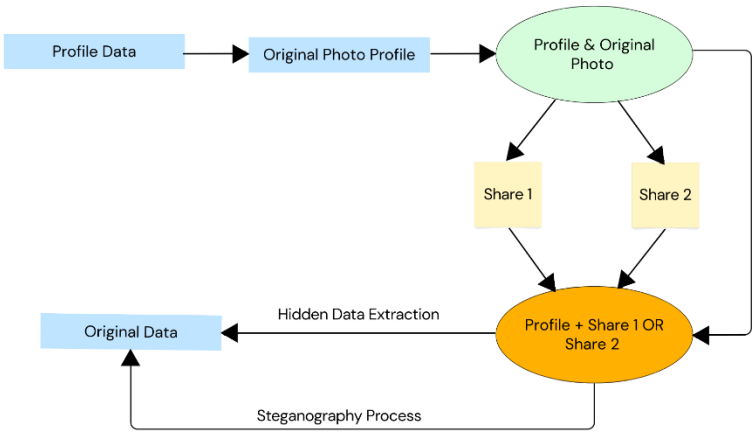


Figure 5. Reconstruction of the Algorithm for Combining Visual Cryptography and Steganography

System testing is conducted to ensure that the developed system aligns with the results of the analysis and design, and to draw conclusions on whether the system meets the expected outcomes. The aspects to be analyzed and evaluated include quality analysis and security analysis. Quality analysis involves comparing the cover image and the stego image by calculating the PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Square Error) (Sara et al., 2019). These values are useful for determining the similarity of pixel values between the stego image and the original cover image. Security analysis is performed to assess the system's resistance to visual detection attacks. It examines whether there are noticeable differences in the image before and after embedding the secret message, and whether the message remains intact and unchanged after the cryptographic process.

## 3. RESULTS AND DISCUSSIONS

In this study, 10 sample images were used are images dataset obtained from the internet which is not licensed for use. Figure 6 shows some sample examples.

Figure 6. Image samples

The results of measuring the dimensions and size of the image data samples can be presented in the Table 1 and the first stage encryption test using visual cryptography k out of 2, produces the same dimensions as the original profile photo.

Table 1. Steganography measurement share 1

| Item | Dimension | Original Size (KB) |
|---|---|---|
| Fotoprofil-01 | 300x252 | 12 |
| Fotoprofil-02 | 322x157 | 8 |
| Fotoprofil-03 | 277x182 | 5 |
| Fotoprofil-04 | 184x208 | 6 |
| Fotoprofil-05 | 225x225 | 8 |
| Fotoprofil-06 | 247x204 | 7 |
| Fotoprofil-07 | 285x177 | 7 |
| Fotoprofil-08 | 300x168 | 5 |
| Fotoprofil-09 | 300x168 | 5 |
| Fotoprofil-10 | 250x201 | 7 |

While the file size of both share 1 and share 2 becomes larger as seen in Table 2.

Table 2. Dimensions and sizes of share 1 and share 2 files

| Item | Dimension | Size Share 1 (KB) | Size Share 2(KB) |
|---|---|---|---|
| Fotoprofil-01 | 300x252 | 53 | 53 |
| Fotoprofil-02 | 322x157 | 33 | 34 |
| Fotoprofil-03 | 277x182 | 34 | 33 |
| Fotoprofil-04 | 184x208 | 26 | 26 |
| Fotoprofil-05 | 225x225 | 34 | 34 |
| Fotoprofil-06 | 247x204 | 34 | 34 |
| Fotoprofil-07 | 285x177 | 34 | 33 |
| Fotoprofil-08 | 300x168 | 33 | 34 |
| Fotoprofil-09 | 300x168 | 33 | 34 |
| Fotoprofil-10 | 250x201 | 34 | 34 |

Share 1 and share 2 are stacked again, the result will also provide the same dimensions as the original profile photo with a file size that is smaller than the file size of share 1 and share 2 as in Table 3.

