Optimizing data security by using Integration between double stegging by pixel value difference and advanced encryption standard

M S Elden.1*, K Shehata.1, H Badwy.1, A Medny.1
1Computer engineering, Arab Academy for Science, Technology and Maritime Transport (AAST), Cairo, Egypt.

*Corresponding author: m.sala779@gmail.com

Abstract. Advancement of internet technology has led to massive text and multimedia data delivery over the internet, Steganography and cryptography are two prominent methods for secure communication through public network such as the Internet. Steganography predates cryptography somewhat Because of its stealthy features. In this paper, a new method has been proposed which combines cryptography and steganography to make communication even more secure. In this method first the secret data is embedded inside digital image (cov 1) using adaptive pixel value difference (PVD) technique, thereafter advanced encryption standard (AES) algorithm is applied to encrypt the previous digital image. Then encrypted digital image (cov1) will embed inside another digital image (cov2) using the same previous embedding technique. An additional layer of security has been introduced by applying double steganography to ensure the security of sensitive data, also this proposed method aims to keep the value of (PSNR) and (MSE) within accepted range and enhance the amount of secret data to be embedding. Peak signal to noise ratio (PSNR) and mean square error (MSE) are used as a benchmark to measure the performance of the proposed method.

1. Introduction
Nowadays, steganography is the famous technique that use to hide sensitive information, it is the art of conceal secret data into any form of digital media such as images files, audio files, text files and video files, Steganography is split into spatial domains and frequency domains. Spatial domain involves embedding hidden message by explicitly altering the strength of pixels of the cover image while in methods of frequency domains the coefficients of the transformed domain are modified to embed hidden data. Spatial domain methods need less computational complexity and have greater potential for embedding than the frequency domain methods. The main difference between steganography and cryptography is that cryptography aimed to distort the secret data, so it cannot be understood, further Encryption guarantees the message is not leaked even though the message is revealed, thus providing a higher degree of protection, whereas steganography helps to keep the existence of the message as a secret. Even though the message is revealed, thus providing a higher degree of protection, whereas steganography helps to keep the existence of the message as a secret. Steganography consists of three components that can be concluded as secret data that we need to protect it, Cover image referring to the image used as the carrier for embedding messages in and finally stego image that refers to the object used as the carrier to embed messages into. The combination between steganography and cryptography will make the data embedded safer [1]. This combination will meet demands such as
capacity, Security and robustness for secure, open channel data transmission. This paper discuss also the structure of AES as proposed cryptographic symmetric algorithm to integrate with adaptive-PVD in order to ensures that the message does not get disclosed even if the existence of the message is discovered, thus, ensuring higher security level, on other hand adaptive PVD technique was proposed for achieving high embedding capacity[12]

1.1 steganography and Pixel value differencing (PVD)

The Pixel Value Differencing (PVD) [2] system utilizes the difference value in a block between two consecutive pixels to determine how many secret bits should be embedded. The Pixel Value Differencing (PVD) scheme offers elevated imperceptibility to the stego image by choosing two successive pixels and designing a quantization range table to determine the payload by the gap between the successive pixels.

Figure 1. Basic method of steganography[20]

In general, steganography methods of spatial domain image are preferred in utmost implementation due to Their depressed difficulty of computing, wide potential for embedding [3,4], High hiding ability, High imperceptibility of vision and protection versus steganalysis are the key issues in image steganography. Adaptive PVD-based color image exploit the vertical and horizontal edges used in each block during the message embedding process, so it increase the amount of data embedding [5] and keep high imperceptibility. Furthermore in this proposed method we aim to exploit the edge areas to be utilized to hide large number of data compared to smooth areas, because the change in smooth area can be observed easier than in edges.
1.2 Encryption using AES algorithm

AES is a block cipher which is also known as Rijndael Algorithm [23], AES relies on a style principle referred to as a substitution-permutation network, In contrast to its forerunner DES and AES doesn't use a Feistel network. The robust AES development process and its complex internal structures ensures very secure algorithm and has no known weaknesses. It has three category according to the key length used 128, 192 or 256-bits, the both data block and key length are not fixed, They can be set to 128, 192 or 256 bits and The amount of rounds differs as 10, 12, 14 according to key length 128, 192, 256 bits respectively, and its mechanism illustrated below as in Fig 3.

Cryptography is a technique of storing and communicating information in a way that can be read and processed only by those for which it is designed. It is a science of data protection by encoding it in an unreadable form.

