A Pioneer Image Steganography Method Using the SOD Algorithm

Pabak Indu, Sabyasachi Samanta, and Souvik Bhattacharyya

Abstract Steganography is a technology that has gained popularity in recent years as people's fears and susceptibilities have increased in today's digital environment. As a result of this work, we have shed light on the existing popular techniques of Image Steganography in great detail, and we have also demonstrated a new Spatial Domain Image Steganography technique based on the 'SOD'—Sum-Of-Digit method, wherein secret data is embedded in an image through the use of the proposed algorithm. Moreover, the presented method is compared with existing methodologies on a variety of parameters and found to be efficient and robust, which makes this steganography technique effective. The experimental results can demonstrate the effectiveness and accuracy of the proposed technique in terms of several image similarity metrics, which is a significant benefit.

Keywords Sum of Digits · Spatial method · Steganalysis · Steganography · Ensemble · SRM

1 Introduction

Technological advancements are substantial, and nothing appears to be preventing even our most secret information from falling into the wrong hands. However, our efforts in the field of Cyber-Security have not slowed down when it comes to preventing the breach of personal information. The protection of sensitive information has been a long-standing concern for millennia, and as a result, we have

P. Indu (✉)
Department of Computer Science and Engineering, Adamas University, Kolkata, West Bengal, India
e-mail: pabakindu@yahoo.co.in

S. Samanta
Haldia Institute of Technology, Haldia, West Bengal, India

S. Bhattacharyya
Department of Computer Science and Engineering, University Institute of Technology, University of Burdwan, Burdwan, West Bengal, India

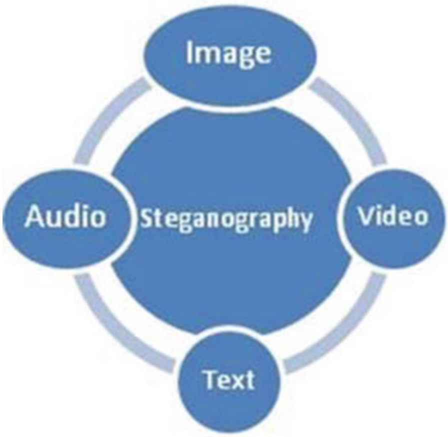
S. Bhattacharyya et al. (eds.), *Intelligent Systems and Human Machine Collaboration*, Lecture Notes in Electrical Engineering 985,
https://doi.org/10.1007/978-981-19-8477-8_10

continually developed new concepts and strategies to ensure that this information is not compromised as it is transferred from one location to another. Cryptography, Steganography, and watermarking are some of the techniques that are currently in widespread usage. Encryption is a cryptographic technique that takes a message and causes disorder in it or scrambles its arrangement, resulting in a cypher text, and the process is referred to as Encoding. This type of information can only be decoded with the use of a secret key, and the process of obtaining the information is referred to as Decryption. The opponent is aware of the concealed secret information contained within the cypher, and the likelihood of it being deciphered is quite high as a result. In order to protect intellectual property rights in data, watermarking must be used, either with or without the suppression of the presence of communication [1]. Steganography, on the other hand, is intended to conceal the very presence of communication and secret data.

For the past several decades, image steganography has piqued the curiosity of a large number of scientists and academics. If a secret message is intercepted, the primary purpose of image steganography is to conceal the existence of the secret message in order to avoid discovery even if it is discovered. This is accomplished by embedding the secret message inside an innocent cover object (text, audio, video, and picture), which creates the stego object, and then transferring it to the desired destination over a public channel. It is possible that a purposeful or inadvertent obstacle will occur during the transmission process, preventing the message from being correctly transmitted. An optimal steganography strategy should be created in order to preserve an impenetrable stego image, as shown in Fig. 1. The following literatures have a variety of steganography schemes to choose from [2–11]. When it comes to the extraction of these hidden facts, this process is referred to as steganalysis. Almost identical to the steganography idea, with the primary distinction being that it is really a reversed version of the steganography technique.

