Image Steganography in Spatial Domain

A Comparative Literature Review of SCI Articles

Musawer Muradi
195112046

29.11.2020
Class Id: BTM551 Supervisor: Asst. Prof. SERDAR SOLAK
Department of Computer Engineering
Kocaeli University, 41380, Kocaeli
musavir.muradi@gmail.com

Abstract

The sending of encrypted messages attracts the attention of programmers and crackers who would seek to intercept and uncover the messages before arrive their intended destination. Steganography is one way to mask communication by hiding unrevealed message inside another unsuspecting message. [1] *Steganography can be combined with cryptography in order to offer a satisfactory measure of privacy and security. In this study, at least 3 SCI articles on image steganography in spatial domain published in 2020 have been reviewed. The articles selected based on the image stenography techniques and algorithms in spatial domain. Even though it is interesting to highlight that the existing embedding techniques may not be perfect, the objective of this paper is to provide a comprehensive survey and to highlight the pros and cons of existing up-to-date techniques for researchers that are involved in the designing of image steganographic system. Furthermore, different performance matrices are also discussed. The paper concludes with recommendations and good practices drawn from the reviewed papers.*

Keywords: *Image Steganography · Least Significant Bit (LSB) · Spatial Domain Image Steganography · Review on image steganography · Systematic review of spatial domain steganography techniques · Pixel Value Differencing Steganography*

1. Introduction

The Internet revolution offers digital communication simplicity; meanwhile, it also becomes a challenge to protect data over the open network. In order to solve information security, various approaches to information encryption and information hiding have been suggested in the field of security systems, as shown in Fig. 1. The encryption of data known as cryptography scrambles the hidden message to make it an unintelligent message for eavesdroppers. This however, is still unable to encrypt the hidden message, which draws attention. Therefore, an invisible communication is needed without noticing to anyone that in certain cases the communication will occur. This is why a mechanism for hiding information is needed. Two subdisciplines, i.e. steganography and watermarking [2], consist of information hiding.

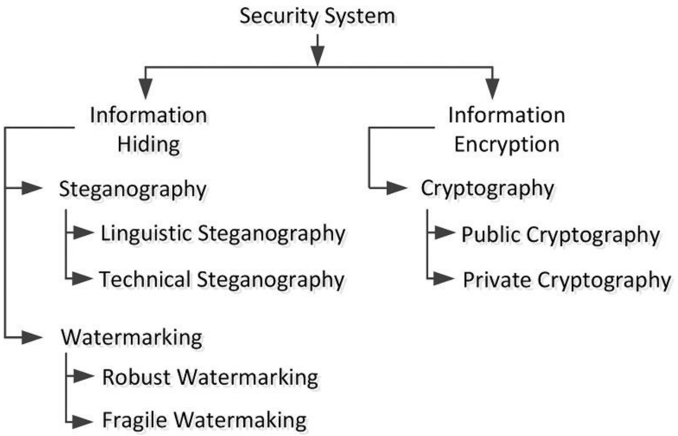


Figure 1. Basic security system branches (based on Cheddad et al.) [3]

Steganography is a secret communication technique when the messages between to edge are encrypted and no one can detect the existence of hidden messages except the sender and the receiver of the message [4]. Steganography is considered a kind of a hidden communication which means literally the "covered writing". Originally, it has been derived from the two Greek words stegano which refers to "covered" and graphos which refers to "to write". The goal of applying the steganography is to hide the information message inside a harmless cover medium in a certain way that makes it impossible to detect the secret information and even its existence in the cover medium [5].

Generally, communication mediums/carriers are digital files or data i.e. image, video, text, audio, network protocol and DNA(Figure 1) [6].

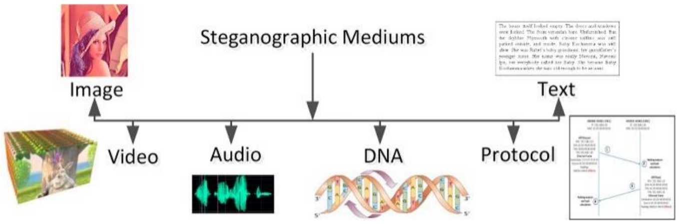


Figure 2. Steganographic mediums.

