ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse100862019.pdf
https://doi.org/10.30534/ijatcse/2019/100862019

Multiple Level Information Security Using Image Steganography and Authentication

Marilou O. Espina[1], Arnel C. Fajardo[2], Bobby D. Gerardo[3], Ruji P. Medina[4]
[1]1Technological Institute of the Philippines, Quezon City, Philippines, marilouespina67@gmail.com
[2]Manuel L. Quezon University, Philippines, acfajardo2011@gmail.com
[3]West Visayas State University, Iloilo, Philippines, bobby.gerardo@gmail.com
[4]Technological Institute of the Philippines, Quezon City, Philippines, ruji.medina@tip.edu.ph

ABSTRACT

The security of information during transmission in the open network is crucial. While sharing digital data on the internet, it is essential to observe information security goals: confidentiality, integrity, authenticity, and accuracy. This paper presents a multiple tier information security through image steganography technique using a novel puzzle in YCbCr color space, and digitally signed stego image for authentication. Experimental results show that the resemblance between the stego-images and cover images is high. The recognition of the stego image is small, with the use of the Human Visual System (HVS) having an average PSNR value of 47.72db. The probability of detection of the stego-images using Chi-Square Analysis is low, with the average value of 4.39E-05.

Key words: Steganography, Data Hiding, LSB, Novel Puzzle, PSNR.

1. INTRODUCTION

Internet revolution paves the way for various modern Digital communication. It eases up the exchange of information in different forms, be it text, image, audio, video, and other formats; however, it becomes a challenge to secure the data during transmission in the open network. It is essential to observe information security goals: confidentiality, integrity, authenticity, and accuracy [1][2]. There is a necessity for a robust technique to protect digital information. One of the approaches in digital security is steganography. It is a form of protection through obscurity [3], [4]. The word steganography comes from the Greek words "stegos" which means "cover" and "grafia" means "writing" [5] [6], [7] defining it as "covered writing" or information hiding [8]. It is an art and science of writing the hidden data in such a way that no one, other than the sender and intended receiver is aware of the existence of the data [9] by covering the message existence in another medium such as audio, video, image or communication protocol. One of the steganography algorithms is the Least Significant Bit(LSB) substitution that directly replaces the LSBs of the cover image with the secret message bits. It generates only a slight distortion and maintains high image quality [10], [11]. The LSB algorithm also results in High Embedding Capacity [12], [13]; however, it suffers from low security due to the predictability of the embedding pattern [14][15]. If an image is detected to have a hidden message, the secret message can easily be retrieved [16], [17]. Thus, there remains a need to develop a new embedding pattern that offers a vast solution space. The use of novel puzzle in determining the embedding location is suitable to increase the security of steganography since it provides huge solution space just like other puzzles.

Other than steganography, other techniques such as cryptography, hashing, digital signature can be utilized for the primary purpose of data protection and security [18]. As [19], [20] said that implementing a combination of these different information security schemes simultaneously is a powerful tool for secret communications and strengthens digital data security.

This paper introduces the multiple-layer security of digital data using novel puzzle image steganography in YCbCr color space and digital signature. The rest of the paper is organized as follows: Section 2 presents a brief discussion about topics related to the study; Section 3 describes the proposed method; Section 4 shows the result and discussion and Section 5 the conclusion.