It is the objective of this research to examine a specific spatial domain picture steganography approach in further detail. Steganalysis is something we come upon

Fig. 1 Types of steganography



later on. Instead of concealing data, steganography is a procedure for detecting hidden data, in which the concealed data is recognised from its cover source, as opposed to steganography. Further, the suggested article is separated into a number of different sections. This paper is divided into five sections: Sect. 2 contains a literature survey on existing models, Sect. 3 describes the proposed model, including an overview of the embedding and extraction algorithms, Sect. 4 presents experimental results on various test images and their corresponding benchmark images, and also compares it with some existing models, and Sect. 5 elaborates the steganalysis results on various image datasets, including comparisons with other models. and concludes with a summary of the proposed paper, which is presented in the form of a conclusion.

2 Review on Existing Methods

Generally, image steganography may be divided into two categories: spatial steganography and transform steganography. The majority of the surveys [12] are concerned with the overall topic of picture steganography. This section discussed well-known picture steganography approaches in the spatial domain that have been utilised in recent years, as well as the emergence of adaptive steganography techniques.

For the most part, this is the most straightforward and well-known option: the least significant bit (LSB) approach, in which data is concealed directly inside the LSB of the pixel values. The development of steganographic technologies necessitated the use of many versions of the existing LSB approach in various bit planes as time went by. Others include adaptive LSB replacement based on several criteria such as edges, texture and brightness of the cover picture estimate the depth of LSB embedding [12–15] and advanced LSB models [12–16], which are described in more detail below.

In addition to the pixel value differencing approach suggested by Wu and Tsai [16], another prominent method is based on pixel value difference (PVD). This is determined by the difference between the values of two adjoining pixels, which determines the number of hidden bits that should be inserted. When the original difference value is not equal to the secret message, the difference values of the two consecutive pixels will be directly adjusted so that their difference values can represent the secret message. However, when the PVD approach adjusts the two successive pixels in order to conceal the secret data in the difference value, a significant degree of distortion may occur in the stego image. A texture picture with a greater resolution can encode more hidden data within the pixel pairs. LSB and PVD have similar payloads, however, PVD has a greater visual imperceptibility and higher visual imperceptibility. The PVD approach avoids the RS detection attacks, but it has a significant disadvantage in that it betrays the existence of a secret message through the use of a histogram. One of the most serious issues is the slipping between the cracks. Furthermore, because general photos have a smooth texture, any secret data will be concealed in the regions with a tiny value, as is the case with most photographs. Many efforts were provided in the literature study that sought to alleviate the constraints of PVD while also enhancing its steganographic aims as a whole. Among them are Multi-Pixel Differencing (MPD) [17], Modulus Function (MF) [18, 19], PVD with LSB [20, 21], block-based PVD [22], and other approaches detailed in [23] and [24]. Other examples include:

Chang et al. [25] propose a unique steganographic approach based on Tri-Way PVD, which is described in detail.

In contrast to the original PVD, the concealing capacity is increased by taking into account three separate directional edges, and the quality distortion is decreased by picking a reference point and applying adaptive algorithms to that point. Dual statistical stego-analysis is used to provide robustness as well as security in this method of study.

Another method, Capacity raising using multi-pixel differencing and pixel-value shifting [17], takes four block pixels and uses the difference between the lowest gray-scale value and the surrounding pixel. The sharpness and smoothness of the embedding are determined using the difference between the lowest gray-scale value and the surrounding pixel. If the difference is significant, it is placed in the sharp block, and if the difference is little, it is placed in the smooth block. When a smooth zone is present, the total embedding capacity diminishes. Following that, pixel-value shifting is performed to improve the overall image quality.

LSB substitution is used in conjunction with a novel approach of modulus function introduced by the Wang et al. Method [26], which is described further below. The main notion of a smooth region is embedded with LSB, and the edges are implanted with the PVD process, with the edges being embedded with LSB. This results in a significant increase in capacity while having no effect on human eyesight.

