Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Cryptography Application on RGB Overlapping Block Based PVD Using AES

Andi Marwan Elhanafi[1)*], Tommy[2)], Rosyidah Siregar[3)], Manovri Yeni[4)], Shahira An-Nissa[5)]
[1,2,3,5)] Universitas Harapan Medan, Indonesia [4)] Universitas Muhammadiyah Aceh, Indonesia
[1)]andimarwanelhanafi@gmail.com, [2)]tomshirakawa@gmail.com, [3)]rosyidah_siregar.unhar@harapan.ac.id,
[4)]manovri.yeni@unmuha.ac.id, [5)]shahira.nissa@gmail.com,

Submitted : Aug 16, 2022 | **Accepted** : Aug 17, 2022 | **Published** : Aug 19, 2022

Abstract: Pixel Value Differencing is a data hiding method in digital images that uses the difference in pixel values as a reference for inserting secret data bits. RGB Overlapping Block Based PVD is an optimization of PVD steganography. RGB Overlapping Block Based PVD provides much larger capacity with acceptable quality. In this study, the AES cryptography application is used as an additional layer on RGB Overlapping Block Based PVD to provide additional security. Testing and observations have been carried out on the capacity and quality aspects of the embedding results using additional AES encryption. on the capacity used during the embedding process, Embedded pixels and bits per pixel between using AES and without using AES did not change significantly where the addition was caused by the padding process of the input block. In terms of quality observation, AES application causes a decrease in quality but is not significantly different from that without using AES, where the quality degradation that occurs based on the difference in the average RMSE value is only 0.052 and 0.492 for PSNR. Based on the results, AES cryptography applications can be implemented properly where there is no significant change in terms of capacity and quality to the default RGB Overlapping Block Based PVD.

Keywords: Steganography; PVD; Overlapping; Block Based; AES;

INTRODUCTION

Information security is a very important aspect in today's digital era. The information contained in the data can be found in the form of text, digital images, video, audio and other digital forms. The security of information contained in digital data in general can be done in two ways, namely by encoding it into other forms using cryptographic methods and by hiding it in other media which is often known as steganography. The development of research that has been carried out on these two topics has resulted in many alternatives that can be applied in information security. Cryptography and steganography have the same purpose but have some differences in the output data. Cryptography encodes data so that the output data will have a different form where the output text data produced will become unreadable but can be seen by other parties. Steganography on the other hand, secures data by hiding it on other media so that the data will not be seen but only the container media as the output (Subramanian, Elharrouss, Al-Maadeed, & Bouridane, 2021). However, the two approaches can be combined to increase layers of security.

Digital image is a medium that is widely used in steganography applications. In addition to digital images, there are other media that can be used in steganography applications such as text, video and audio. In steganography using digital image media there are several approaches that can be used in the message hiding process such as least significant bit substitution (LSB) (Bender, Gruhl, Morimoto, & Lu, 1996) (Reddy, Subramanyam, & Reddy, 2011), most significant bit substitution (MSB) (Ali, Ali, & Qudr, 2019) (Garg & Scholar, 2012), hybrid (LSB and MSB)) (Wai & Myat, 2018), pixel value decomposition (Alade, Amusan, Adedeji, & Alo, 2021) (Sahu & Swain, A review on LSB substitution and PVD based image steganography techniques, 2016), and several other approaches. Pixel value decomposition is one approach to digital image steganography that is quite good which can provide a balance between the quality produced and the capacity that can be used in the container image. Improvised pixel value decomposition has been carried out in several studies such as pixel overlapping (Sahu & Swain, Pixel overlapping image steganography using PVD and modulus function, 2018), multi-directional PVD (Sahu, Padhy, & Gantayat, 2021), adjacent PVD (Kalita, Tuithung, & Majumder, 2019), and so on. Prasat and Pal in their research propose an improvisation of digital image steganography using a pixel overlapping block-based approach that can be applied to color images using RGB

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

value components (Prasad & Pal, 2017). Block-based overlapping pixels are able to provide greater storage capacity on the container media with good quality. Block-based overlapping pixels are focused on capacity and quality, thus requiring additional steps so that hidden data cannot be read directly after the extraction process. Therefore we need a combination of block-based PVD overlapping pixel steganography with cryptographic methods to add a layer of security to the hidden data.

