

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications



ISSN: 0005-1144 (Print) 1848-3380 (Online) Journal homepage: <https://www.tandfonline.com/loi/taut20>

Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods

T. D. Sairam & K. Boopathybagan

To cite this article: T. D. Sairam & K. Boopathybagan (2019) Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods, *Automatika*, 60:3, 285-293, DOI: 10.1080/00051144.2019.1579434

To link to this article: <https://doi.org/10.1080/00051144.2019.1579434>



© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 13 Jun 2019.



Submit your article to this journal [↗](#)



Article views: 328



View related articles [↗](#)



View Crossmark data [↗](#)



Computational intelligence-based steganalysis comparison for RCM-DWT and PVA-MOD methods

T. D. Sairam ^a and K. Boopathybagan^b

^aDepartment of Electronics and Communication Engineering, SKR Engineering College, Nazarath Pettai, Chennai, Tamil Nadu, India;

^bDepartment of Electronics Engineering, Anna University, MIT Campus, Chromepet, Chennai, Tamilnadu, India

ABSTRACT

This research article proposes data hiding technique for improving the data hiding procedure and securing the data transmission with the help of contrast mapping technique along with advanced data encryption standard. High data hiding capacity, image quality and security are the measures of steganography. Of these three measures, number of bits that can be hidden in a single cover pixel, bits per pixel (bpp), is very important and many researchers are working to improve the bpp. We propose an improved high capacity data hiding method that maintains the acceptable image quality that is more than 30 dB and improves the embedding capacity higher than that of the methods proposed in recent years. The method proposed in this paper uses notational system and achieves higher embedding rate of 4 bpp and also maintain the good visual quality. To measure the efficiency of the proposed information hiding methodology, a simulation system was developed with some of impairments caused by a communication system. PSNR (Peak Signal to Noise ratio) is used to verify the robustness of the images. The proposed research work is verified in accordance to noise analysis. To evaluate the defencing performance during attack RS steganalysis is used.

ARTICLE HISTORY

Received 28 October 2018

Accepted 2 February 2019

KEYWORDS

AES; DES; stenographic; steganalysis; PSNR; PVD; RCM_DWT and PVA_MOD

1. Introduction

The pixel value differencing method has been found to exhibit efficiency in terms of embedding the secret contents in digital images. This method also excels in portraying minimum artifacts in the cover images as far as human visualization is considered, therefore the method stands ahead in exhibiting good encoding ranges [1]. Internet today is viewed as the backbone of communication; with rapid expansion in the communication arena safety of the transmitted contents always stands as a question. Measures to protect the secrecy of such contents must be standardized appropriately. Steganography is observed as one of the technique that can be suitably incorporated for concealing the secret data contents. Unauthorized access of the secret contents can be prevented in this method by encoding the contents into an invariably different medium [2]. This method also enables the user to encode the contents suitably as per the requirements before transforming the same into another medium, this way enhanced security levels can be achieved. As far as covered media is concerned different forms of encoding strategies have been developed in this Steganography technique. The traditional strategy prevalent so far for the covered media is the digital images [3].

Encoding secret contents into images is not an easy task as it relies on the transformation of the existing

redundant bits of the concerned images. Modification or transformation of the redundant bits would lead to certain distortions that would remain subtle to the human eyes; one such is the disruption of the media related properties [4]. The ultimate objective of the Steganalysis strategy is to determine the encoding architecture, as whether the concerned objects are encoded with data contents or not. The objective or focus of this paper can be categorized into two different strategies: The very first strategy would be to determine the encoding efficiency of various available techniques in comparison with the Steganalysis technique, the second strategy would be to analyse the performance levels of the Steganalysis technique with respect to the image properties. Certain factors such as Security, Capacity and Robustness have been found to disturb the quality and utility of Steganography. The strength of a Steganography technique lies in the inability of an attacker in hacking the confidential contents. Storage capacity of an image is assessed by verifying the total amount of contents that can be encoded into it. Exhibiting strong immunity against attacks is considered as the robustness of the concerned stegno medium [5].

2. Steganalysis

Identification of confidential contents inside images is not an easy task as it requires specialized techniques for

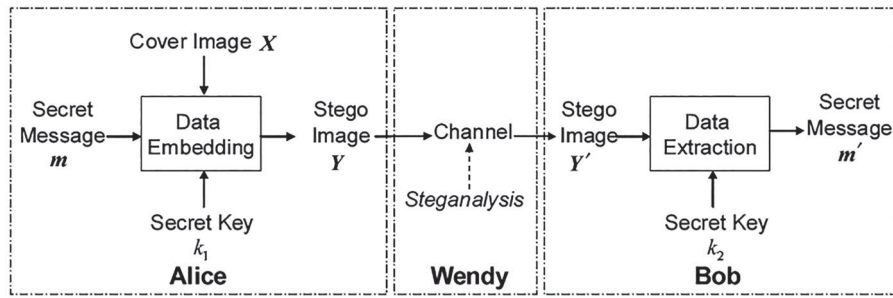


Figure 1. The model of steganography and steganalysis.