3 The Proposed Method

This approach is limited to gray-scale photos alone, as the name suggests. The fundamental notion employed in this strategy is the Sum of Digits. We choose a group of bits and modify the pixel in such a way that the sum of its digits equals the decimal value of the pixel we chose. Using this method, we can pick the group so that the change in the pixel value is the smallest possible. The results demonstrate that this innovative method keeps the quality of the image while remaining undetectable by a variety of steganalysis algorithms. This is a decent and acceptable signal-to-noise ratio (PSNR), co-relation, and entropy value for the data we have collected. In the next section, you will find a flow chart that illustrates the embedding and extraction processes in detail, followed by their methodology. Figure 2 shows the embedding process. Figures 3 and 4 show the change in pixel values before and after embedding.

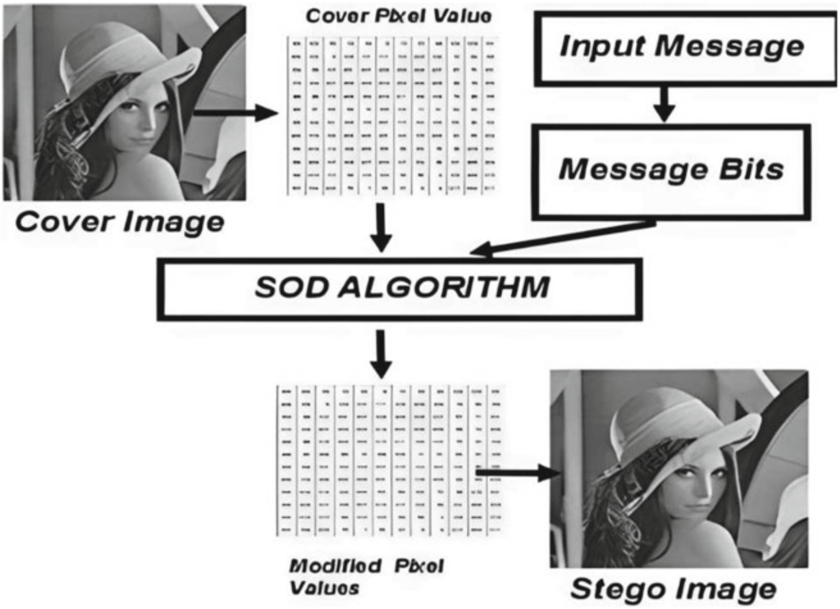


Fig. 2 Block diagram of the embedding algorithm

Fig. 3 Cover image block before embedding

240	123	76
60	135	50
86	55	240

Fig. 4 Cover image block after embedding

240	121	79
60	131	46
90	53	245

3.1 Flow Analysis of the Embedding Algorithm with Following Cases

Step 1: Select the cover image and secret message. Let the Secret Message be 'AB'.
Step 2: Convert the secret message into binary bits. Thus, the bit pattern we get is

$$\beta_n\beta_{n-1}\beta_{n-2}\beta_{n-3}\beta_{n-4}\beta_{n-5}\beta_{n-}\ldots\beta_7\beta_6\beta_5\beta_4\beta_3\beta_2\beta_1\beta_0$$

Secret Message: AB
'A' => 65 => 01000001
'B' => 66 => 01000010
So the bit pattern is: 0100000101000010
Step 3: Now take each pixel p_{ij} and find the sum of its digits. Say $\rho_{ij} = \varphi_2 \times 100 + \varphi_1 \times 10 + \varphi_0$, now sum of digits we get is $\sum_{i=0}^{n} \varphi_i = \varphi_{ij}$
76 => Sum of Digits => 13 => 1101
Step 4: Insert β_n bits into each pixel in such a way, that φ_{ij}, is the decimal equivalent of the selected binary bits β_n. To find the optimal condition in which β_n can be embedded into ρ_{ij} we check few cases:
Case 1: If β_n consists of 0's then we convert ρ_{ij}, such that $\rho_{newij} = \varphi_2 * 100 + \varphi_1 * 10$ and ρ_{nextij}, , μ*η being the resolution of the image, $0 \leq i \leq \mu$, $0 \leq j \leq \eta$,

$$\rho_{nextij} = \rho_{i+1 j=0};\ if\ j+1 \geq \eta$$

$$\rho_{nextij} = \rho_{ij+1};\ if\ j+1 \leq \eta$$

$$\rho_{nextij} = \varphi_2 * 100 + \varphi_1 * 10 + n$$

So the new pixels will be: 240 -> 240 and 123 -> 121
<u>0</u> 100000101000010
Case 2: Evaluate the value of $\sum_{i=0}^{n} \varphi_i = \varphi_{ij}$, insertion of β_n into ρ_{ij} depends onφ_{ij}, we take nearest value of φ_{ij} as β_n. We calculate the min_∂, for this we start from the β_n^{th} bit and move forward.