Table 3. Cryptographic visual encryption test results

| Item | Dimension | Size Result (KB) |
|---|---|---|
| Fotoprofil-01 | 300x252 | 32 |
| Fotoprofil-02 | 322x157 | 21 |
| Fotoprofil-03 | 277x182 | 21 |
| Fotoprofil-04 | 184x208 | 16 |
| Fotoprofil-05 | 225x225 | 21 |
| Fotoprofil-06 | 247x204 | 20 |
| Fotoprofil-07 | 285x177 | 21 |
| Fotoprofil-08 | 300x168 | 20 |
| Fotoprofil-09 | 300x168 | 21 |
| Fotoprofil-10 | 250x201 | 21 |

The second stage of the encryption testing involved the use of steganography with the random LSB method, where Share 1 obtained from the visual cryptography process was used to store profile information. Based on the results, the steganography process produced images with the same dimensions as Share 1, and the file sizes remained approximately the same.

Table 4. Share 1 steganography encryption test results

| Item | Dimension | Size Result (KB) |
|---|---|---|
| Fotoprofil-01 | 300x252 | 51 |
| Fotoprofil-02 | 322x157 | 33 |
| Fotoprofil-03 | 277x182 | 34 |
| Fotoprofil-04 | 184x208 | 26 |
| Fotoprofil-05 | 225x225 | 35 |
| Fotoprofil-06 | 247x204 | 34 |
| Fotoprofil-07 | 285x177 | 34 |
| Fotoprofil-08 | 300x168 | 34 |
| Fotoprofil-09 | 300x168 | 34 |
| Fotoprofil-10 | 250x201 | 34 |

The PSNR value after the message was embedded is higher than the PSNR value before the message was embedded. This indicates that the difference between the stego image and the cover image is minimal, thus achieving the main objective of securing the document as seen as Tabel 5.

Table 5. PSNR and MSE test results for share 1 with share 1 that has been steganographed

| Item | Dimension | PSNR | MSE |
|---|---|---|---|
| Fotoprofil-01 | 300x252 | 71.9977 | 0.0041 |
| Fotoprofil-02 | 322x157 | 70.3301 | 0.006 |
| Fotoprofil-03 | 277x182 | 70.3038 | 0.0061 |
| Fotoprofil-04 | 184x208 | 69.0741 | 0.008 |
| Fotoprofil-05 | 225x225 | 70.3936 | 0.0059 |
| Fotoprofil-06 | 247x204 | 70.3829 | 0.006 |
| Fotoprofil-07 | 285x177 | 70.2923 | 0.0061 |
| Fotoprofil-08 | 300x168 | 70.4178 | 0.0059 |
| Fotoprofil-09 | 300x168 | 70.2696 | 0.0061 |

| | | | |
|---|---|---|---|
| Fotoprofil-10 | 250x201 | 70.2332 | 0.0062 |

Share 1 and 2 steganography results and stacked the results also produce the same dimensions as the original profile photo with a smaller file size, presented in the Table 6.

Table 6. Results of share 1 and share 2 stacking tests

| Item | Dimension | Size Result (KB) | Size Result (KB) – share 1 steganographed |
|---|---|---|---|
| Fotoprofil-01 | 300x252 | 32 | 32 |
| Fotoprofil-02 | 322x157 | 21 | 21 |
| Fotoprofil-03 | 277x182 | 21 | 21 |
| Fotoprofil-04 | 184x208 | 16 | 16 |
| Fotoprofil-05 | 225x225 | 21 | 21 |
| Fotoprofil-06 | 247x204 | 20 | 21 |
| Fotoprofil-07 | 285x177 | 21 | 21 |
| Fotoprofil-08 | 300x168 | 20 | 20 |
| Fotoprofil-09 | 300x168 | 21 | 21 |
| Fotoprofil-10 | 250x201 | 21 | 21 |

The test results showed that hiding profile information was good, but if the profile photos were stacked, they looked less clear, presented in the Table 7. Although there is a decrease in visual quality, this can be considered normal in data security systems such as visual cryptography and steganography, because the main goal is security, not perfect visual quality.