The combination of cryptography and digital image steganography aims to increase the security of hidden data. By using cryptography, hidden data cannot be directly read by parties who do not have the key needed for the decryption process. The application of cryptography as an additional layer in digital image steganography has been widely applied in several studies (Biswas, Gupta, & Haque, 2019) (Vinothkanna, 2019). Several cryptographic algorithms can be used in digital image steganography such as ECC (Duan, et al., 2020), RSA (Wahab, Khalaf, Hussein, & Hamed, 2021) (Al-Juaid, Gutub, & Khan, 2018) and AES (Alexan, Hamza, & Medhat, 2019) (Yasser, Hesham, Hassan, & Alexan, 2020). To add a layer of security to digital image steganography on pixel overlapping block-based PVD, this research will use the AES cryptography method for the text to be inserted into the container image. Measurements were then made on time, capacity consumption and quality obtained on the container image resulting from the combination process of AES and pixel overlapping block-based PVD to obtain a performance measure of the combination carried out in this research.

LITERATURE REVIEW

Pixel Value Differencing

Pixel value differencing is a steganography that uses the difference value between two adjacent pixels as the basis for determining the number of message bits that can be inserted in the pixel. So that the greater the difference in value between two adjacent pixels, the greater the number of message bits that can be inserted in these pixels which results in an increase in the capacity of the container image. This method was originally proposed by Wu and Tsai (Wu & Tsai, 2003) which was applied to grayscale images. Along with the development of research, this method has been improvised so that it can be applied to color images. In simple terms, the stages of PVD can be described as follows:

1. Transform image pixels to 1d array of pixels ($P_1, P_2, P_3, \dots, P_n$)
2. Calculate the distance d_i pair of two adjacent pixels (P_i dan P_{i+1}) using equation (1).

$$d_i = |P_i - P_{i+1}| \qquad (1)$$

3. Calculate the number of bits (t) of messages that can be inserted based on the value of the lower and upper limits of the distance d_i obtained using the distance table which can be seen in table 1.

$$t = \lfloor log_2(u_i - l_i + 1) \rfloor \qquad (2)$$

4. Take the t-bits of the sequence of message bits to be inserted.
5. Calculate the new distance value (d_i'):

$$d_i' = l_i + message\ bits\ in\ decimal \qquad (3)$$

6. Calculate the value of the difference (m) between the distance before (d_i) and after insertion (d_i').

$$m = |d_i' - d_i| \qquad (4)$$

7. Calculates the new pixel values for P_i' and P_{i+1}' :

$$(P_i', P_{i+1}') = \begin{cases} \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), if\ P_i \geq P_{i+1}\ and\ d_i' > d_i \\ \left(P_i - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), if\ P_i < P_{i+1}\ and\ d_i' > d_i \\ \left(P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), if\ P_i \geq P_{i+1}\ and\ d_i' \leq d_i \\ \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), if\ P_i < P_{i+1}\ and\ d_i' \leq d_i \end{cases} \qquad (5)$$

In PVD, pixel pairs that have been used in the insertion process cannot be used (overlapping) in the next insertion. So that in the next message bit, P_{i+1} cannot be used for a new pair of pixels, but instead uses the next pair that has not been used in the insertion process.

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 1. Lower and Upper Range

Range	R1	R2	R3	R4	R5	R6
Lower	0	8	16	32	64	128
Upper	7	15	31	63	127	255

To extract the message bits can be done using a simple operation as shown in the following equation.

$$message\ bits\ = l_i - |P'_i - P'_{i+1}| \quad (6)$$

RGB Overlapping Block Based PVD

Overlapping block based PVD uses a pair of RGB color channels on a pixel compared to using a pair of pixels. RGB overlapping block based PVD was proposed by Prasad et al (Prasad & Pal, 2017) which divides the RGB color channel into pairs (R, G) and (G, B) which will produce pairs of insertion results, namely (R_s, G_s) and (G_s, B_s). The insertion process flow of overlapping block based PVD can be seen in Figure 1. PVD is calculated in pairs (R, G) and (G, B) and will produce (R_1, G_1) and (G_1, B_1). G_s is then obtained from the mean G_1 and G_2 while R_s and B_s are obtained from readjust R_1 and B_1 to G_s.