the determination of the same. Various stages must be broken down in order to get into the inner encoded zones [6]. A cover in the form of text or image is preferably utilized for the purpose of concealing the confidential contents. Various statistical properties of the concerned cover images pave way for the breaking process due to its vulnerability, such as that of the histogram analysis [7–9], chi-square test and universal detectors [1]. Certain Steganography algorithms have been identified and introduced for the purpose of encoding data in digital images irrespective of their domains, namely the spatial and frequency domains. Few techniques such as detection destruction, extraction, or transformation have been considered as the Steganalysis practices involved in the Steganography strategy attacks [10]. It is important to understand about the various available strategies that can be incorporated by the attackers to access the confidential contents, it is this knowledge that can assist the user in designing a highly strong Steganography system shown in Figure 1. A Steganography system that exhibits increased immunity against the offenses is considered to be the most superior kind of system [11]. Identifying the presence of secret contents inside the cover images is considered to be the ultimate aim of the Steganalysis process. Cover images are usually preferred for the encoding process. Revealing the presence of the secret contents turns out to be the task of Steganalysis.

Encoding confidential contents inside the cover images is not an easy task as it requires complete understanding and knowledge about the concerned cover images; hence Steganalysis is considered as a very challenging field [5].

Steganographic techniques retains the secrecy of communication on creating stego images using concealment function. The weakness of secret data hiding is when the attacker suspect the existence of hidden image. The hidden image must be invisible both perpetually and statistically. The stegenography technique is suitable when no difference is between cover and stego file, i.e. the characteristics and attributes of cover file are not changed while embedding and no distortions is shown in the result. Thus the steganographic system is imperceptible.

Steganographic systems aim to maximize the steganographic capacity which is number of bits embedded in cover file. Regarding robustness, as most of the steganographic system use network and internet channels that cause no degradation, robustness is not an issue in priority to stegano techniques whereas watermark is robust system.

The main aim of steganography is to increase capacity and imperceptibility which is not possible to achieve simultaneously. This is because there must be tradeoff between amount of embedding information, artefacts introduced in cover. Therefore, the technique has to balance according to the requirement. The proposed work focus on the same requirement.

2.1. Various fields relying on steganalysis for their real time application

- (1) Medical Field
- (2) Terrorism
- (3) Hacking
- (4) Intellectual property offenses
- (5) Corporate espionage
- (6) Watermarking
- (7) Indexing of video mail
- (8) Military application
- (9) Automatic monitoring of radio advertisements

2.2. Classification of steganalysis

Steganalysis is classified into two different types:

- (1) Signature Steganalysis
- (2) Statistical Steganalysis

The Signature Steganalysis scheme can be classified into two categories is shown in Figure 2:

- (1) Specific Steganalysis
- (2) Universal Steganalysis

Specific Steganalysis techniques adopt the strategy of first analyzing the inbuilt encoding operation followed by which the obtained knowledge would be utilized for