Usually, image steganography can be categorized into different (spatial and transform) embedding domains. spatial domain directly exploits the cover image data/pixels to conceal the secret information, e.g. substitution of secret bits inside pixel value [6]. In contrast transform domain, the data of the cover image is first converted into other signal/form before applying the embedding process [6]. Due to simplicity in the embedding and extraction process, spatial domain embedding methods are more common than domain transformation, but have less robustness [6].

This paper focuses on researches made on spatial domain image steganography techniques published in 2020 onwards.

The rest of the paper is organized as follows. The methodology and material are presented in section 2. The analysis of the techniques discussed in the papers are presented in section 3. The conclusion and results are given in section 4.

2. Methodology and Materials

A comparative literature review about spatial domain image steganography techniques on SCI articles published onwards 2020 was conducted to summarize and compare the steganography techniques.

2.1. Methods

The review started with planning and selection of the articles, since the articles were required to contain a technique or algorithm of image steganography.

The search focused on SCI articles published in 2020 on domains such as IEEE, Scopus, Elsevier, ResearchGate, ScienceDirect, Google Scholar, arXiv, etc.

The search strings were: spatial domain image steganography · image steganography · least significant bits (lsb) · pixel value differencing (pvd) · data hiding techniques.

At least 20-30 articles published by the mentioned domains examined and the most relative 3 selected. The value and motivation of each paper summarized and then gone over each for reviewing

2.2. Materials

Articles reviewed in this paper is as followed:

- A Secure Image Steganography using LSB and Double XOR Operations published IJCSNS

International Journal of Computer Science and Network Security in July 2020.

- The Steganographic Approach to Data Protection Using Arnold Algorithm and the Pixel-Value Differencing Method published in IEEE Third International Conference on Data Stream Mining & Processing in 2020.
- LSB and RLE Based Approach for Increasing Payload and Security of Stego Images published in Advances in Intelligent Systems and Computing in 2020.

2.3. Validation Metrics

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to compare image compression quality [7].

PSNR

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image [7].

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right)$$

MSE

The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error [7].

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

3. Analysis

In this chapter, all three articles are analyzed and resulted in the next chapter.

3.1. A Secure Image Steganography using LSB and Double XOR Operations

This study proposes two layers of encryption and hiding stages. Here, first the message is encrypted by using a Secret key (extract from MSB) and double XOR operations using binary representation, and then an encrypted stream of bits is hidden into the cover image using the LSB technique. To ensure the quality of our proposed method, a well-known evaluation measure, such as MSE, PSNR, Entropy and histogram distribution, was calculated [8].

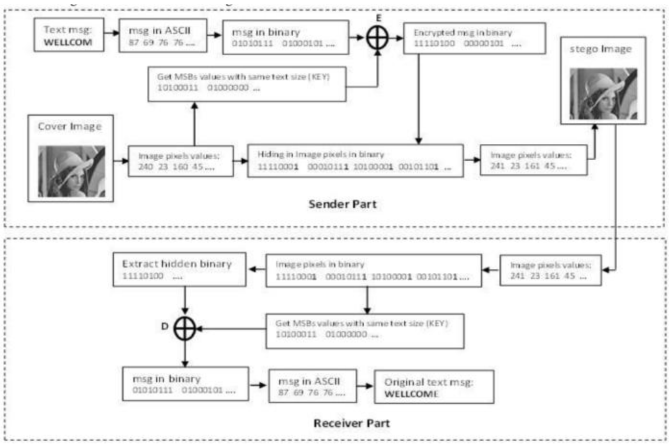


Figure 3. The encryption/decryption workflow of the proposed technique.