2. RELATED LITERATURE

2.1 YCbCr Color Space

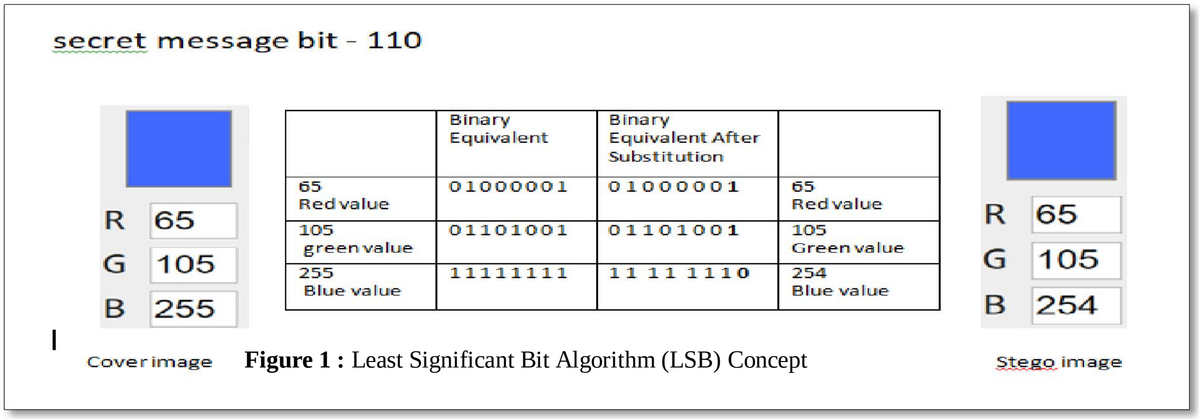
Color space is a mathematical representation of color information as three or four different color components. This color space represents each color with three (3) values, in the same way as the RGB space. The Y component represents the intensity of the luminance. The Cb component indicates the blue intensity relative to the green component, and the Cr component indicates the intensity of the red relative to the green component [18].

2.2 Digital Signature

One of the techniques in ensuring the integrity of digital data is the digital signature. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that a known sender created the message, and that it was not altered in transit [21]. It enables the recipient of a message to authenticate the sender of a message and verify that the message is intact. A digital signature algorithm includes a signature generation process and a signature verification process. The digital signature of an image is produced by using a hash function to create the message digest, and public-key encryption algorithm is used in conjunction with the message digest before transmission [22].

2.3 Least Significant Bit (LSB) Algorithm

LSB Algorithm is spatial steganography that hides data by modifying directly the image pixel values[12], which results in a technique that is simple, with low computational cost [18]. Eight (8) bits represent the red, green, blue(RGB) value of every single pixel of the color image, and the bits from the secret message replaced the least significant bit or the 8th bit sequentially [20].



	Binary Equivalent	Binary Equivalent After Substitution	
65 Red value	01000001	01000001	65 Red value
105 green value	01101001	01101001	105 Green value
255 Blue value	11111111	11 11 1110	254 Blue value

Figure 1 : Least Significant Bit Algorithm (LSB) Concept

For example, one pixel cover medium with a color of royal blue. Shown in figure 1 is the RGB value and its equivalent binary number of the colors. The secret message bit ***110*** is embedded in the cover medium by substituting the least significant bit which is the eight (8th) bit of every binary equivalent of the RGB value. The binary equivalent of the secret message is embedded in sequence in the pixels of the cover-image. As presented in figure 1 only the blue value of the pixel is changed . There is no apparent difference between the cover image pixel and the stego image pixel, hence the secret message is successfully concealed.

There are several studies conducted to the modification of the Least Significant Bit (LSB) Algorithm. Numerous studies focus in changing the embedding pattern such as the study [24] wherein it creates a non-overlapping blocks of the cover image and in each block it is divided again into sub blocks. Then ‘Z’ pattern is used in the selection of the sub-blocks, and the ‘I’ pattern is used in the selection of the pixels. It resulted in a low value of PSNR for images other than the medical image.

A different method to modify the LSB algorithm is by changing the embedding pattern in the color plane. In the paper of [25], it introduces a technique that hides the message in the red, green, and blue planes of the image. It used the 2-2-4 LSB insertion. 2 data bits hidden in 2 least significant bit of red plane, 2 data bits hidden in 2 least significant bit of green plane, and 4 data bits hidden in 2 least significant bit of blue plane. It inserted the secret message in each plane based on color sensitivity in which the blue plane is less sensitive to light; thus, human eyes will find it very difficult to detect minor changes in the color intensity.