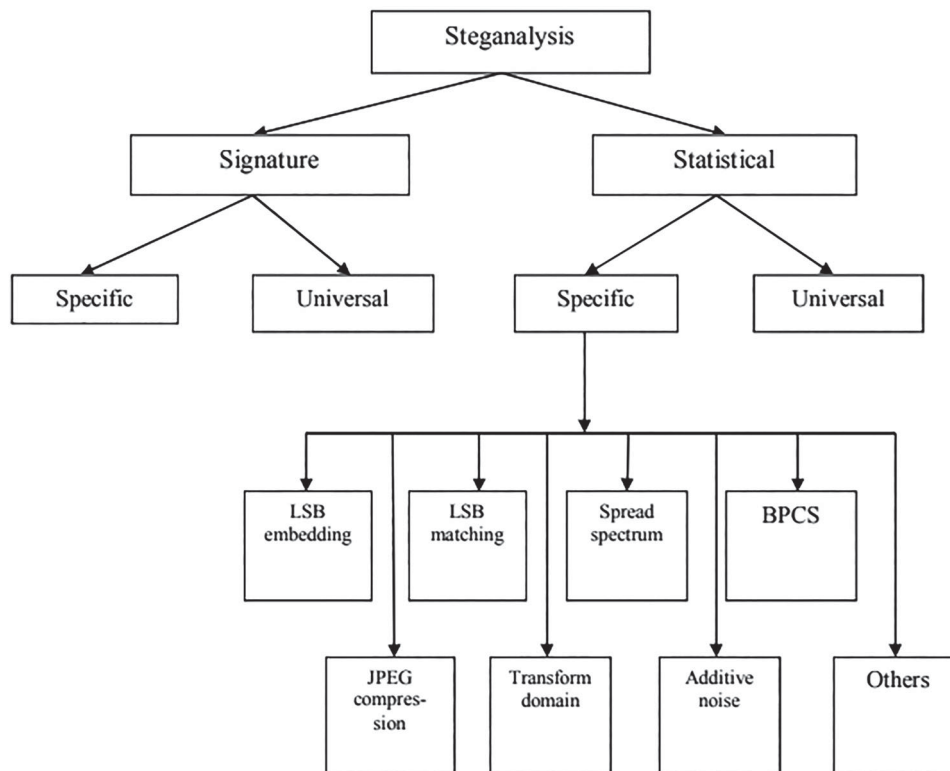


Figure 2. Classification of steganalysis.

the purpose of understanding the image properties that have been transformed during the encoding process. Certain specialized Steganalysis techniques would rely on the in-depth knowledge of the concerned concealing strategy. Acquiring increased levels of knowledge about the encoding technique would result in accurate decisions [5].

Universal Steganalysis strategy [6] functions as an individual scheme without depending on the Steganography algorithm. Comparison of the universal method with the specific method reveals that the specific method performs better than the universal method. Even though the performance of this method is found to be inferior it never ends up in meaningless results hence it can be very well preferred as a common solution for certain practical applications.

One of the Steganalysis processes that differentiate the cover images from the secret images is the Passive Steganalysis process. On the other the active form of Steganalysis strategy removes the secret contents from the concerned cover images [12].

The Steganalysis strategy is classified into the following five categories [10]: stego-only, known cover, known message, chosen stego, and chosen message. The stego-only attack performs its analysis with the help of the available stego-image. Functioning of this offense is found to be similar to that of the cipher text only attack and it is considered to be a vulnerable form of attack. As far as the known cover attack is concerned it is observed that it incorporates both the original cover and a corresponding stego-image [13]. This offense commences

when the Steganalyst becomes aware of the secret message that is encoded in a stego-image. Availability of the message removal tool is the case witnessed in the chosen-stego attack, this makes it easier for the attacker to decode the cover image and thereby access the secret contents without the need of an encoding algorithm. This offense is therefore considered as the most powerful offense as the tool box is readily available and easily accessible.

2.3. Classification of the steganalysis strategies based on the detection of the secret contents [14]

- (1) Statistical Steganalysis.
 - (a) Spatial domain.
 - (b) Transform domain.
- (2) Feature based Steganalysis

Statistical steganalysis

This method makes use of the image pixels for the purpose of identifying the confidential contents.

In the spatial domain type of statistical Steganalysis strategy the difference between the selected pair of pixels is considered for the detection process, followed by which the difference between them is suitably evaluated. Selection of the pixel pairs can be done in many ways; one such is the selection of any two neighbouring pixels. Selection of the neighbouring pixels can be done either inside a single block or across two different blocks. Once the evaluation process is

completed the obtained values can be used for plotting the corresponding histograms, it is these plotted histograms that reveal the confidential contents [15].

The transform domain technique when applied to the image, the transform is based on orthogonal transformation of two components, magnitude and phase. The magnitude is the frequency content of the image and phase is used to restore the image back to spatial domain.

The image is enhanced on computing the 2D discrete transform of the image.

The frequency counts of the corresponding coefficients are evaluated followed by the commencement of the histogram analysis. Histogram analysis assists in the determination of the difference between the cover and stego images.

The following three approaches are basic types of transform domain approach

- (a) Wavelet Transform
- (b) Fourier Transform
- (c) Cosine Transform

Since the transform is performed on frequency content, the high frequency content such as edges can be easily enhanced. The noticeable drawback of this method is the absence of encoding algorithms. This problem can be alleviated by carefully choosing suitable feature based Steganalysis strategies [16].

Feature-based steganalysis

This technique follows the strategy of suitably selecting and retaining the relevant feature based image information's. These extracted features thus assist in the determination of the hidden confidential contents, further these features can also be used for training the classifiers.

Few statistical Steganalysis of Steganography and watermarking are as follows [17,18]:

- (1) Histogram analysis
- (2) Chi-Square Attacks
- (3) RS Steganalysis
- (4) LSB embedding
- (5) LSB matching Pixel-pair analysis
- (6) Bit plane analysis
- (7) JPEG compression

Identification of various attacks based on the noise analysis and RS Steganalysis strategies was performed by Jiri Fridrich et al, where he developed a Steganalysis technique with respect the above based mentioned idea for the detection of LSB encoding in colour and gray scale images [14]. This strategy can be used for concealing lossless type of data in LSBs. Randomizing these LSBs would minimize this concealing capacity. Image determination would be done on the basis of

the defined Regular groups (R) and Singular groups (S) of pixels based on their specific properties. The levels of the implemented encoding can be determined by analysing the relative frequencies of the selected pixels in the concerned image, further the LSBs of both the original and the obtained images can be flipped and then randomized for predicting the encoding levels [18].