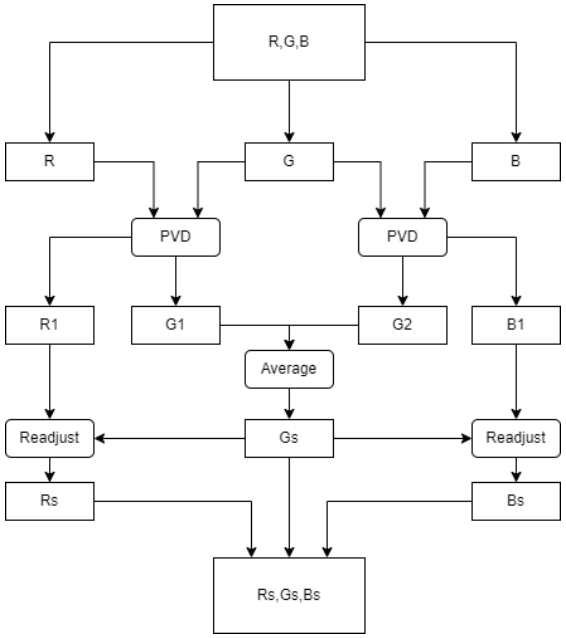

Fig. 1 Embedding process of RGB Overlapping Block Based PVD

The embedding procedure for overlapping block based PVD can be described as follows:

1. Defined the threshold.
2. Take and divide RGB values into two separate pairs (R, G) and (G, B).
3. Compute t1 = |R − G| and t2 = |G – B|
4. If (t1 + t2) < threshold jump to step 8.
5. Apply pixel value differencing (PVD) in both (R,G) and (G,B) pairs to embed the secret message bits.
6. Get intermediate stego color components.
   a. R_1 and G_1 from (R, G) pair
   b. G_2 and B_1 from (G, B) pair
7. Perform readjustment process to form final RGB based on the following sub steps:
   a. Compute $G_s = Round\left(\frac{G_1+G_2}{2}\right)$ (7)
   b. Modify R_1 as final stego red color component
      $R_S = R_1 - \left(G_1 - G_{average}\right)$ (8)
   c. Modify B_1 as final stego green color component
      $B_S = B_1 - (G_2 - G_{average})$ (9)
8. Process rest of the color pixels using step 1 to 7.

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Advanced Encryption Standard

AES is a symmetric cryptography proposed by Joan Daemen and Vincent Rijmen (Daemen & Rijmen, 1999). AES is a block cipher algorithm that can have input and key block lengths of 128, 192 or 256 bits. The input block will be formed into an array that has four rows and several columns which are determined by the length of the input block divided by 32. Each input block will be processed using transformation round. In each round, AES uses a different key or key schedule obtained from the key expansion process.