To further strengthen the security of LSB, it is combined with other techniques. In the study of [26], it included the authentication process, the message is encrypted using AES, and the hash value of the message is also encrypted as well as the key using RSA to produce the digital signature. All the encrypted files form the complete message and embedded in the image using steganography.

3. THE PROPOSED METHOD

In this section, the different procedures of the proposed method are presented.

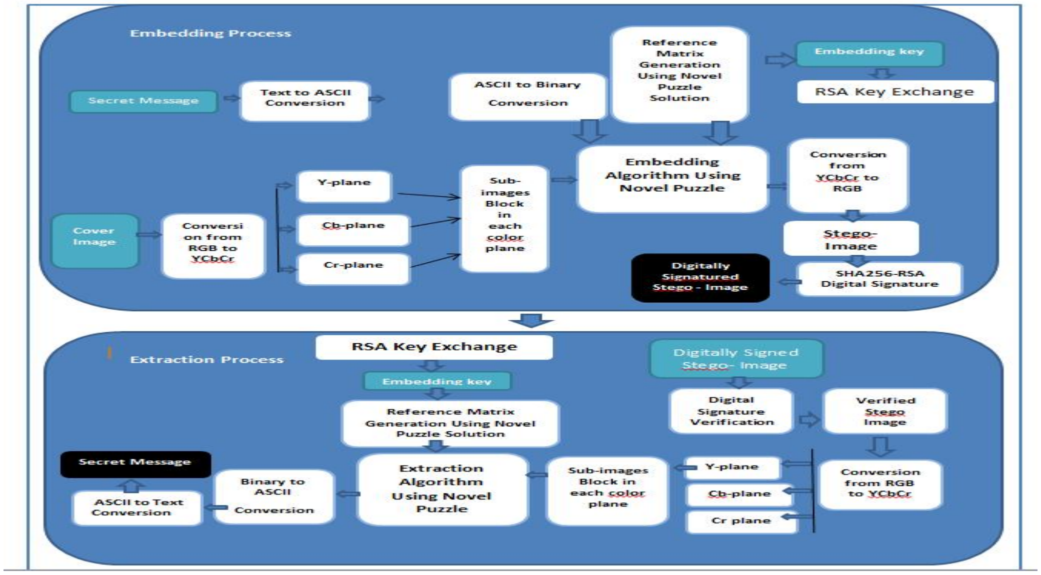

Embedding Process
Secret Message
Text to ASCII Conversion
ASCII to Binary Conversion
Reference Matrix Generation Using Novel Puzzle Solution
Embedding key
RSA Key Exchange
Cover Image
Conversion from RGB to YCbCr
Y-plane
Cb-plane
Cr-plane
Sub-images Block in each color plane
Embedding Algorithm Using Novel Puzzle
Conversion from YCbCr to RGB
Stego-Image
SHA256-RSA Digital Signature
Digitally Signatured Stego - Image
Extraction Process
RSA Key Exchange
Embedding key
Reference Matrix Generation Using Novel Puzzle Solution
Digitally Signed Stego- Image
Digital Signature Verification
Verified Stego Image
Conversion from RGB to YCbCr
Y-plane
Cb-plane
Cr plane
Sub-images Block in each color plane
Extraction Algorithm Using Novel Puzzle
Binary to ASCII Conversion
ASCII to Text Conversion
Secret Message