With reference to the dual statistics obtained from spatial correlations in images Fridrich et al, further introduced a Steganalysis technique for determining hidden messages embedded inside colour images and gray images that are suitably named as RS Steganalysis. In this method it is observed that the stego image is classified into three different disjoint groups. Adjacent pixels of the images are considered for the determination of the noise levels, where the absolute mean value of the differences between these adjacent pixels are utilized for the evaluation process. A mask is suitably adopted for the purpose of flipping the LSBs of a fixed set of pixels in each group [19]. The observed pixel noise can either be increased or decreased with respect to the flipping operation and this property is effectively utilized for grouping or classifying the pixels into various groups such as that of the "regular" or "singular" groups. Theoretical analysis of this property would assist in the determination of the quantity of confidential contents that can be encoded by the LSB method, Formation of the quadratic curves depends on the proportion of both the regular and singular groups. Comparison of the RS Steganalysis and Chi-square attack reveals that the RS Steganalysis method is more reliable. The percentage of pixels would also determine the identification ability; if it is less than 0.005 bits per pixel then the method would be unable to perform the detection process [17].

3. Image noise

Degradation in an image signal is considered as Noise, this degradation is caused by external disturbance during the transmission of the image from one place to another via Satellite, Wireless, and Network cable [20].

Types of image noise:

- (1) Salt and Pepper Noise
- (2) Gaussian Noise
- (3) Speckle Noise
- (4) Periodic Noise

Salt and pepper noise: This type of noise is also called as the Impulse Noise. Certain sharp and sudden disturbances cause this noise. The appearance of this image can be determined by monitoring its scattered appearance usually in the form of pixels, either in white or black colours over the corresponding images [21].

Gaussian noise: Digital images can be affected by Gaussian noise which is a statistical noise expressed as Gaussian distribution function.

This noise is usually caused by certain random fluctuations in the image signal. Modelling of this noise is done by appending random values to the image [22].

Speckle noise: This type of noise is obtained by multiplying pixel values of an image to certain random values. The noticeable undesirable effects produced by this noise are artifacts, unrealistic edges, unseen lines, corners, blurred objects and disturbs background scenes.

Probability density function (PDF) or Histogram can be incorporated designing and characterizing the noise models. Below are few noise models, their types and categories in digital images [23].

Periodic noise: A common source of periodic noise in an image is from electrical or electromechanical interference during the image capturing process. In a video stream, periodic noise is typically caused by the presence of electrical or electromechanical interference during video acquisition or transmission.

3.1. Gaussian noise model

The Gaussian noise appears commonly on images from natural sources.

The other name for Gaussian noise model is statistical noise model. The characteristic of this noise model is that it possesses Probability density function (PDF) that is equal to that of the normal distribution, which is also termed as the Gaussian distribution. The most common name used for this noise model is the additive white Gaussian noise. The function of this noise model is that it involves in the distribution of gray values in digital images. It is because of the above mentioned function this Gaussian noise model is essentially designed and characterized by its PDF with respect to the gray values [24].

The PDF (Probability density function) of a Gaussian random variable Z is expressed as follows,

$$p(z) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(z-\bar{z})^2}{2\sigma^2}},$$

where Z denotes the grey level, \bar{z} represents the mean value and σ denotes the standard deviation and its square is variance.

Gaussian noise in digital image can be reduced using spatial filter even an undesirable outcome results in blurring of edges when smoothing an image. Generally Gaussian noise mathematical model gives correct approximation of real images.

3.2. Impulse valued noise

This noise is called as the salt and pepper noise. Another name commonly used for representing this noise is the data drop noise as this noise involves in statistically

dropping the original data values. As far as this noise is concerned it involves in the modification of few pixel values in the image. Noise pulses are usually witnessed during the data transmission process. Noise intrusion usually encounters by replacing the original pixel values by corrupted pixel values either in the maximum “or” minimum pixel value range, i.e. 255 “or” 0 respectively, when the number of pixels counts to 8 during the transmission process then the noise pulses would be inserted in the dead pixels either in the dark or bright coloured pixels. These dead pixels appear due to the presence of errors in the analog to digital conversions and errors that encounter during the bit transmission. The pixel metrics in this type is determined by estimating the percentage of noisy pixels.