A combination of steganography and cryptography techniques will ensure better information confidentiality and meet the requirements of protection and robustness for the transmission of significant information. For the combination of both strategies, Figure 3 presents the proposed process. A one-time pad (OTP) symmetric double XOR encryption algorithm is used; this algorithm is noted to be very fast and unbreakable as it performs a single operation on both plain text and random key streams of bits. In the concept of key generation, there are additional good and powerful features of this system, and neither a need for a key to be produced nor sent to the receiver component. A key used by both parties would automatically extract from the most important bits of cover and stego-image image pixels; the only information we need to send is the length of the plain text message of the recipient. For this reason, the authors proposed to retain a few first bytes (always first 32) of the cover image to send the duration of the binary user text message and to locate it on the second LSBs to prevent hidden text messages from overlapping, the following algorithm shows steps in both the sender and receiver sections [8]:

```
Start Encryption
Key1 ← Extract string of bits from MSBs of C as same length of m
m-in-bits=convert message m to string of bits
EMtemp = m-in-bits XOR Key1
Key2 = flip (Key1)// turns over all bits
EM = EMtemp XOR Key2 // EM is encrypted user message
for i = 1 to length (m) do
    Si ← LSB1(Ci) = EMi // hiding encrypted message in first LSB
end for
Lkey=dec2bin(length (m))
for i = 1 to length Lkey (in bits)
    Si ← LSB2(Ci) = Lkey // hiding
```

```
length of message in second LSB
end for
end

Start Decryption

for i = 1 to first 32 bytes of S do //always length of m is first 32 bytes
Lkey ← Extract string of bits for message length from LSB2(Si)
end for
length (m)=bin2dec(Lkey)
for i = 1 to length (m) do
key1 ← Extract string of bits from MSBs of S
end for
for i = 1 to length (m) do
EM ← Extract string of bits from LSB1(Si)
end for
EMtemp = EM m-in-bits XOR Key1
Key2 = flip (Key1)
m-in-bits = EMtemp XOR Key2 // user message m
End
```

Results:

The images encrypted using the proposed technique:

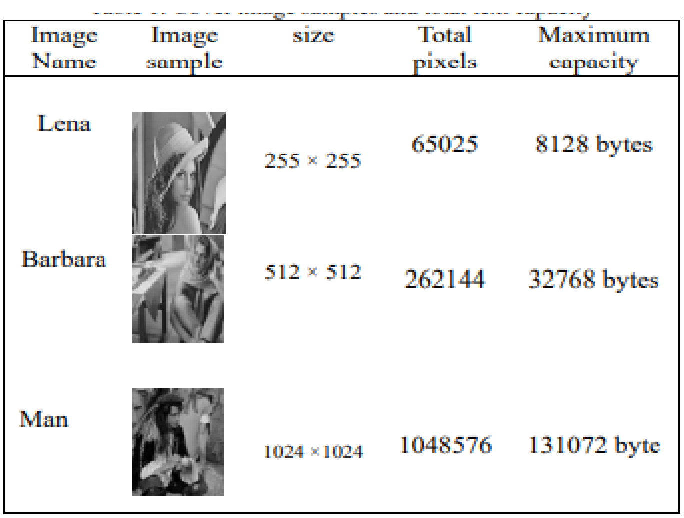


Image Name	Image sample	size	Total pixels	Maximum capacity
Lena		255 × 255	65025	8128 bytes
Barbara		512 × 512	262144	32768 bytes
Man		1024 × 1024	1048576	131072 byte

Figure 4. Cover image samples and total text capacity

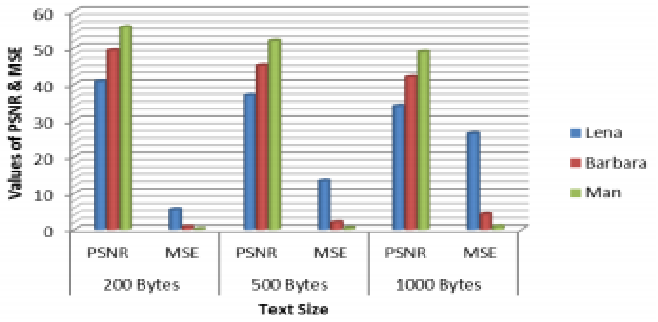


Figure 5. PSNR and MSE metrics of the given images.

Most values of PSNR are greater than 40 dB, which is considered as being an acceptable performance, as reported by Nolkha et al [9]. And in the figures below shows the cover and stego images of the encryption as well as their histogram plots.