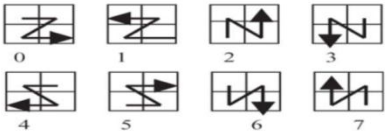
Figure 2: Proposed Framework

Figure 2 describes the conceptual framework of the study. It involves the embedding process and the extraction process. In the embedding process, it will have three inputs, which are the cover image, secret message, and embedding key. The embedding key will be shared using RSA. The color cover image will be converted into YCbCr color space, and each color plane will be divided into blocks of sub-images. The solution of the novel puzzle will be the bases of the reference matrix. The secret message will be embedded in each color plane of the image cover in the least significant bit using the reference matrix as the embedding pattern. The image will be converted back to RGB color space from YCbCr color space to produce the stego-image. The stego image will be digitally signed by using the SHA-256 hash algorithm to generate the message digest, and RSA Digital Signature Algorithm will be used to produce the signature. In the extraction process, the stego image will be verified, whether it is modified or not during transmission. The Conversion of the verified stego image from RGB color space to YCbCr color space will be done. RSA decryption will be done on the embedding key to get the reference matrix using the novel puzzle solution. The extraction of the secret message utilizes the reference matrix as the pattern.

3.1 The Embedding Procedure

Algorithm 1 - **Embedding Algorithm**

```
Input: Cover image I, Secret Message S
Cover Image Pre Processing
    1. Initialize I ← Cover Image, S ← Secret Message
    2. Convert the Cover Image (I) from RGB to YCbCr.
    3. Separate the Y, Cb and Cr color plane.
    4. In each color-plane, Split the image into a non-overlapping block (sub-image) and label each block B1, B2,... $B_j$ following the value of the reference matrix
Novel Puzzle Matrix Generation
    5. Initialize the size of the matrix.
    6. The value in the circles will have values ranging from 1 to $X$ where $X =( N*N) –N$
    7. Generate a value of every cell of the matrix with values from $1$ to $M$, wherein $M = N x N$ having no repetition of numbers.
    8. The values in each cell must follow the rule that the numbers in the circles are the multiplication modulo $X$ of the two adjacent cells where $X$ represents any number from 2 to $Y$ denoted by $Y =( N*N) –N$
    9. For the expansion of the original matrix:
        a. Get the middle pixel value in the red plane
              Pixel value =image[row div 2][col div2]
        b. Shifting code = pixel value mod 8
```



```
10. Embed the secret message in the least significant
    bit (LSB) of the pixel in each color plane. Use the
    values of the expanded reference matrix as the bases
    for the location of the pixel to be embedded.
11. Convert the YCbCr image back to RGB to have the
    stego-image.
10. Use SHA 256-RSA for Digital Signature and insert
    the digest at the end of the file.
Output: Stego Image with Digital Signature
```

3.2 The Secret Message Extraction Procedure

```
Algorithm 2- Extraction Algorithm
Input: Stego Image,

1. Verify the Digital  Signature.
2. If Verification =ok
       Secret Message Extraction
   a.  Convert the RGB stego image to YCbCr
   b.  In each color plane determine the block and
       embedded pixel location using the reference
       matrix,
   c.  Convert the value of the embedded pixel to its
       equivalent bits.
       c.   Retrieve the hidden bits from the LSBs of
       the embedded pixel location and convert to
       equivalent ASCII code to get the secret message
       S.
   Else
       Notification of Compromised Stego Image
Output: Extracted Secret Message
```

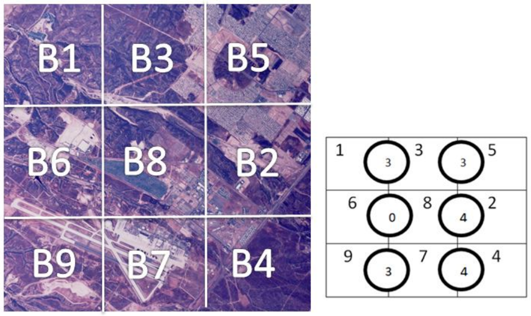


Figure 3: Cover Image Blocks

The cover image is divided into non-overlapping blocks based on the solution of the puzzle. As shown in figure 3, the number of cells in the matrix is the same as the non-overlapping blocks in the cover image, and the block number will follow the value of the matrix. The embedding of the secret message will start from Block 1 (B1), then to Block 2 (B2), and so on until the entire secret message is embedded.