Salt and pepper noise is also known as bipolar impulse model. As far as the Salt and pepper noise is concerned it is identified as an impulse type of noise, therefore it is also referred to as the intensity spikes. Spikes are produced due to the encountered errors in the data transmission process. The observed probability is observed to be typically less than 0.1. The image of this salt and pepper noise is due to the alternating minimum or maximum values, giving it the required appearance. Malfunctioning of the pixel elements in the camera sensors and memory is the reason for the salt and pepper noise.

The PDF of the bipolar impulse noise model is expressed as follows:

In above expression, z is pixel intensity value in noisy image. If $b > a$, then the grey-level b appears as a light dot (salt) in the image, else a as dark dot (pepper) would appear. If either P_a , P_b is zero, then the PDF appears to be unipolar. The a and b are saturated values with positive impulse resulting in white and negative impulse resulting in black

4. Steganalysis evaluation against the proposed RCM_DWT and PVA_MOD strategies

Criteria for steganalysis

The main goal of Steganalysis is to identify whether or not a suspected medium is embedded with secret data, in other words, to determine the testing medium belong to the cover class or the stego class. If a certain steganalytic method is used to steganalyze a suspicious medium, there are four possible resultant situations.

True positive (TP): meaning that a stego medium is correctly classified as stego.

False negative (FN): meaning that a stego medium is wrongly classified as cover.

True negative (TN): meaning that a cover medium is correctly classified as cover.

False positive (FP): meaning that a cover medium is wrongly classified as stego.

Table 1. Comparison of PSNR of embedded secret image to extracted secret image on using Gaussian noise attack with $P = 0.99$.



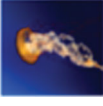





Target image	Secret image	PSNR(Embedded before attack)	Gaussian noise	PSNR (Extracted after attack)	Error ratio (degraded % appr)
		28.2567	mean 0variance 0.01	27.5181	Correct = 97% Error = 3%
		28.6441	mean 0variance 0.1	27.2340	Correct = 95% Error = 5%

Table 2. Comparison of PSNR of embedded secret image to extracted secret image on using salt and pepper noise with $p = 0.99$.

Target image	Secret image	PSNR(Embedded before attack)	Salt and pepper noise	PSNR(Extracted after attack)	Error ratio (degraded % appr)
		28.2567	Density0.05	27.5373	Correct = 95% Error = 5%
		28.6441	Density0.5	27.0578	Correct = 94% Error = 6%

Reversible contrast mapping and discrete wavelet transform are the strategies incorporated by the proposed method, these strategies are used for the encoding process in both the spatial and frequency domains. Reversible mapping and wavelet transform techniques are utilized in the initial phase for creating the mosaic images. The next step is to encrypt and decrypt these mosaic images using the Advanced Encryption Standard. The Steganalysis of the Gaussian noise and the salt and pepper noise is evaluated for two standard images of size (512×512) after suitable encryption using the RCM-DWT techniques. The corresponding image and PSNR values are portrayed in Tables 1 and 2 respectively.

From the table of Gaussian and salt –pepper the resultant image after the noise attack is degraded approximately by 3–5% for Gaussian noise varying variance and by 5% -6% for salt and pepper noise of density parameter respectively which means the algorithm is robust to the subjected noise.

4.1. Security of the pixel value techniques

Various techniques have been proposed for the safety of the PVD and Modulus PVD methods respectively [1,25]:

Wang et al introduced a PVD model incorporating a modulus function Steganography strategy in order to increase the standard and quality of the concerned image by minimizing the difference between the pixel pairs before and after the encoding process. The strategy adopted here was to transform the corresponding pixel pairs rather than utilizing their difference values. It was observed that the PSNR value of this method was

higher than that of the original PVD method. Readjusting conditions were adopted in this strategy in order to solve the falling-off boundary problem when the pixel exceeds the value of 255 after the completion of the data encoding process.

The following steps would briefly describe the modulus PVD technique:

- (1) The initial step would be to determine the difference between the consecutive pixels that appear similar to the original PVD assisting in the identification of the range within which the difference value falls.
- (2) The second step would be to compute the remainder value using the following expression:

$$F_{rem(i)} = (P_i + P_{i+1}) \bmod t'_i \quad (1)$$

where $t'_i = 2^{t_i}$ and t_i is the hiding capacity of the pixel block.

- (3) The final step would be to encode the n secret bits into the corresponding pixel blocks in such a way that appears to be equivalent to the decimal value b that is further equal to F_{rem} .

A specialized technique has been proposed in order to maintain the difference in the same range both before and after the encoding process so as to alter the remainder of the pixel-pair. Apart from the mentioned enhancements of the PVD with a modulus function, it is found that it produces a certain number of artifacts, such as abnormal enhancements and fluctuations in the PVD histogram, which can be incorporated for the purpose of exposing the presence of the confidential contents [21].