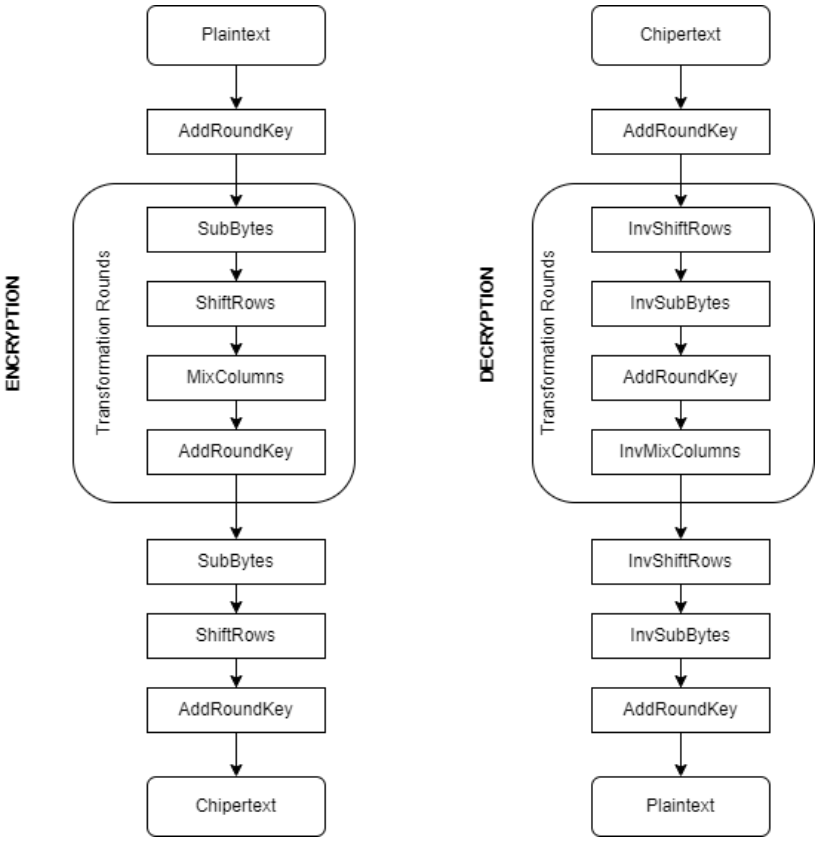

Fig. 2 AES Encryption and Decryption illustration

Broadly speaking, the main operations of AES consist of AddRoundKey, SubBytes, ShiftRows, and MixColumns. While in the decryption process the main process consists of the inverse process of the encryption process, namely AddRoundKey, InverseShiftRows, InverseSubBytes, and InverseMixColumns.

METHOD

Digital image steganography in RGB color space proposed by Prasad and Pal (Prasad & Pal, 2017) is able to provide a balance between capacity and quality compared to ordinary PVD. This study adds a security layer to digital image steganography using overlapping block based PVD in the RGB color space by adding encryption to the data to be inserted.

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

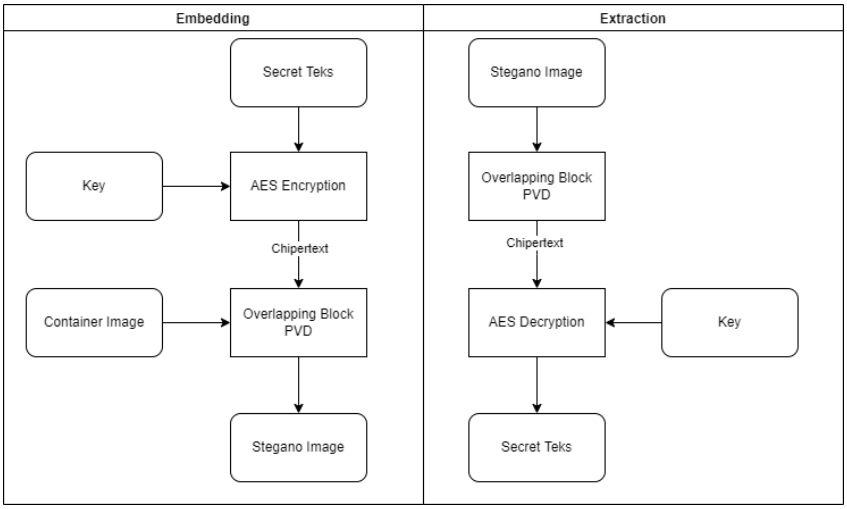

Fig 3. Embedding and Extraction process

The process of hiding information begins by reading the text that will be inserted into the container media. The text will then be encrypted using the AES method. After the encryption process is complete, the ciphertext bits will then be inserted into the container image using overlapping block based PVD.