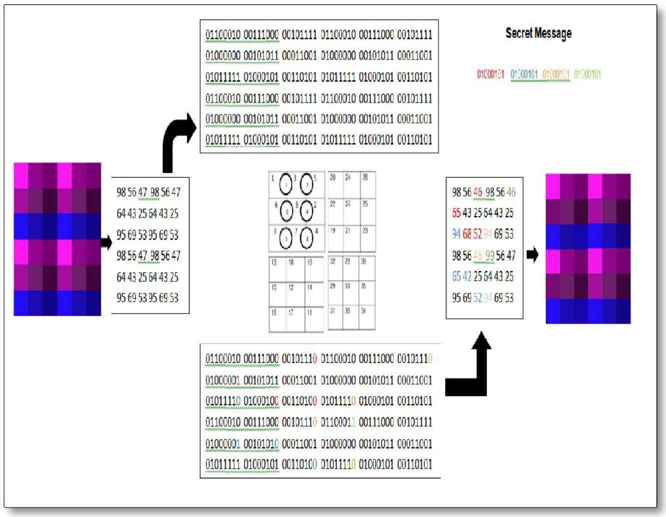


Figure 4: Embedding Process Simulation

In a portion of the cover image, the embedding process is simulated, as shown in figure 4. The cover image in the Cb plane is converted to its binary value, and the secret message is embedded in the least significant bit using the pattern in the reference matrix. The first bit in secret message is 0, and referring from the order in the reference matrix the number 1 is at row[1]col[1]; therefore, the secret message will be embedded in that location. Since the least bit value in that location is already 0, so no changes will take place. There are no changes to the cover image in embedding the secret bits 1 to 3. In row[3]col[3], where the value 4 in the reference matrix is located, the cover image lsb is changed from 1 to the value of the 4th secret bit 0. The process will continue until the entire secret message is already embedded. The bold-colored lsb are the only bits changed in the embedding process. The bits are converted back to its ASCII equivalent, which is the value of the pixel in the Cb plane.

4. RESULTS AND DISCUSSION

The results of the simulation conducted are presented and discussed in this section. In the simulation, images from the University of Washington Department of Computer Science and Engineering Ground Truth Database are utilized for testing, and the secret message embedded is 3600 bits. We selected 45 color images of size sizes 756 x 504. The simulation of the proposed method is performed on MATLAB R2016a with Intel Core i7 2.7GHz CPU and 8GB DDR4 RAM.

4.1 Imperceptibility

The imperceptibility of the stego-images is essential, which means that after the embedding of the secret message to the cover image, there should not be any visible distortion. The Peak-Signal to-Noise Ratio (PSNR) is utilized to measure the extent of visual distortions of the stego image. PSNR is a quality measuring metric, calculating the amount of distortion between the cover image and stego image in the unit of decibel (dB). A higher score of PSNR indicates a better image. To calculate the PSNR, we must first calculate the Mean Square Error (MSE) between the hidden image and the cover image[24], which will be calculated using equation 1 and equation 2, respectively.

$$MSE = \frac{1}{mxn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(I_{ij} - SI_{ij}\right)^2 \qquad (1)$$

The I_{ij} is the cover image pixel value and SI_{ij} is the stego-image pixel value at ith row and jth column. The m and n are the numbers of rows and columns in the digital image. The MSE should have a small value as possible.