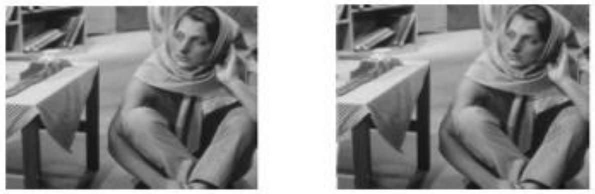


Figure 6. a) Barbara cover image b) Barbara stego image

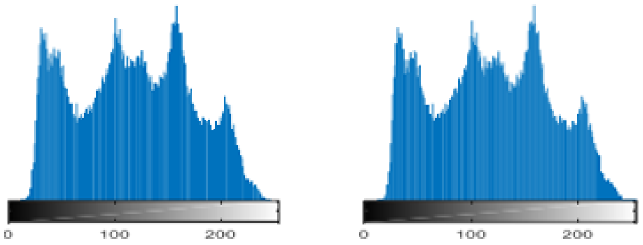


Figure 7. Histogram for fig.6a and 6b

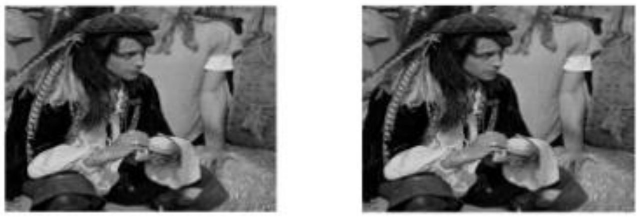


Figure 8. a) Man cover image b) Man stego image

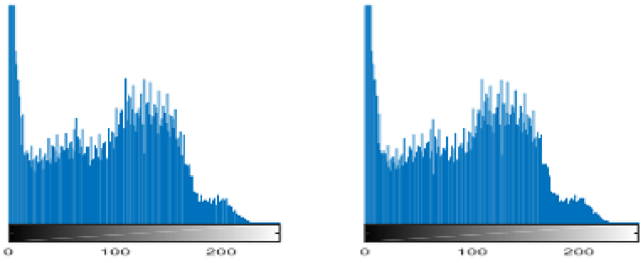


Figure 9. Histogram for fig. 8a and 8b

3.2. The Steganographic Approach to Data Protection Using Arnold Algorithm and the Pixel-Value Differencing Method

This article considers the process of embedding confidential information in the spatial domain of BMP format digital images. The most beneficial graphic data format is the BMP format in terms of steganography. The simple structure and large volume of BMP files make it easy to change their contents without the need for decompression and thus, without compromising the secret details that could occur during the compression of the file [10].

In this article the authors implement the steganographic transformations by the pixel difference method (Pixel-Value Differencing – PVD) enhanced by the Arnold Algorithm.

The classic PVD:

The classic PVD method uses the modify brightness values of two adjacent pixels P(i) and P(i+1), for which the absolute difference d = |P(i) – P(i+1)| d(i) ϵ [0,255] is calculated. The lower and upper limits [lower(i), upper(i)] of range R(i) and number of bits t = [log$_2$(upper(i) – lower(i) + 1)], which can embedded in the pixels, are determined based on the obtained value of d(i) in accordance with the table of quantization ranges. The message bits sequence of length t is converted to a decimal value t(d), after which is calculated a new difference value d′(i) = t(d) + lower(i). The brightness values of the pixels P(i) and P(i+1) are modified according to the formula [11]:

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

Where m(i) = |d’(i) – d(i), [.] rounding to a smaller integer, [‘] - rounding to a larger integer.

When the resulting values of pixel brightness are outside the accepted range [0,255], they corrected as follows [12]:

$$(P_i'', P_{i+1}'') = \begin{cases} (255, 255 - d - m), & if\ P_i' > 255; \\ (0, d + m), & if\ \ P_i' < 0; \\ (255 - d - m, 255), & if\ P_{i+1}' > 255; \\ (d + m, 0\ ), & if\ \ P_i' < 0. \end{cases}$$

Errors while extracting secret information from images can be avoided due to using the brightness a correcting procedure [10].

A typical setting of the ranges is that [0, 7], [8, 15], [16, 31], [32, 63], [64, 127] and [128, 255]. You can use several other variants of the quantization tables, which differ in the size of the ranges, and therefore the number of bits that can be embedded [12].

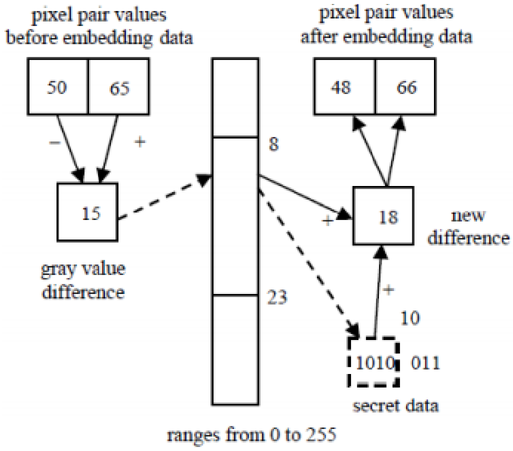


Figure 10. data embedding using PVD.