Figure 2. Pixel value difference[21]

Subbyte in which we put each byte into a substitution box (S-Box) that maps the byte into a different byte. The result is a four-column output matrix with four rows. Shift rows shift the whole rows to the left in this step. But there is no shift in the first row. Second, third and fourth rows, respectively, are shifted by one byte, two byte and three byte. The rows of the other side are wrapped. Mix columns are the process in which the special mathematical function transforms each column of 4 bytes. The function input is the four bytes of a column and the output is the four new bytes that replace the four bytes input. Add round key is the end step at each round, at which the next round key will be applied with an X-OR at the end of each round. We skip the Mix columns step in the final round.

Figure 3. AES algorithm structure [23]
Decryption process is inverse process to the encryption process to retrieve the encrypted data at the recipient.

2. Previous works
LSB replacement is one of the easiest and most well-known information hiding solutions. RS testing identifies this simplest technique and Tsa [6] highlighted the truth is the edge regions in an image can hide more amount of information than the smooth regions. On the basis of this theory, they suggested steganography (PVD). The picture should be divided for various blocks, every square with a volume of 1X2 pixels. The difference value between the two pixels is determined for a block and modified by adding information to it to a new value. But in traditional PVD the histograms of the stego images, some unnecessary measures are added. PVD essentially turns on to avoid any two consecutive non-overlapping elements, resulting in the absence of a straightforward traditional PVD technique to insert the hidden message bits into a color pixel, color pixel compose of three components of color so we prefer adaptive PVD because the idea of overlapping blocks has enhanced the cover image's embedding capability. Luo et al.[7] suggested a three-pixel adaptive PVD steganography that does not suffer from the effects of the steps, also Swain [8] suggested techniques of adaptive PVD steganography using vertical, horizontal and diagonal edges that do not suffer from phase effects. To achieve higher hiding efficiency, Balasubramania. [9] Issued PVD techniques with 3X3 size pixel blocks. Multidirectional edges are exploited in [10] to avoid various techniques of detection such as pixel difference histogram (PDH). Darbkh et al. [11] also suggested steganography of PVD using eight-directional PVD, an expansion of the original PVD of Wu and Tsai. This paper proposes a combination of adaptive PVD and AES to protect sensitive data by making multi-layer of defense by using cryptography and steganography in one algorithm.

3. Proposed system model
The suggested method comprises the mixture of double stages of steganography via adaptive PVD technique that provide high embedding capacity and encryption through AES algorithm To ensure that the message is not leaked even though the presence of message is exposed. Step one: the image is partitioned into blocks with 3×3 pixels in an overlapped fashion and scanned in raster-scan order. For a pixel block the central pixel is targeted for embedding. Both the horizontal and vertical edges are inspected, but one of them is considered for data embedding at the target pixel. The ranges are calculated based upon the local statistics of the blocks and the result will be (stego 1). Step two: AES256 bits algorithm is applied to (stego 1) in order to ensure security. Step three: finally embed encrypted (noisy) output into innocent digital color image (cov 2) by using the same adaptive PVD technique and the result will be (stego 2).
Figure 4. Proposed model

Transmitter process:
Where C1 is cover image 1, C2 is cover image 2, K is key. output: stego 1 input: E(C1, C2, K).

Receiver process
output: S. Where S is secret data input: D(stego1, K)

4. Experimental Results
This proposed system was performed by/MATLABR2016b frame work, we used colour images of BMP format of size (128 x 128) and (512 X 512) as (cover 1) and (cover 2) respectively in the experiments summarized in Table 2, Sample photos from the standard image database USC-SIPI (University of South Carolina-Signal and Image Processing Institute with URL: http://sipi.usc.edu/database/),http://www.imageprocessingplace.com/root_files_V3/image_databases.htm and other online resources, Table 3 summarize the results of experiments. Comparison of hiding capacity and values of PSNR of proposed method with existing methods is shown in Table 4.

The model proposed was executed with the Processor Intel® Core™ i7-6500U CPU @ 2.50GHz, 2592 MHz, dual Cores, RAM 8GB and Operating System Windows 10 Pro 64/bit.

4.1 Evaluation Criteria
- PSNR and MSE
- Image Histogram for both Cover and Stego Images

The reliability of suggested model is calculated by both PSNR and MSE, PSNR tests the quality of final Stego image comparable with the cover image. The higher the PSNR is the better the image quality. On the other side, MSE tests the statistical difference between image cover and Stego image. The smaller the value of MSE, the more efficient the technique of steganography.