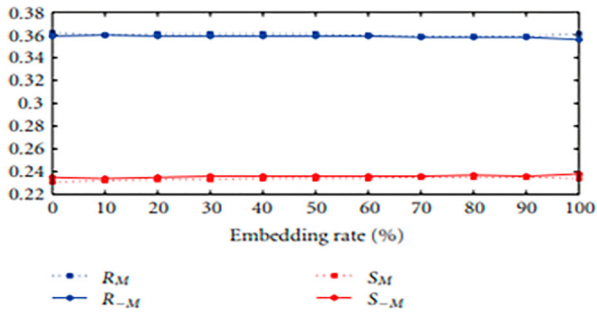


Figure 3. RS analysis for the image Lena (512 × 512) using the pixel value adjustment with mod operation for each embedding rate.

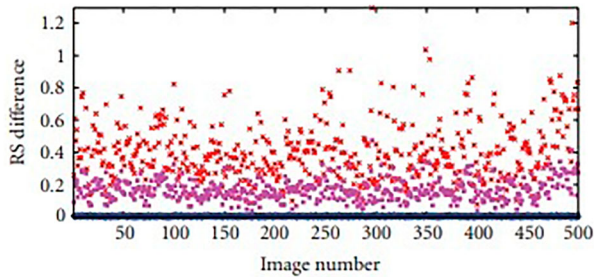


Figure 4. RS detection value for the image LENA.

5. RS Steganalysis strategy for the proposed RCM_DWT and PVA_MOD methods

5.1. RS steganalysis technique

This technique is based on the assumption that a cover image consists of $M \times N$ pixels, where the pixel values are extracted from the set P . The range of an 8 bit grey scale image is given as $P = \{0 \dots 255\}$. Segregating the image into disjoint groups is considered as the initial step of the lossless encoding process, it is therefore grouped into n number of adjacent pixels, as $(x_1 \dots x_n)$, Selection of the pixels can be made in a row, where a defined set of consecutive pixels would be selected, for instance it can be a group of $n = 4$ pixels. This followed by the assignment of a discrimination function f , that is meant for a real number $f(x_1 \dots x_n)$ E, R for each of the pixel groups $G = (x_1 \dots X_n)$. Defining a discrimination function is to capture the smoothness or regularity property of a certain group of pixels, namely G . The noise factor would always determine the value of the discrimination function, the more it is in the group of pixels $G = (x_1 \dots X_n)$, the higher would be the value of the discrimination function. The discrimination function in a given set of pixels is thus expressed as follows:

$$f(x_1, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

Certain image models or statistical assumptions about the cover image would assist in the design process of the various discrimination functions. This ultimately

leads to an invertible operation F on P , suitably termed as the Flipping process. Flipping is otherwise defined as the permutation of grey levels. The permutation of $F1: 0 \dots 1, 2 \dots 3 \dots 254 \dots 255$ denote the flipping (negating) of the LSB corresponding to the gray levels. Shifted LSB flipping F_1 is expressed as $-1 \dots 0, 1 \dots 2, 3 \dots 4 \dots 253 \dots 254$. $F0$ is termed as the identity permutation that involves in the mapping process of the pixel onto itself.

Three different pixel groups have been defined on the basis of the discrimination function f and the flipping operation F ; they are as follows, Regular (R), Singular (S), and Unusable (U),

$$\begin{aligned} G \in R &\Leftrightarrow f(F(G)) > f(G) \\ G \in S &\Leftrightarrow f(F(G)) < f(G) \\ G \in U &\Leftrightarrow f(F(G)) = f(G) \end{aligned}$$

Here $F(G)$ denotes the application of the flipping function F to the components of a vector $G = (x_1 \dots x_n)$. Considering a group G it can be observed that different flipping can be applied to different pixels that can be essentially defined using a mask Jvl . The mask Mis and n -tuple have been found to comprise of values $-1, 0$, and 1 . The flipped group is thus denoted as $F(G)$, beneath the mask Mis is defined as $(FM(1)(x_1), FM(2)(x_2) \dots FM(n)(x_n))$. The function of the Flipping process is to perturb the pixel values in an invertible way by small amounts, which resembles the simulation act of invertible noise addition. Enhancement in the discrimination function can be observed by means of appending small volumes of noise, this will never tend to minimize the discrimination value either. The above strategy would result in an increased number of regular groups rather than the singular groups. Here, RM represents a relative number of regular groups in percentage for a mask NI . SM represents a relative number of singular groups. RS method