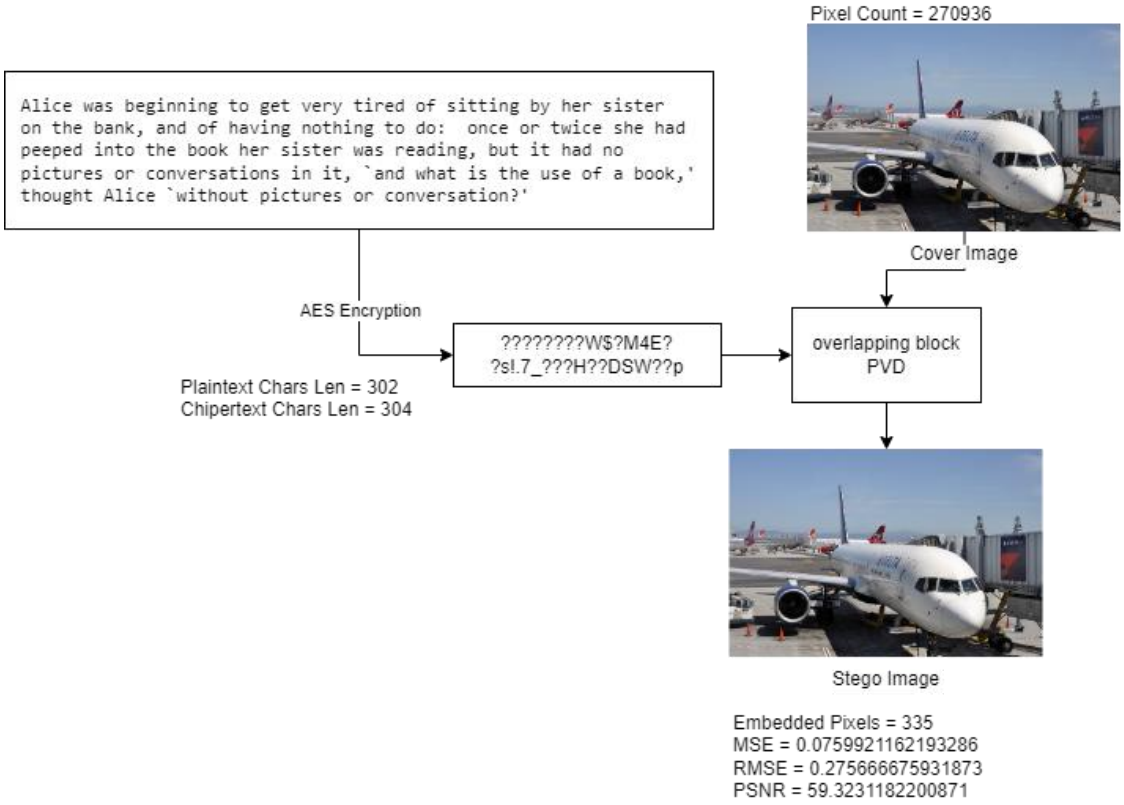

Fig 4. Embedding with AES encryption

The secret message extraction process is the opposite of the embedding process. The ciphertext is first extracted from the stego image which will then be decrypted to obtain the plaintext of the secret message. This study will observe and analyze changes in the number of pixels used as well as changes in the quality of the stego image using MSE, RMSE and PSNR measurements.

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

RESULT

This study uses a digital image dataset obtained from cocodataset.org (COCO, 2022) which consists of 10 images that will be used as cover images. The image dataset can be seen in Figure 5. Each test image will be tested as a cover image using five different texts obtained from the BBC Full Text Document Classification (Kushwaha, 2022).

Testing of each secret message is done by inserting it with an additional encryption process using AES before inserting 10 test images. The encryption key used is the same for each encryption process. The measurement values to be observed are the number of message characters, the number of ciphertext characters, the number of image pixels, the number of pixels used and the resulting image quality (MSE, RMSE and PSNR).

Fig 5. Test Cover Images

Table 2. Cover image spesifications

Cover Image	Resolution	Pixel Count
1	640x427	273280
2	640x427	273280
3	640x427	273280
4	640x398	254720
5	640x426	272640
6	639x428	273492
7	640x427	273280
8	640x480	307200
9	640x428	273920
10	640x427	273280

Each cover image will be named from 1.jpg to 10.jpg, where the order of the names starts from the top left cover image to the bottom right cover image. The test results can be seen in the table 3 as follow :

Table 3. Test Results

Cover Image	Embedded Pixels	MSE	RMSE	PSNR
1	3004	0.73	0.85	49.52
2	3121	0.49	0.69	51.24
3	3095	0.59	0.77	50.35
4	3235	0.42	0.65	51.89
5	2509	2.70	1.64	43.81
6	3015	0.58	0.77	50.45
7	2894	0.81	0.90	49.02
8	2803	1.07	1.03	47.84
9	2753	1.64	1.28	45.97
10	2861	1.31	1.14	46.96

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Based on the value of embedded pixels obtained, we can obtain the percentage of embedded pixels to the total pixels in the cover image and the number of message bits inserted per pixel.