Arnold Algorithm:

To increase the robustness of steganographic transforms, the authors use the image scrambling technique [13]. Image scrambling techniques scramble the pixels of an image in such a manner that the image becomes chaotic and indistinguishable.

In this article for image scrambling the authors use the simple but powerful Arnold transformation [14] [15] which is periodic in nature and is very much popular in spatial domain applications:

$$\binom{x'}{y'} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \binom{x}{y} (mod\ N),$$

where x , y ϵ {0, 1, … .N -1} andN, is the size of a digital image.

The proposed system:

The steps of the confidential information embedding algorithm by a PVD method in pixel of a movable image, which with application Arnold transformation are chaotically disposed in the field container.

Step 1: Firstly, scramble the images using the Arnold transformation.

Step 2: Stop the converting image process by Arnold transformation at the some step for order to hide the message in the resulting modified image. The Arnold transformation series stop number during decoding process uses as the secret key. It is clear that during the converting process, pixels change their locations. The original image is visually distorted [10].

Figure 11. Empty steganography container Lena.bmp

Figure 12. Empty steganographic container scrambled 90 times using Arnold Algorithm.

Step 3: Implement the rest (up to a full period) of Arnold transformation steps to get an image that will not visually different from the original, but will contain a hidden secret information.

After scrambling the PVD is applied as it should be and for decrypting the inverse of the same operation is conducted.

Obviously, this system provides secure transformation of vital data across the peers.

3.3. LSB and RLE Based Approach for Increasing Payload and Security of Stego Images

The attempt is made in this article to achieve both protection and increased payload together. In this the technique of LSB replacement is applied in a simple way. Here the difficulty in measuring complex segments is avoided, instead of using the principle of data compression here, resulting in increased payload and security [16].

The work is essentially a blend of LSB and run-length encoding (RLE) techniques. RLE is lossless image compression technique. The data to be hidden is first encoded using RLE algorithm which results into compaction and data security as well. The ability to embed data is thus enhanced. Data compaction increases data embedding capability [16].

The RLE procedure is explained in Fig. 9. The first three bits in the original stream are compared with the group of next three bits in the sequence until the mismatch is found. The match count which is considered as the "run length" is coded in binary format to form compressed stream. This compressed stream is suitably decoded to obtain original stream as shown in Fig. 9 [16].

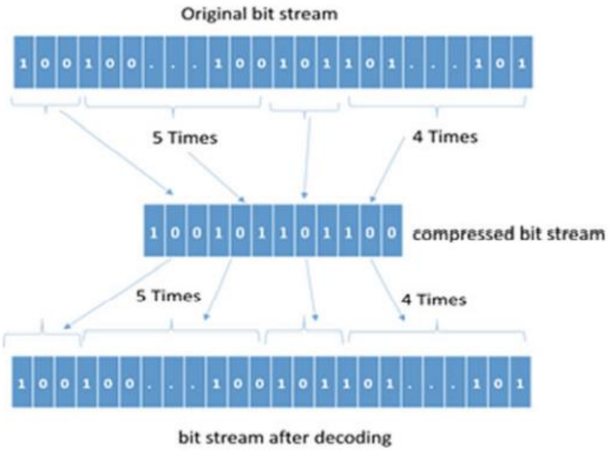
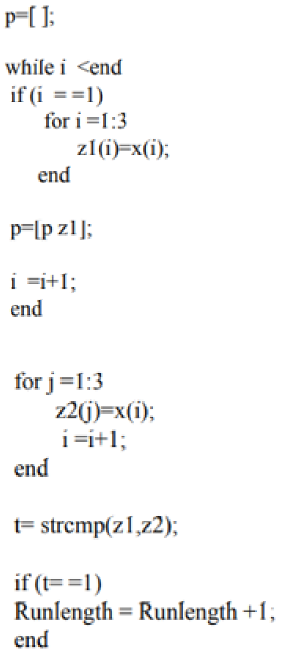


Figure 13. RLE process.