Table 7. The results of the PSNR and MSE tests that have been steganographed with profile photos

| Item | Dimensi | PSNR | MSE |
|---|---|---|---|
| Fotoprofil-01 | 300x252 | 29.5424 | 72.25 |
| Fotoprofil-02 | 322x157 | 26.0109 | 162.9248 |
| Fotoprofil-03 | 277x182 | 27.3563 | 119.5233 |
| Fotoprofil-04 | 184x208 | 28.3212 | 95.7116 |
| Fotoprofil-05 | 225x225 | 29.4596 | 73.6415 |
| Fotoprofil-06 | 247x204 | 28.1772 | 98.9372 |
| Fotoprofil-07 | 285x177 | 27.4858 | 116.0125 |
| Fotoprofil-08 | 300x168 | 30.0057 | 64.939 |
| Fotoprofil-09 | 300x168 | 26.5972 | 142.3497 |
| Fotoprofil-10 | 250x201 | 26.9538 | 131.1284 |

Furthermore, the embedding process using the Random LSB method proved highly effective. This is supported by high PSNR values (averaging above 70 dB) and extremely low MSE values (below 0.01), indicating a high similarity between the stego-image and the original image, as illustrated in Figure 7. The extraction of the hidden data was successful. However, when share 1 and share 2 were stacked for reconstruction, a noticeable decrease in PSNR and an increase in MSE were observed, indicating a reduction in image quality. Nevertheless, the hidden message remained identifiable, suggesting that the system achieved its primary goal of secure data concealment.

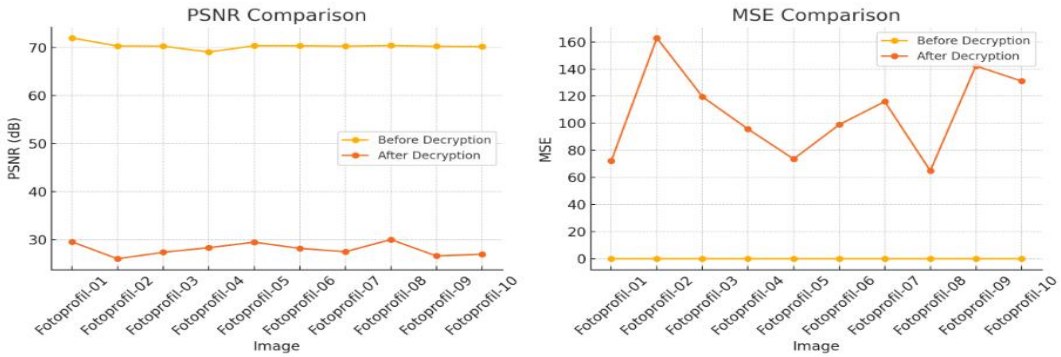


Figure 7. PSNR and MSE Comparasion

Based on the results of experiments and analysis, it can be concluded that the integration of visual cryptography and steganography using the Random LSB method has been successfully

implemented to enhance image data security. The encryption process preserved the image dimensions compared to the original profile image, although file sizes increased. In contrast, the decryption process resulted in smaller file sizes than both share 1 and share 2, while maintaining original image dimensions, as illustrated in figure 8.

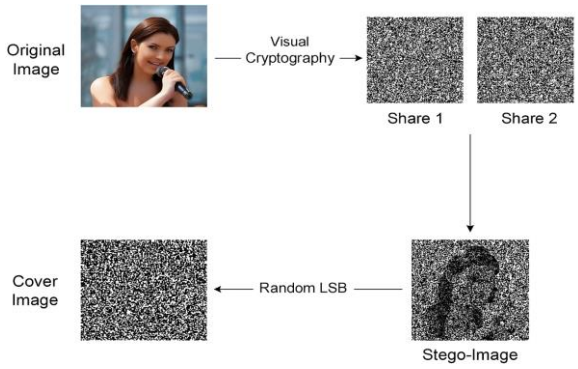


Figure 8. Visual simulation results

## 4. CONCLUSION

Based on the prototype testing results, the integration of visual cryptography and steganography using the random LSB method has proven effective in securing image-based documents, particularly facial photos and personal data. The main findings indicate that the combination of these two techniques provides strong data protection while maintaining high image quality, as evidenced by high PSNR values and low MSE. Furthermore, the system successfully hides and extracts sensitive information with minimal visual distortion, confirming its reliability in document security applications.