Table 4. Pixels consumption with AES

Cover Image	Pixel Count	Embedded Pixels	% Embedded Pixels
1	273280	3004	1.1
2	273280	3121	1.14
3	273280	3095	1.13
4	254720	3235	1.27
5	272640	2509	0.92
6	273492	3015	1.1
7	273280	2894	1.06
8	307200	2803	0.91
9	273920	2753	1.01
10	273280	2861	1.05
Average			**1.07**

Table 5. Bits Per Pixel with AES

Cover Image	Pixel Count	Embedded Pixels	Bit Per Pixel
1	273280	3004	6.82
2	273280	3121	6.56
3	273280	3095	6.62
4	254720	3235	6.33
5	272640	2509	8.16
6	273492	3015	6.79
7	273280	2894	7.08
8	307200	2803	7.31
9	273920	2753	7.44
10	273280	2861	7.16
Average			**7.03**

DISCUSSIONS

The implementation of the AES cryptography layer on digital image steganography does not have a large negative impact, where the size of the encrypted ciphertext only experiences the addition of a few characters due to the padding process during the formation of the input block in AES. In terms of quality, the results of MSE, RMSE and PSNR are also not so bad where the lowest MSE is 0.42 and the largest is 2.7 while the lowest RMSE is 0.65 and the highest is 1.64. For PSNR itself, it can be seen that the lowest value is 43.81 and the highest is 51.89.

When viewed from the average MSE of 1.034 and RMSE of 0.972, it can be seen, in terms of pixel values, there is a fairly large change in the stegano image. However, this can be offset by a fairly large number of bits per pixel, where in table 5 it can be seen that the average number of bits inserted per pixel is 7.03 bits. After observing the results of the capacity and quality of the implementation of AES cryptography on overlapping block based PVD, then we can then compare these results with the capacity and quality of overlapping block based PVD steganography without using AES.

Table 6. Embedding without AES

Cover Image	Embedded Pixels	MSE	RMSE	PSNR
1	3002	0.59	0.77	50.39
2	3120	0.44	0.66	51.69
3	3092	0.51	0.71	51.07
4	3232	0.39	0.62	52.25
5	2506	2.52	1.59	44.12
6	3013	0.54	0.74	50.78
7	2891	0.76	0.87	49.3

*Andi Marwan Elhanafi

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 3, July 2022
DOI : https://doi.org/10.33395/sinkron.v7i3.11685
e-ISSN : 2541-2019
p-ISSN : 2541-044X

8	2801	0.96	0.98	48.31
9	2751	1.42	1.19	46.59
10	2859	1.16	1.07	47.47

In the results of overlapping block based PVD, it can be seen that the number of embedded pixels only differs between 2-3 pixels due to the additional padding character of the AES process. Meanwhile, in terms of quality, in almost every test, overlapping block based PVD with AES resulted in a higher RMSE than overlapping block based PVD without AES. This can be seen where there is an average difference of 0.052. While the PSNR measurement, the average difference obtained is 0.492. But these differences do not have a significant impact on the visual.

Table 7. Bits per pixel without AES

Cover Image	Pixel Count	Embedded Pixels	Bit Per Pixel
1	273280	3002	6.82
2	273280	3120	6.56
3	273280	3092	6.62
4	254720	3232	6.34
5	272640	2506	8.17
6	273492	3013	6.8
7	273280	2891	7.08
8	307200	2801	7.31
9	273920	2751	7.44
10	273280	2859	7.16
Average			**7.03**

In terms of bit per pixel embedding capability, as shown in table 7, it can be seen that the number of bits inserted in the cover image has no difference with overlapping block based PVD using AES.