$$PSNR = 10 \text{ x } \log_{10}\frac{255x255}{MSE} \qquad (2)$$

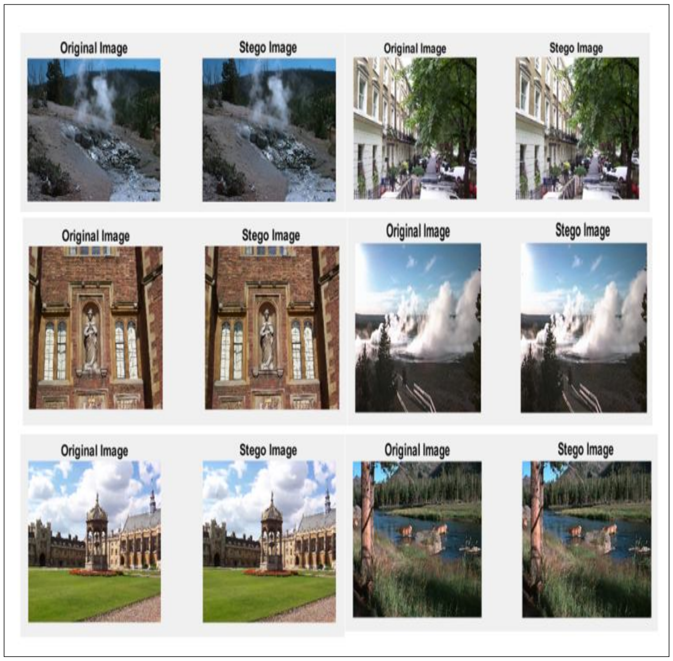


Figure 4 : Original and Stego Images in Proposed Method

The cover image and the stego image after embedding the secret message is shown in figure 4. It can be seen that the human eye cannot tell apart the cover image and the stego image. It cannot distinguish the existence of hidden information in the stego image. Furthermore, from the comparison of Figure 5, the image histogram of the cover image and stego image are almost similar.

As shown in table 1, the average MSE for the 45 images is 1.107. The average PSNR of the proposed technique is 47.72 dB, which is higher than the standard acceptable PSNR. Having a value 28 dB or higher means the quality of the image is satisfactory [25], which means that the larger the value of PSNR, the less distortion of the image. It implies that chance is low in the detection of the stego image using the Human Visual System (HVS).

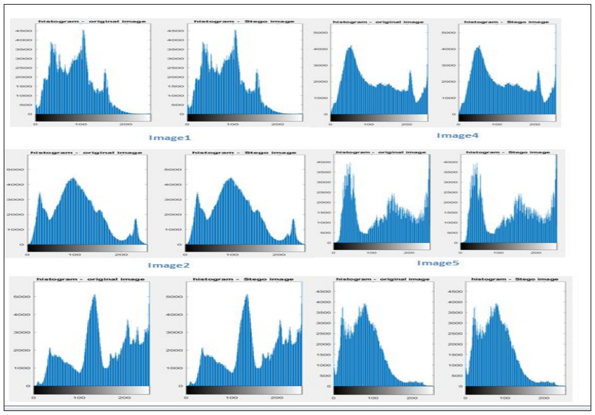


Figure 5 : Original and Stego Images Histogram

Table 1: MSE and PSNR Result

	MSE	PSNR
image 1	1.0463	47.9341
image 2	1.161	47.4825
image 3	1.0463	47.9341
image 4	1.0463	47.9341
image 5	1.0463	47.9341
image 6	1.0463	47.9341
image 7	1.0463	47.9341
image 8	1.0463	47.9341
image 9	1.0463	47.9341
image 10	1.0463	47.9341
image 11	1.0463	47.9341
image 12	1.0463	47.9341
image 13	1.204	47.3245
image 14	1.0463	47.9341
image 15	0.7714	49.2579
image 16	0.967	48.2766
image 17	1.0463	47.9341
image 18	1.1517	47.5175
image 19	0.7931	49.1373
image 20	1.075	47.8167
Average of 45 images	**1.107564**	**47.72309**

4.2 Chi-Square Analysis

Chi-Square Test is a simple statistical attack. The test compares the statistical properties of a questionable image with the expected statistical properties of the medium such that it is possible to determine the likelihood that a suspect image is embedded with a message [26]. Having a probability value near zero 0 means that the stego-image cannot be detected using the chi-square test. Table 2 shows the average P-value (chi-square value) of 4.39E-05. It implies that most of the stego images were given a low probability of having a secret message embedded.