The approach was tested on a small dataset of only 10 facial image samples, which may not fully represent broader variations in real-world scenarios. For future research, it is recommended to explore more advanced visual cryptography schemes—such as those with random grids or additional security layers—to enhance the clarity and robustness of image reconstruction. Moreover, applying the steganography process before visual cryptography could be investigated as an alternative sequence to further strengthen data confidentiality and resistance to detection or tampering.

## REFERENCES

Al Ghifary Sujono, S., Marwati, R., Kustiawan Program Studi Matematika, C., & Pendidikan dan Ilmu Pengetahuan Alam, F. (2024). Pengamanan Citra Grayscale menggunakan Penggabungan Kriptografi Visual Secret Sharing dan Steganografi Enhanced Least Significant Bit. *Jurnal EurekaMatika*, *12*(2), 67–78. https://doi.org/10.17509/JEM.V12I2.72580

Al Najjar, Y. (2024). Comparative Analysis of Image Quality Assessment Metrics: MSE, PSNR, SSIM and FSIM. *International Journal of Science and Research (IJSR)*, *13*(3), 110–114. https://doi.org/10.21275/sr24302013533

Aszalós, L. (2021). Decompose boolean matrices with correlation clustering. *Entropy*, *23*(7), 1–12. https://doi.org/10.3390/e23070852

Bhawna, B., & Malik, S. K. (2023). Triple Layered Security for Data Hiding Using Steganography and Visual Cryptography. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(10s), 335–345. https://doi.org/10.17762/IJRITCC.V11I10S.7634

Biswal, M., Shao, T., Rose, K., Yin, P., & Mccarthy, S. (2024). *StegaNeRV: Video Steganography using Implicit Neural Representation* (pp. 888–898).

Dutta, A., & Zisserman, A. (2019). The VIA annotation software for images, audio and video. *MM 2019 - Proceedings of the 27th ACM International Conference on Multimedia*, 2276–2279. https://doi.org/10.1145/3343031.3350535

Ediriweera, S., Dilhara, B., & Disanayake, C. (2023). Web-Based Data Hiding: A Hybrid Approach Using Steganography and Visual Cryptography. *Proceedings - International Research Conference on Smart Computing and Systems Engineering, SCSE 2023*, *6*(October 2024), 1–7. https://doi.org/10.1109/SCSE59836.2023.10214994

Ehsan Ali, U. A. M., Ali, E., Sohrawordi, M., & Sultan, M. N. (2021). A LSB Based Image Steganography Using Random Pixel and Bit Selection for High Payload. *International Journal of Mathematical Sciences and*

*Computing*, *7*(3), 24–31. https://doi.org/10.5815/ijmsc.2021.03.03

Elmurod, A., Ogli, T., Элмурод, А., & Угли, Т. (2021). RASTER AND VECTOR FORMATS OF ELECTRONIC DOCUMENT OF TECHNICAL DOCUMENTATION. *Universum: Технические Науки*, *7-3 (88)*. https://doi.org/10.32743/UniTech.2021.78.8-3.12088

Eze, P., Parampalli, U., Evans, R., & Liu, D. (2019). Integrity verification in medical image retrieval systems using spread spectrum steganography. *ICMR 2019 - Proceedings of the 2019 ACM International Conference on Multimedia Retrieval*, *29*, 53–57. https://doi.org/10.1145/3323873.3325020

Francis, N., & Monoth, T. (2023). Security enhanced random grid visual cryptography scheme using master share and embedding method. *International Journal of Information Technology (Singapore)*, *15*(7), 3949–3955. https://doi.org/10.1007/S41870-023-01381-W/METRICS

Georgi, P., Wei, Q., Sain, B., Schlickriede, C., Wang, Y., Huang, L., & Zentgraf, T. (2021). Optical secret sharing with cascaded metasurface holography. *Science Advances*, *7*(16), 9718–9732. https://doi.org/10.1126/SCIADV.ABF9718/SUPPL_FILE/ABF9718_SM.PDF