CONCLUSION

Based on the development and testing that has been carried out in this study, it can be concluded that the addition of cryptographic methods, especially AES, on overlapping block based PVD digital image steganography does not have a significant impact compared to without using AES. Where the decrease in quality that occurs based on the difference in the average RMSE value is only 0.052 and 0.492 for PSNR. So that AES cryptography applications can be implemented properly without giving a significant decrease in quality. While in terms of capacity and the number of insertion bits per pixel, there is no significant difference between using AES and without using AES. Tests and observations that have been carried out show that the application of AES on overlapping block based PVD digital image steganography can be applied to add a layer of security to overlapping block based PVD steganography.

REFERENCES

Alade, O., Amusan, E., Adedeji, O., & Alo, O. (2021). Image Steganography Using Pixel Value Differencing (PVD) Technique Based on Firefly Algorithm. *Journal of Scientific Research & Reports, 27*(7), 80-86.

Alexan, W., Hamza, A., & Medhat, H. (2019). An aes double–layer based message security scheme. *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, 86-91.

Ali, S., Ali, M., & Qudr, L. (2019). PDA: A private domains approach for improved msb steganography image. *Periodicals of Engineering and Natural Sciences (PEN), 7*(3), 1405-1411.

Al-Juaid, N., Gutub, A., & Khan, E. (2018). Enhancing PC data security via combining RSA cryptography and video based steganography. *Journal of Information Security and Cybercrimes Research, 1*(1), 5-13.

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM systems journal, 35*(3.4), 313-336.

Biswas, C., Gupta, U., & Haque, M. (2019). An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. *2019 international conference on electrical, computer and communication engineering (ECCE)*, 1-5.

*Andi Marwan Elhanafi

COCO. (2022). cocodataset.org. COCO. Retrieved from https://cocodataset.org/#explore

Daemen, J., & Rijmen, V. (1999). *AES proposal: Rijndael.* Retrieved from https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access, 8*, 25777-25788.

Garg, M., & Scholar, M. (2012). Comparison Of Lsb & Msb Based Steganography. *International Journal of Engineering Research & Technology (IJERT), 1*(8), 1-6.

Kalita, M., Tuithung, T., & Majumder, S. (2019). An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. *Cryptologia, 43*(5), 414-437.

Kushwaha, S. (2022). BBC Full Text Document Classification. Kaggle. Retrieved from BBC Full Text Document Classification

Prasad, S., & Pal, A. (2017). An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society open science, 4*(4), 1-14. doi:https://doi.org/10.1098/rsos.161066

Reddy, V., Subramanyam, A., & Reddy, P. (2011). Implementation of LSB steganography and its evaluation for various file formats. *Int. J. Advanced Networking and Applications, 2*(5), 868-872.

Sahu, A., & Swain, G. (2016). A review on LSB substitution and PVD based image steganography techniques. *Indonesian Journal of Electrical Engineering and Computer Science, 2*(3), 712-719.

Sahu, A., & Swain, G. (2018). Pixel overlapping image steganography using PVD and modulus function. *3D Research, 9*(3), 1-14.

Sahu, M., Padhy, N., & Gantayat, S. (2021). Multi-directional PVD steganography avoiding PDH and boundary issue. *Journal of King Saud University-Computer and Information Sciences*. doi:https://doi.org/10.1016/j.jksuci.2021.10.007

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE access, 9*, 23409-23423.

Vinothkanna, M. (2019). A secure steganography creation algorithm for multiple file formats. *Journal of Innovative Image Processing (JIIP), 1*(1), 20-30.

Wahab, O., Khalaf, A., Hussein, A., & Hamed, H. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE Access, 9*, 31805-31815.

Wai, Y., & Myat, E. (2018). Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image. *International Journal of Engineering Trends and Applications, 5*(4), 16-19.

Wu, D., & Tsai, W. (2003). A steganographic method for images by pixel-value differencing. *Pattern recognition letters, 24*(9-10), 1613-1626.

Yasser, S., Hesham, A., Hassan, M., & Alexan, W. (2020). Aes-secured bit-cycling steganography in sliced 3d images. *2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)*, 227-231.

*Andi Marwan Elhanafi