Table 2 – Result of the Simulation to the stego-images against Chi-Square Steganalysis

	P value
image 1	3.97E-16
image2	1.32E-10
image 3	4.00E-09
image 4	1.41E-04
image 5	3.23E-07
image 6	1.52E-19
image 7	5.95E-21
image 8	2.72E-06
image 9	2.23E-10
image 10	1.95E-06
image 11	9.43E-06
image 12	4.87E-14
image 13	4.16E-17
image 14	6.32E-04
image 15	1.48E-22
image 16	1.40E-19
image 17	1.01E-18
image 18	6.28E-25
image 19	9.26E-04
image 20	4.64E-06
Average of 45 images	4.39E-05

4.3 Hamming Distance

Hamming distance refers to the number of bit positions in which two objects differ. Having a result of zero (o) means that the images are the same and if the value is less than ten(10) there is s slight difference between the images and having a value of more than ten (10) means that the images compared are different[27]. As shown in table 3, the average Hamming distance between the stego image before the digital signature and after the digital signature is zero(0). It implies that the two images are the same and not distorted after digitally signing the stego image.

Table 3 – Hamming distance between the stego image before the and after the digital signature

	Hamming Distance
image 1	0
image2	0
image 3	0
image 4	0
image 5	0
image 6	0
image 7	0
image 8	0
image 9	0
image 10	0
image 11	0
image 12	0
image 13	0
image 14	0
image 15	0
image 16	0
image 17	0
image 18	0
image 19	0
image 20	0
Average of 45 images	0

5. CONCLUSION

New multiple layer security of digital data using novel puzzle image steganography in YCbCr color space and digital signature has been presented. The secret message was embedded with the use of the novel puzzle solution as the determinant of the embedding location. Performing the steganography in the YCbCr color space added another layer of security. To further strengthen the security, the stego image will be authenticated through digital signature. Experimental results show that the resemblance between the stego-images and cover images is high. The recognition of the stego image is small, with the use of the Human Visual System (HVS) having an average PSNR value of 47.72db. The probability of detection of the stego-images using Chi-Square Analysis is low, with the average value of 4.39E-05. Furthermore, there is no difference between the stego image before and after the inclusion of the digital signature with an average value of zero (o) for the hamming distance.

REFERENCES

[1] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," *Signal Process. Image Commun.*, vol. 65, pp. 46–66, 2018. https://doi.org/10.1016/j.image.2018.03.012

[2] A. E. Karrar, M. Fadl, and I. Fadl, "International Journal of Advanced Trends in Computer Science and Engineering Security Protocol for Data Transmission in Cloud Computing," vol. 7, no. 1, pp. 1–5, 2018. https://doi.org/10.30534/ijatcse/2018/01712018

[3] G. Karthigai Selvi, L. Mariadhasan, and K. L. Shunmuganathan, "Steganography using edge adaptive image," *2012 Int. Conf. Comput. Electron. Electr. Technol. ICCEET 2012*, pp. 1023–1027, 2012. https://doi.org/10.1109/ICCEET.2012.6203727

[4] C. Paper and N. Akhtar, “An improved inverted LSB image steganography,” no. February 2014, pp. 749–755, 2014.

[5] M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” *Comput. Sci. Rev.*, vol. 13–14, no. C, pp. 95–113, 2014.

[6] M. K. Rao, K. P. Reddy, and K. E. Saranya, “Security Enhancement in Image Steganography a MATLAB Approach,” *Middle East J. Sci. Res.*, vol. 23, no. 2, pp. 357–361, 2015.

[7] I. Kajal, H. Rohil, and A. Kajal, “LZW based Image Steganography using Kekre ’ s Algorithm,” *Int. J. Comput. Sci. ad Inf. Technol.*, vol. 5, no. 2, pp. 2643–2648, 2014.

[8] A. Lec and M. H. Abood, “Steganography with RC4 and Pixel Shuffling Encryption Algorithms,” no. March, pp. 7–9, 2017.