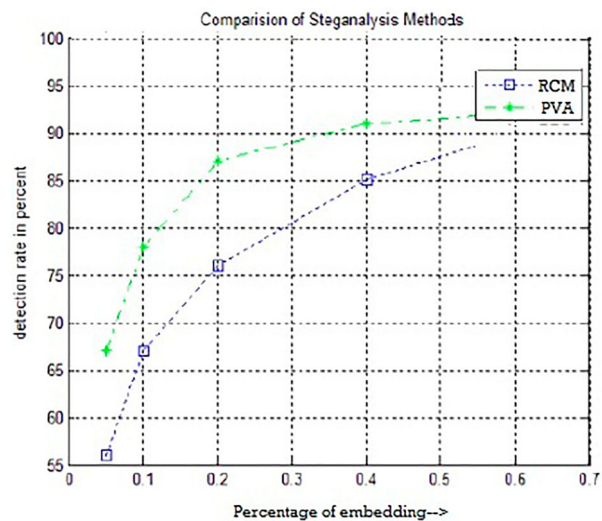


Figure 5. Error in the length estimation by the RS steganalysis incorporating both the methods.

is based on the hypothesis strategy than the one that is represented in a typical cover image; the expression is as follows,

$$R_M \approx R_{-M} \text{ and } S_M \approx S_{-M}$$

Flipping operation F_1 is observed to be similar to the process of applying F_1 to an image, the corresponding image experiences colours shifts by one. Significant absence of reasons for the modification in the number of R and S with respect to the colour shifts beforehand has been observed.

With respect to certain extensive experimental evidences they state that the above equation holds very accurately for various types of images. Flipping of the LSBs of the pixels in the corresponding images is the function of the replacement Steganography. The other observed functionality is the encoding of the random bit sequence of length $p\%$ (in percent of pixels) that flips $p/2\%$ of pixels. The variation between the R_M and S_M is due to the randomization of the LSB plane, it is found that the value decreases as the length p of the concerned encoded content enhances. An equivalent status is observed when 50 percent of the pixels are flipped. Extensive experimental evidences portraying the modelling process of the R_M and S_M curves with linear equations and second degree polynomials have been found.

It is found that the point of intersection of the curves R_M and R_{-M} possess the same x coordinate as the point of intersection for the curves S_M and S_{-M}

The hidden message length p is therefore evaluated from the value x using the equation,

$$p = \frac{x}{x - \frac{1}{2}}$$

where x represents the x -coordinate respectively.

Five standard test images of size 512×512 have been selected. The proposed two methods are thus applied to the corresponding images possessing a pixel insertion rate in the ratio of $p = 0, 10\%, 20\% \dots, 90\%$. In the experiments, we have incorporated 0110 and $0-1-10$ as M and $-M$, respectively.

The proposed method has been found to be much more secure than the RS-analysis, in common with the other PVD methods, where x denotes the x -coordinate.

It is clear from the above RS-diagram shown in Figure 3–5 of our method that the stego images do not comprise of any of the encoded data in their LSBs as their relative values of percentages R_M and S_M seems to be invariant with respect to the increasing encoding capacity. It is this strategy that proves the security aspect of the Steganography method from the viewpoint of the corresponding dual statistics method. It is also evident that in the PVA-MOD method, the modulus operator utilized for the concealing process acts as a mean in order to generate random locations for the encoding

process, increase in the effects by means of a relative increase in the number of bit planes prove that this method is better than the RCM-DCT. The simulation results run on several images further prove that the LSB approach is very useful for increased payloads that can be encoded within the bmp images [26]. Determination of statistics in the frequency domain is thus prevented by the transform domain techniques, as they do not support increased payloads like the LSB method, due to the constraints such as hiding within the concerned coefficients.

6. Conclusion

In the proposed research work, the stego images do not compromise with encoded information in LSB, since the R_M and S_M relative value percentage looks like invariant in nature, which improves the encoding efficiency in steganography. The proposed strategy assure the security by using dual statistics method, the results of the system showed as evidence in a PVA-MOD method, where concealing process utilizes the modulus operator that acts as mean to generate random locations during encoding. Comparing with the relative increase in some bit planes the proposed methodology works better than RCM-DCT. The experimental results were achieved by using simulator tools, the results of the system were runs on several images simultaneously to compare and justify the LSB approach is better when compared to payload adjustments. The statistics evaluation in the frequency domain is restricted by transform domain methods. Also, it does not support the increased payload. The proposed research work RCM-DCT is efficient to gaussian and salt & pepper noise attacks compared to other algorithms. The effect of salt & pepper noise is greatly reduced by proper selection variations and density learning rate. Results are compared by using the parameter called PSNR (Peak Signal to Noise Ratio) of different images. Greater the PSNR value implies more robust is the technique against attack. Based on the results achieved, the error rate of approximately 3% to 6% for both the gaussian and salt-pepper noise is proved to be the best candidate for the digital image embedding, since its having greater PSNR value even after the noise technique.