$$\partial_0 = \varphi_{ij} - (\beta_n)_{10}\partial_1$$

$$\partial_1 = \varphi_{ij} - (\beta_n\beta_{n-1})_{10}$$

$$\partial_2 = \varphi_{ij} - (\beta_n\beta_{n-1}\beta_{n-2})_{10}$$

$$\partial_3 = \varphi_{ij} - (\beta_n\beta_{n-1}\beta_{n-2}\beta_{n-3})_{10}$$

$$\partial_4 = \boldsymbol{\varphi}_{ij} - \left(\boldsymbol{\beta}_n \boldsymbol{\beta}_{n-1} \boldsymbol{\beta}_{n-2\boldsymbol{\beta}_{n-4}\boldsymbol{\beta}_{n-5}}\right)_{10}$$

$$\boldsymbol{min}_\partial = \mathbf{min}(\partial_4, \partial_3, \partial_2, \partial_1, \partial_0)$$

$\partial_\mathbf{n} = \boldsymbol{min}_\partial$
$\boldsymbol{\varphi}_{newij} = \boldsymbol{min}_\partial$,
So we have to choose $\boldsymbol{\rho}_{newij}$ such that
$\boldsymbol{\rho}_{newij} = \boldsymbol{\varphi}_{new2} \times 100 + \boldsymbol{\varphi}_{new1} \times 10 + \boldsymbol{\varphi}_{new0}$,
And,
$\boldsymbol{\varphi}_{newij} = \sum_{i=0}^{3} \boldsymbol{\varphi}_{newi}$.
Nearest is 10000 which is the next set of 5 bits.
76 => 1101 => 10000 => (16) => 79
0 10000 0101000010
Step 5: The Remaining bit stream is

$$\boldsymbol{\beta}_{n-1}\boldsymbol{\beta}_{n-2}\boldsymbol{\beta}_{n-3}\boldsymbol{\beta}_{n-4}\boldsymbol{\beta}_{n-5}\boldsymbol{\beta}_{n-} \cdots \boldsymbol{\beta}_7\boldsymbol{\beta}_6\boldsymbol{\beta}_5\boldsymbol{\beta}_4\boldsymbol{\beta}_3\boldsymbol{\beta}_2\boldsymbol{\beta}_1\boldsymbol{\beta}_0$$

Step 6: Now repeat 3–5 for remaining pixels.

3.2 Flow Analysis of the Extraction Algorithm with Following Cases

Step 1: Select the stego image.
Step 2: For extracting we follow the criteria, such as:
Case 1: If $\mathbf{mod}(\boldsymbol{\rho}_{ij}, 10) = 0$, $\boldsymbol{\beta}_n$ Consists of 0's, and n $= \boldsymbol{mod}(\boldsymbol{\rho}_{nextij}, 10)$, $\boldsymbol{\beta}_n = 000\ldots \boldsymbol{nterms}$
240 => 0's
121 => 1 => 0
0
Case 2: If $\mathbf{mod}(\boldsymbol{\rho}_{ij}, 10) \neq 0$, represent it as
$\sum_{i=0}^{n} \boldsymbol{\varphi}_i = \boldsymbol{\varphi}_{ij}$, where
$\boldsymbol{\rho}_{ij} = \boldsymbol{\varphi}_2 \times 100 + \boldsymbol{\varphi}_1 \times 10 + \boldsymbol{\varphi}_0 \partial_n = \boldsymbol{\varphi}_{ij}\boldsymbol{\beta}_n = \boldsymbol{bin}(\partial_n)$
79 => 7 + 9 => 16 => 10000
0 10000
Step 3: Evaluate all such $\boldsymbol{\beta}_n$ values for all the pixel values in the image.
Step 4: All the $\boldsymbol{\beta}_n$ evaluated from the pixel values are represented as a whole, such as, $\boldsymbol{\beta}_n\boldsymbol{\beta}_{n-1}\boldsymbol{\beta}_{n-2}\boldsymbol{\beta}_{n-3}\boldsymbol{\beta}_{n-} \cdots \boldsymbol{\beta}_4\boldsymbol{\beta}_3\boldsymbol{\beta}_2\boldsymbol{\beta}_1\boldsymbol{\beta}_0$.
01000001 01000010 11
Step 5: Divide them into group of $\boldsymbol{\beta}_8$, and then convert them into their equivalent character form.
01000001 => 65 => A
01000010 => 66 => B