Hasugian, P. S. H., & Simangunsong, A. (2020). Implementation Of Least Significant Bit (LSB) Algorithm For Data Security In Digital Imagery. *Jurnal Info Sains : Informatika Dan Sains*, *10*(2), 6–12. https://doi.org/10.54209/INFOSAINS.V10I2.31

Hu, O. R. T., Zuffo, M. K., Kurashima, C. S., & Lopes, R. de D. (2007). Panoramic Images Composition with Positioning Maps for Virtual Telepresence. *2007 IX Symposium on Virtual and Augmented Reality*, *March 2014*.

Jena, D., & Jena, S. K. (2009). A novel visual cryptography scheme. *Proceedings - International Conference on Advanced Computer Control, ICACC 2009*, *January 2009*, 207–211. https://doi.org/10.1109/ICACC.2009.109

Kumar, M., Aggarwal, J., Rani, A., Stephan, T., Shankar, A., & Mirjalili, S. (2022). Secure video communication using firefly optimization and visual cryptography. *Artificial Intelligence Review*, *55*(4), 2997–3017.

Mahdi, M. H., Abdulrazzaq, A. A., Mohd Rahim, M. S., Taha, M. S., Khalid, H. N., & Lafta, S. A. (2019). Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. *IOP Conference Series: Materials Science and Engineering*, *518*(5). https://doi.org/10.1088/1757-899X/518/5/052002

Pandey, B. K., Pandey, D., Wairya, S., Agarwal, G., Dadeech, P., Dogiwal, S. R., & Pramanik, S. (2022). Application of Integrated Steganography and Image Compressing Techniques for Confidential Information Transmission. *Cyber Security and Network Security*, 169–191. https://doi.org/10.1002/9781119812555.CH8

Ryden, T., Van Essen, M., Marin, I., Svensson, J., & Bernhardt, P. (2021). Deep-Learning Generation of Synthetic Intermediate Projections Improves 177Lu SPECT Images Reconstructed with Sparsely Acquired Projections. *Journal of Nuclear Medicine*, *62*(4), 528–535. https://doi.org/10.2967/JNUMED.120.245548

Şahin, F., Çevik, T., & Takaoğlu, M. (2021). Review of the Literature on the Steganography Concept. *International Journal of Computer Applications*, *183*(2), 38–46. https://doi.org/10.5120/ijca2021921298

Sansone, E. (2022). LSB: Local Self-Balancing MCMC in Discrete Spaces. *Proceedings of Machine Learning Research*, *162*, 19205–19220.

Sara, U., Akter, M., Uddin, M. S., Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *7*(3), 8–18. https://doi.org/10.4236/JCC.2019.73002

Sharma, K., Aggarwal, A., Singhania, T., Gupta, D., & Khanna, A. (2019). Hiding Data in Images Using Cryptography and Deep Neural Network. *Journal of Artificial Intelligence and Systems*, *1*(1), 143–162. https://doi.org/10.33969/AIS.2019.11009

Vanitha, M., & Mangayarkarasi, R. (2020). Comparative Study of Different Cryptographic Algorithms. *Journal of Information Security*, *11*(3), 138–148. https://doi.org/10.4236/JIS.2020.113009

Wu, X., & Yao, P. (2023). Boolean-based Two-in-One Secret Image Sharing by Adaptive Pixel Grouping. *ACM Transactions on Multimedia Computing, Communications and Applications*, *19*(1). https://doi.org/10.1145/3517140/ASSET/CCD9168E-86EC-4FB3-B4D8-AF7DD618E7E8/ASSETS/GRAPHIC/TOMM-2021-0149-F10.JPG

Yu, J., Zhang, X., Xu, Y., & Zhang, J. (2023). CRoSS: Diffusion Model Makes Controllable, Robust and Secure Image Steganography. *Advances in Neural Information Processing Systems*, *36*. https://arxiv.org/abs/2305.16936v1