[9] K. H. Raviya, D. V. Vyas, and A. M. Kothari, “SVD Based Performance Improvement in Hiding a Message Behind an Image,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 2, pp. 182–186, 2019. https://doi.org/10.30534/ijatcse/2019/12822019

[10] K. Thangadurai and G. Sudha Devi, “An analysis of LSB based image steganography techniques,” *2014 Int. Conf. Comput. Commun. Informatics Ushering Technol. Tomorrow, Today, ICCCI 2014*, pp. 3–6, 2014. https://doi.org/10.1109/ICCCI.2014.6921751

[11] N. Jiang, N. Zhao, and L. Wang, “LSB Based Quantum Image Steganography Algorithm,” *Int. J. Theor. Phys.*, no. 201406545034, 2015.

[12] B. Li, J. He, J. Huang, and Y. Qing Shi, “A Survey on Image Steganography and Steganalysis,” *J. Inf. Hiding Multimed. Signal Process.*, vol. 2, no. 2, pp. 142–172, 2011.

[13] S. N. Kishor, “A REVIEW ON STEGANOGRAPHY THROUGH.”

[14] R. Roy, S. Changder, A. Sarkar, and N. C. Debnath, “Evaluating Image Steganography Techniques : Future Research Challenges,” pp. 309–314, 2013.

[15] M. June, R. J. Rasras, M. Rasmi, A. Sara, Z. A. Alqadi, and R. Abu, “Comparative Analysis of LSB , LSB2 , PVD Methods of Data Steganography,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 3, pp. 748–754, 2019. https://doi.org/10.30534/ijatcse/2019/64832019

[16] N. Akhtar, P. Johri, and S. Khan, “Enhancing the security and quality of lsb based image steganography,” *Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013*, pp. 385–390, 2013. https://doi.org/10.1145/3288155.3288181

[17] S. N. Gowda, “Advanced Dual Layered Encryption for Block Based Approach to Image Steganography,” pp. 250–254, 2016. https://doi.org/10.1109/CAST.2016.7914975

[18] M. R. D. Molato, B. D. Gerardo, and R. P. Medina, “Secured Data Hiding and Sharing using Improved LSB-based Image Steganography Technique,” pp. 238–243, 2019.

[19] S. Mittal, S. Arora, and R. Jain, “PData Security using RSA Encryption Combined with Image Steganography,” 2016.

[20] H. Ge, M. Huang, and Q. Wang, “Steganography and steganalysis based on digital image,” *Proc. - 4th Int. Congr. Image Signal Process. CISP 2011*, vol. 1, pp. 252–255, 2011. https://doi.org/10.1109/CISP.2011.6099953

[21] U. Somani, K. Lakhani, and M. Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing,” pp. 211–216, 2010. https://doi.org/10.1109/PDGC.2010.5679895

[22] A. Sinha and K. Singh, “A technique for image encryption using digital signature,” vol. 218, pp. 229–234, 2003. https://doi.org/10.1016/S0030-4018(03)01261-6

[23] S. Mohan and S. Singh, “Image Steganography : Classification , Application and Algorithms,” *Int. J. Core Egineering Manag.*, vol. 1, no. 10, 2015.

[24] M. R. Mani, V. Lalithya, and P. S. Rekh, “An Innovative Approach for Pattern Based Image Steganography,” *IEEE*, pp. 2–5, 2015.

[25] A. Singh and H. Singh, “An Improved LSB Based Steganography Technique for RGB Color Images,” *Int. J. Comput. Commun. Eng.*, pp. 513–517, 2015.

[26] C. Biswas, “An Efficient Algorithm for Confidentiality , Integrity and Authentication Using Hybrid Cryptography and Steganography,” *2019 Int. Conf. Electr. Comput. Commun. Eng.*, pp. 1–5, 2019. https://doi.org/10.1109/ECACE.2019.8679136