Step 6: Repeat step 2–5 for all message bits.

4 Experimental Results and Analysis

There is a thorough explanation of the experimental analysis that was performed using this approach included in this document. According to certain current approaches, we assess and compare both the original and stego photos in this paper. In order to test the findings, the 'lena.pgm' cover picture, as shown in Fig. 5, is utilised. The sizes of the photos are determined at random. It is decided on the usage of a sequence of randomly generated digits or characters as the secret message to be placed into the cover graphics. The peak signal-to-noise ratio (PSNR) was used to assess the overall picture quality of the image. The probability of a signal being received is defined as follows:

$$\text{PSNR} = 10.\log_{10}\frac{\left(2^{\text{B}}-1\right)^2}{\text{MSE}}\text{PSNR} = 10.\log_{10}\frac{\left(2^{\text{B}}-1\right)^2}{\text{MSE}}\text{dB}$$

And

$$\text{MSE} = \frac{1}{\mu \times \eta}\sum_{i=0}^{\mu-1}\sum_{j=0}^{\eta-1}\left(\gamma_{ij} - \ddot{\Upsilon}_{ij}\right)^2.$$

As shown in this illustration, is the cover image pixel with the coordinates (ij), and is the stego-image pixel with the same coordinates. The greater the PSNR number, the greater the likelihood that the difference between the cover picture and the stego image is undetectable by human eyes. Table 1 displays the results of the experiments conducted on a variety of typical cover pictures.

As we can see in Table 1, there is little question that the stego-image quality created by the suggested technique was pretty good, with no discernible difference

(a) **(b)** **(c)** **(d)**

Fig. 5 Visual effects of proposed steganography scheme **a** PSNR 58.8 dB, **b** PSNR 52.8 dB, **c** PSNR 48.4 dB, **d** PSNR 37.58 dB

Table 1 Experimental result

Image	Length of embedding (bpp)	PSNR (dB)	Correlation	Entropy
lena512.bmp (512 × 512)	327	60.492	0.999987	7.445684
	3270	50.105	0.999863	7.445894
	8192	46.075	0.999660	7.441868
	16,384	43.085	0.999342	7.426170
	32,768	40.065	0.999034	5.981834
zelda512.bmp (512 × 512)	327	60.260	0.999981	7.267064
	3270	50.094	0.999808	7.266713
	8192	46.042	0.999523	7.262412
	16,384	43.066	0.999086	7.245796
	32,768	40.025	0.998766	7.359929
Cameraman.bmp (512 × 512)	327	53.754	0.999971	6.910685
	3270	44.014	0.999738	6.920358
	8192	40.019	0.999391	6.874710
	16,384	37.098	0.998964	6.565247
	32,768	36.617	0.998872	6.443998
barbara.pgm (512 × 512)	327	59.809	0.999988	7.632077
	3270	50.053	0.999893	7.631960
	8192	46.027	0.999736	7.627175
	16,384	42.944	0.999480	7.607857
	32,768	39.975	0.999035	7.532511
boat.512.tiff (512 × 512)	327	59.573	0.999983	7.191792
	3270	50.125	0.999856	7.193764
	8192	46.135	0.999647	7.193725
	16,384	43.074	0.999307	7.184372
	32,768	40.090	0.998712	7.143109

between the original cover picture and the final product. Furthermore, as shown in Table 2, embedding has a greater capacity than the other approaches now in use. In addition, we analyse the payload capacity of the suggested scheme in order to determine the overall quality of the technique. When it comes to payload capacity, it is defined as the ratio of the number of embedded bits to the number of cover bits in a message. It is denoted by the symbol.