The RLE Algorithm:

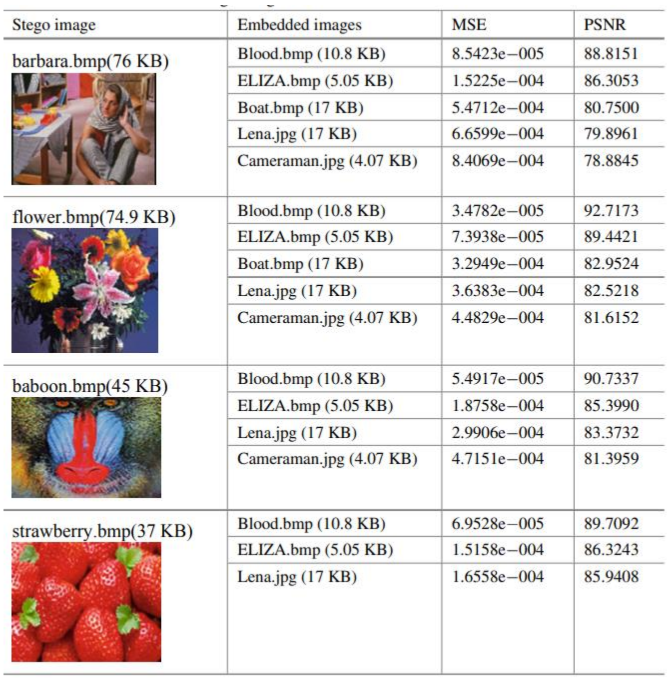


```
p=[ ];

while i  <end
 if (i  = =1)
      for i =1:3
           z1(i)=x(i);
     end

 p=[p z1];

 i  =i+1;
 end


 for j =1:3
       z2(j)=x(i);
        i =i+1;
 end

 t= strcmp(z1,z2);

 if (t= =1)
 Runlength = Runlength +1;
 end
```

Run-length encoding is applied to the secrete image M as per the described method at beginning. This compressed data M' is then hidden into cover image using LSB substitution technique to get the stego image S. At receiver, M' is obtained from stego image using suitable extraction algorithm. Finally, decoding algorithm gives secrete image M from M'.

The MSB bits of secrete images (which are to be hidden) are separated and embedded in place of LSB bits of vessel image. This modified image is known as "stego image." Later on, at the receiver side, the LSB bits of stego image are extracted and skillfully managed to get back secret image.

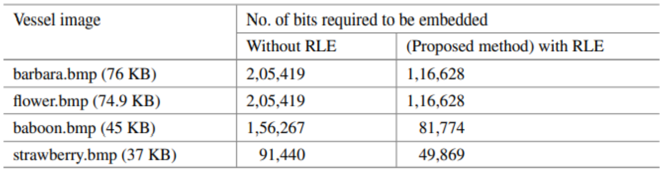
Figure 14. Secret Images



Stego image	Embedded images	MSE	PSNR
barbara.bmp(76 KB)	Blood.bmp (10.8 KB)	8.5423e−005	88.8151
	ELIZA.bmp (5.05 KB)	1.5225e−004	86.3053
	Boat.bmp (17 KB)	5.4712e−004	80.7500
	Lena.jpg (17 KB)	6.6599e−004	79.8961
	Cameraman.jpg (4.07 KB)	8.4069e−004	78.8845
flower.bmp(74.9 KB)	Blood.bmp (10.8 KB)	3.4782e−005	92.7173
	ELIZA.bmp (5.05 KB)	7.3938e−005	89.4421
	Boat.bmp (17 KB)	3.2949e−004	82.9524
	Lena.jpg (17 KB)	3.6383e−004	82.5218
	Cameraman.jpg (4.07 KB)	4.4829e−004	81.6152
baboon.bmp(45 KB)	Blood.bmp (10.8 KB)	5.4917e−005	90.7337
	ELIZA.bmp (5.05 KB)	1.8758e−004	85.3990
	Lena.jpg (17 KB)	2.9906e−004	83.3732
	Cameraman.jpg (4.07 KB)	4.7151e−004	81.3959
strawberry.bmp(37 KB)	Blood.bmp (10.8 KB)	6.9528e−005	89.7092
	ELIZA.bmp (5.05 KB)	1.5158e−004	86.3243
	Lena.jpg (17 KB)	1.6558e−004	85.9408

Figure 15. Metrics resulted from hiding secret images into cover images.

it is observed that PSNR value of stego image does not decrease much when all secret images are hidden in vessel image. Thus, the perception of stego image is very much similar to original image, and it is impossible to predict that the data might be hidden secretly.



Vessel image	No. of bits required to be embedded	
	Without RLE	(Proposed method) with RLE
barbara.bmp (76 KB)	2,05,419	1,16,628
flower.bmp (74.9 KB)	2,05,419	1,16,628
baboon.bmp (45 KB)	1,56,267	81,774
strawberry.bmp (37 KB)	91,440	49,869

Figure 16. Bits needed to embed message with/without RLE.