PSNR =20\log_{10} \frac{Z^b-1}{\sqrt{MSE}}

Where B: is the number of bits per sample representing the color of the pixel
MSE = \| \frac{X - Y}{N} \|^2

Where N: number of pixels per image, X and Y are the image and its approximation or (Cover and Stego image).

**Table 1. The images of experiment**

| Image number | Image name | Image size   | Cover image |
|--------------|------------|--------------|-------------|
| Cover 1      | Lena       | 128X128 192KB| ![Lena](image) |
| Cover 2      | baboon     | 512X512 772KB| ![baboon](image) |

Different secret data (nonsense words) with different sizes were applied to the proposed algorithm. Table 3 summarizes these secret data used in the experiment.

**Table 2. Summary of the secret messages used in the experiment**

| item | Data content     | Size (bytes) |
|------|------------------|--------------|
| 1    | Secret data 1    | 11958        |
| 2    | Secret data 2    | 33718        |
| 3    | Secret data 3    | 44598        |
| 4    | Secret data 4    | 77238        |
| 5    | Secret data 5    | 109878       |

**Table 3. Experiment result of proposed algorithm using adaptive PVD and AES**

| Cover 1 size    | Cover 2 size    | Secret data (bytes) | Stego image size | PSNR     | MSE     |
|-----------------|-----------------|---------------------|------------------|----------|---------|
| 128X128 (192KB) | 512x512 (772KB) | 11958               | 772KB            | 61.9471  | 0.0415  |
| 128X128 (192KB) | 512x512 (772KB) | 33718               | 772KB            | 57.1594  | 0.1250  |
| 128X128 (192KB) | 512x512 (772KB) | 44598               | 772KB            | 55.9425  | 0.1655  |
| 128X128 (192KB) | 512x512 (772KB) | 77238               | 772KB            | 53.5033  | 0.2902  |
| 128X128 (192KB) | 512x512 (772KB) | 109878              | 772KB            | 51.9381  | 0.4161  |

From Table 4 we notice that the PSNR values starts from 61.94 db. according to secret data (message) size of 11958 bytes and decreasing as the secret data size increased. Further, the MSE values starts
from 0.0415 and increased as the size of the secret data (message) increased as shown in figures 8 and 9. From Table 4 we observed also that our proposed algorithm achieved better result in values of PSNR comparable with earlier exist method Wu et al[14], Khodaei etal[16], Hussain,etal[22] and it reflects on quality of stego image.

Table 4. Comparison of hiding capacity (bits) of secret data of proposed algorithm with earlier methods

| Wu et al[14] | Khodaei etal[16] | Hussain,etal[22] | Proposed algorithm |
|--------------|------------------|------------------|--------------------|
| capacity     | PSNR             | capacity         | PSNR               | capacity | PSNR          |
| 409811       | 41.53            | 806948           | 36.20              | 800673   | 3.05          | 11958           | 61.947           |
| 457170       | 37.44            | 851311           | 32.70              | 825881   | 3.15          | 33718           | 57.159           |
| 407257       | 41.39            | 803184           | 34.03              | 798636   | 3.04          | 44598           | 55.942           |
| 409819       | 40.70            | 805809           | 35.69              | 795304   | 3.03          | 77238           | 53.503           |
| 459565       | 38.13            | 847945           | 35.04              | 865093   | 3.30          | 109878          | 51.938           |

Figure 5. Values of PSNR for proposed system using all secret messages

Figure 6. Values of MSE for the proposed system using all secret messages
Figure 7 showed histogram analysis between cover image and stego image measured the robustness against common statistical attacks, also it showed that there is little difference between them.

5. Conclusion
All cryptography and steganography have limitations and may be abused if implemented separately. By combining them together, a strong algorithm is produced. We suggest an algorithm based on hybrid approach via double steganography stages (adaptive PVD + AES + adaptive PVD) to make it difficult to detect concealed information, moreover an additional security stage (AES) is provided in our algorithm in order to ensure that the secret data is not discovered even though the presence of message is exposed. The produced stego-image has a great quality according to values of PSNR, MSE and image histogram. The proposed model proves that it can be applied for transmitting secret data securely through public network. The future works of the similar projects will be on including use another steganography technique to increase the amount of secret data to be embedded and enhance imperceptibility.