The work can be extended in framing an objective that measure the quality of the system based on reliability of stego image results which is still a challenge. Additionally, the future direction of the research can be in involving the features of cover and stego image and the relation between them to increase the quality.

Thus, designing or finding out an objective image quality measure that can predict the perceived quality and provide reliable results with stego images still represent a challenge. Additionally, the reliability of other available methods of objective measures can be tested and examined with stego images.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

T. D. Sairam  <http://orcid.org/0000-0001-9165-6061>

References

- [1] El-Alfy E-SM, Al-Sadi AA. Pixel-Value Differencing Steganography: Attacks and Improvements, ICCIT 2012.
- [2] Fridrich J, Goljan M, Du R. Reliable detection of LSB Steganography in grayscale and color images, Proceeding of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, 2001, pp. 27–30.
- [3] Chu R, You X, Kong X, et al. A DCT-based image steganographic method Resisting statistical attacks. ICASSP, Montreal, Que., Canada; 2004, pp. V–953.
- [4] Kaur P, Singh J. A Study on the effect of Gaussian noise on PSNR value for digital images. *Int J Comput Electric Eng.* 2011;3(2):1793–8163.
- [5] Kharrazi M, Sencar HT. Performance study of common image steganography and steganalysis techniques. *J Electron Imaging.* 2006;15(4):041101–16.
- [6] Joo J-C, Lee H-Y, Lee H-K. Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function, Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing 2010, Article ID 249826, 13 pages.
- [7] Lerch-Hostalot D, Megías D. Steganalytic methods for the detection of histogram shifting data hiding schemes, 2013.
- [8] Joo J-C, Lee H-Y, Lee H-K. Improved Steganographic Method Preserving pixel-value differencing histogram with Modulus function. *EURASIP J Adv Signal Process.* 2013;2010:1–13.
- [9] Jung K-H. Comparative histogram analysis of LSB-based image Steganography. *WSEAS Trans Syst Control.* 2018;13:103–112.
- [10] Lin E, Delp E. A Review of data hiding in digital images. CERIAS Tech Report. 1999;299:274–278.
- [11] Kaur M, Kaur G. Review of Various Steganalysis Techniques, Manveer Kaur, et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1744-1747.
- [12] Rajkumar P, Kar R, Bhattacharjee AK, et al. A Comparative analysis of steganographic data hiding within digital images. *Int J Comput Appl.* 2012;53:1–6.
- [13] Chen Y-S, Wang R-Z, Lee Y-K, et al. Steganalysis of Reversible Contrast Mapping Watermarking, Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008.
- [14] Mařcal ARS, Patricia R, Pereira A. Steganographic Method for Digital Images Robust to RS Steganalysis, ICIAR 2005, LNCS 3656, pp. 1192.
- [15] Coltuc D, Chassery J-M. Very Fast watermarking by Reversible contrast mapping. *IEEE Signal Process Lett.* 2007;14(4):255–258.
- [16] Voyatzis G, Nikolaidis N, Pitas I. Digital watermarking: An overview. *EUSIPCO.* 1998;1:9–12.
- [17] Nallagarla R, Varadarajan S. Effect of various attacks on Watermarked images. *Int J Comput Sci Inf Technol.* 2012;3:3582–3587.
- [18] Verma HK, Singh AN, Kumar R. Robustness of the digital image watermarking techniques against Brightness and Rotation attack. *Int J Comput Sci Inf Security.* 2009;5.
- [19] Chauhan N, Wao AA, Patheja PS. Attack detection in Watermarked images with PSNR and RGB intensity. *Int J Adv Comput Res.* 2013;3(9):41–45.
- [20] Bhosale N, Manza R, Kale KV. Analysis of effect of Gaussian, salt and pepper noise removal from noisy Remote Sensing images. *Emerg Res Comput Inf Commun Appl.* 2016:386–390.
- [21] Fridrich J, Goljan M, Hoge D, et al. Quantitative steganalysis of digital images: estimating the secret message length. *Multimedia Syst.* 2003;9(3):288–302.
- [22] Westfeld A, Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned.
- [23] Srinivas R, Panda S. Performance analysis of various Filters for image noise removal in different noise Environment. *Int J Adv Comput Res.* 2013;3:47–52.
- [24] Jena SK, Krishna GVV. Blind Steganalysis: estimation of hidden message length. *Int J Comput Commun Control.* 2007;II:149–158.
- [25] Nagaraj V, Vijayalakshmi V, Zayaraz G. Color image Steganography based on pixel value modification method using modulus function. *Int Conf Electron Eng Comput Sci.* 2013;4:17–24.
- [26] Molaei AM, Sedaaghi MH, Ebrahimnezhad H. Steganography scheme based on Reed-Muller Code with improving payload and ability to Retrieval of Destroyed data for digital images. *AUT J Electric Eng.* 2017;1:53–62.