Fig 12. lists experimental results obtained by calculating the number of bits required to be embedded without RLE and with RLE (proposed method). There is significant decrease (almost 50%) in number of bits if we use RLE compression. This allows more images (data) to embed in vessel image which in turn increases the payload capacity of stego image [16].

4. Conclusions

In this paper, three SCI articles are reviewed comparatively, the methods and steganography techniques compared. In A Secure Image Steganography using LSB and Double XOR Operations article the authors proposed add a Double XOR cryptology algorithm before applying the Least significant bit steganography which resulted in enhancing the security of the steganography method. The PSNR value for aforementioned technique was above 40 dB, which according to the authors is an acceptable performance. In second article reviewed, the authors proposed a pixel value differencing method enhanced with Arnold scrambling algorithm. The PVD itself is more secure than LSB method and furthermore the Arnold algorithm adds up to the extra security. Guessing the number of times of scrambling is a challenging task for the intruder. In third article, LSB method summed up with Run-length encoding in order to enhance the capacity and security of the steganography technique. In this approach, more messages were able to be hid in the images comparing to the non-RLE methods. Out of these techniques, LSB with XOR method is considered to be unbreakable according the authors itself.

References

[1] "Rachael, Olomo & Misra, Sanjay & Ahuja, Ravin & Adewumi, Adewole & Ayeni, Foluso & Maskeliunas, Rytis. (2019). Image Steganography and Steganalysis Based on Least Significant Bit (LSB). 10.1007/978-3-030-30577-2_97.".

[2] A. R. K. M. Petitcolas F.A., "Petitcolas F.A., Anderson R.J., Kuhn M.G.," in *IEEE*, 1999.

[3] A. C. J. C. K. M. K. P. Cheddad, "Digital image steganography: Survey and analysis of current methods," in *Signal Processing*, pp. 727-752.

[4] W. L. B. T. S. B. M. a. H. J. Tang, "CNNbased adversarial embedding for image steganography. IEEE," *IEEE,* 2019.

[5] U. A. Hemalatha.S, "Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains," *International Journal of Advanced Information Technology,* vol. 3, no. 3, pp. 1-9, 2013.

[6] A. W. A. W. Y. I. B. I. A. T. H. K.-H. J. Mehdi Hussain, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication,* vol. Volume 65, pp. 46-66, 2018.

[7] "mathworks.com," [Online]. Available: https://www.mathworks.com/help/vision/ref/psnr.h

tml#:~:text=The%20mean%2Dsquare%20error%20(MSE,MSE%2C%20the%20lower%20the%20error..

[8] A. A. a. A. Ahmed, "A Secure Image Steganography using LSB and Double XOR," *IJCSNS International Journal of Computer Science and Network Security,* vol. 20, no. 5, 2020.

[9] H. K. S. a. S. C. Sharma, " Steganography Techniques Using Cryptography-A Review Paper," 2014.

[10] A. L. O. P. Nataliia Kukharska, "The Steganographic Approach to Data Protection Using Arnold Algorithm and the Pixel-Value Differencing Method," in *IEEE Third International Conference on Data Stream Mining & Processing*, Lviv, Ukraine, 2020.

[11] A. K. A.-D. a. I. F. J. Khalid A. Darabkh, "A New Steganographic Algorithm Based on Multi Directional PVD and Modified LSB," *Journal of Information Technology and Contro,* vol. 46, 2017.

[12] a. V. V. K. A. V. Akhmametieva, "Development of the steganographic method of embedding of additional information into the spatial domain of color images," *Informatics and Mathematical Methods in simulation,* vol. 8, pp. 110-120, 2018.

[13] P. M. M. C. A. a. S. K. M. Mishra, "Image encryption using Fibonacci-Lucas transformation," *International Journal on Cryptography and Information Security,* vol. 2, pp. 121-141, 2012.

[14] a. A. A. V. I. Arnold, Ergodic Problems in Classical Mechanics, New York: Benjamin, 1968.

[15] a. S. S. Q. Z. G. Ma, "An image cryptosystem based on general cat map," *Journal of China Institute of Communications,* vol. 24, pp. 51-57, 2003.

[16] R. Sanjay Pawar, "LSB and RLE Based Approach for Increasing Payload and Security of Stego Images," *Advances in Intelligent Systems and Computing,* no. 1133, pp. 647-658.