References
1. HAYFAA ABDULZAHRA, ROBIAH AHMAD, NORLIZA MOHD NOOR “Combining Cryptography and Steganography for Data Hiding in Image”, Conference: Proceeding of the 13th international conference on applied computer and applied computational science (ACACOS’ 14), At Kuala Lumpur.
2. Aditya Kumar Sahu*, Gandharba Swain “A Review on LSB Substitution and PVD Based Image Steganography Techniques”, /ijeecs.v2.i3.pp712-719 2016 International Conference on Computer Systems and Applications.
3. K. C. Chang, C. P. Chang, P. S. Huang, and T. M. Tu, “A novel image steganographic method using tri-way pixel-value differencing,” Journal of Multimedia, vol. 3, no. 2, pp. 37–44, 2008.
4. Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, I.-J. Su, and C.-P. Chang, “High-payload image hiding with quality recovery using tri-way pixel-value differencing,” Information Sciences, vol. 191, pp. 214–225, 2012.
5. Swain G. 2016 Adaptive pixel value differencing steganography using both vertical and horizontal Edges. Multimedia. Tools Appl. 75, 13 541–13 556.
6. Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters.2003; 24: 1613-1626.
7. W. Luo, F. Huang, and J. Huang, “A more secure steganography based on adaptive pixel-value differencing scheme,” Multimedia Tools and Applications, vol. 52, no. 2-3, pp. 407–430, 2011.
8. G. Swain, “Adaptive pixel value differencing steganography using both vertical and horizontal edges,” Multimedia Tools and Applications, vol. 75, no. 21, pp. 13541–13556, 2016.
9. C. Balasubramanian, S. Selvakumar, and S. Geetha, “High payload image steganography with reduced distortion using octonary pixel pairing scheme,” Multimedia Tools and Applications, vol. 73, no. 3, pp. 2223–2245, 2014.
10. A. Pradhan, K. R. Sekhar, and G. Swain, “Digital image steganography based on seven way pixel value differencing,” Indian Journal of Science and Technology, vol. 9, no. 37, pp. 1–11, 2016.
11. K. A. Darabkh, A. K. Al-Dhamari, and I. F. Jafar, “A new stenographic algorithm based on multi directional PVD and modified LSB,” Information Technology and Control, vol. 46, no. 1, pp. 16–36, 2017.
12. AWDHESH K. SHUKLA, AKANKSHA SINGH, BALVINDER SINGH and AND AMOD KUMAR “A Secure and High-Capacity Data-Hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing” IEEE access Digital Object Identifier 10.1109/ACCESS.2018.2868192
13. Shavetaarora“color image enhancement based on histogram equalization”, electrical and computer engineering/ an international journal septemper 2015.
14. C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Huang, “Image stenographicscheme based on pixel-value differencing and LSB replacement methods,” IEE Proc.-Vis., Image Signal Process., vol. 152, no. 5, pp. 611–615, Oct. 2005.
15. H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, “Varied PVD+LSB evading detection programs to spatial domain in data embedding systems,” J. Syst. Softw., vol. 83, no. 10, pp. 1635–1643, 2010.
16. Khodaei and K. Faez, “New adaptive stenographic method using least significant bit substitution and pixel-value differencing,” IET Image Process., vol. 6, no. 6, pp. 677–686, Aug. 2012.
17. M. Hussain, A. W. A. Wahab, N. Javed, and K.-H. Jung, “Recursiveinformation hiding scheme through LSB, PVD shift, and MPE,” IETE Tech. Rev., vol. 35, no. 1, pp. 53–63, 2018.
18. AWDHESH K. SHUKLA, AKANKSHA SINGH, BALVINDER SINGH and AND AMOD KUMAR “A Secure and High-Capacity Data-Hiding Method Using Compression, Encryption and Optimized Pixel Value Differencing”IEEE access DOI 10.1109/ACCESS.2018.2868192.
19. Quang Do Vinh, Insoo Koo and Member, KIICE “FPGA Implementation of LSB-based Steganography” School of Electrical Engineering, University of Ulsan, Ulsan 680-749, Korea.
20. Biswapati Jana, Debasis Giri and Shyamal Kumar Mondal “Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion” International Journal of Network Security, Vol. 18, No. 4, PP. 633-643, July 2016.
21. Sandeep Panghal, Sachin Kumar and Naveen Kumar “Enhanced Security of Data using Image Steganography and AES Encryption Technique” International Journal of Computer Applications (0975–8887) Recent Trends in Future Prospective in Engineering & Management Technology 2016.