$$\mathtt{C} = \frac{\text{number of } \beta_n}{\mu \times \eta}$$

$$\mathtt{C}_{\text{avg}} = 2.54\,\text{bits/pixel}$$

Table 2 Comparison of embedding capacity with existing method

Existing solutions	Cover image	Capacity (bytes)	PSNR (dB)
Wu and Tsai original PVD [16]	Lena	50,960	41.79
	Baboon	56,291	37.90
	Pepper	50,685	40.97
	Jet	51,243	40.97
Wang et al.'s method [26]	Lena	51,226	46.96
	Baboon	57,138	43.11
	Pepper	50,955	46.10
	Jet	51,234	46.19
Yang and Weng's method [17]	Lena	73,814	35.98
	Baboon	78,929	33.17
	Pepper	74,280	34.79
	Jet	73,001	33.89
Chang et al.'s method [27]	Lena	76,170	40.80
	Baboon	82,672	32.63
	Pepper	75,930	40.25
	Jet	76,287	38.46
Chang et al.'s tri-way PVD [25]	Lena	75,836	38.89
	Baboon	82,407	38.93
	Pepper	75,579	38.50
	Jet	76,352	38.70
SOD method (proposed method)	Lena	78,000	36.43
	Baboon	75,000	36.16
	Pepper	75,000	36.03
	Jet	65,000	36.05

Table 2 compares and contrasts the suggested technique with an alternative algorithm. Because the PSNR value is higher than that of the previous algorithm, we may conclude that it is superior to the existing Yang and Weng's technique. The concessions made in terms of image quality are negotiated in light of the unpredictable nature of the medium.

In current times, steganalysis is performed in two stages: first, the image models are extracted, and then the image models are trained using a machine learning tool to discriminate between the cover picture and the stego image. The training is carried out with the use of appropriate picture models, which allow for the differentiation of each and every cover and stego image.

We employed Rich models for steganalysis of digital pictures [28] for the extraction phase, and the procedure begins with the assembly of distinct noise components retrieved from the submodels produced by neighbourhood sample models. The primary goal is to discover various functional connections between nearby pixel blocks in order to recognise a diverse range of embedding models. In the approach, we employed a straightforward way to produce the submodels, which we then combined into a single feature before developing a more complicated submodel and classifying them. Both the cover picture and stego image are used in the extraction procedure, and the attributes of each are extracted.

During the training phase, we begin by dividing the picture database into sets, with each set including the same number of matching stego images as well as associated cover images. In order to do this, we employed the ensemble classifier, as described in [29] and [30]. The ensemble classifier is made up of L binary classifiers, which are referred to as the basis learners.

1, 2, 3,…, L, each trained on a distinct submodel of a randomly selected feature space. In order to evaluate the performance detection of the submodel on an unknown data set, it is convenient to use the out-of-band error estimate. The rich model is then assembled using the OOB error estimates from each submodel in the following step. Figure 6 depicts the progress made in estimating out-of-band error estimates in the proposed model. Following the generation of the OOB estimations [31], the implementation of a Receiver Operating Characteristic (ROC) graph is carried out, which conveys the categorisation of the models into stegogramme and non-stegogramme classes. The ROC curve of 50 stegogrammes and non-stegogrammes from our picture dataset on different embeddings of 0.01, 0.1, and 0.25 bpp is depicted in Fig. 7. The embeddings with a bpp of less than 0.25 are acceptable and are not identified by the model (Fig. 8).

It is noticed that the suggested technique outperforms the well-known Tri-Way PVD when the ROC curves for Tri-Way PVD and the proposed method are shown at an embedding rate of 0.25 bps. When comparing the two methods at an embedding rate of 0.25 bpp, the ensemble recognises the Tri-Way PVD completely, but the suggested approach is only partially identified by the ensemble.

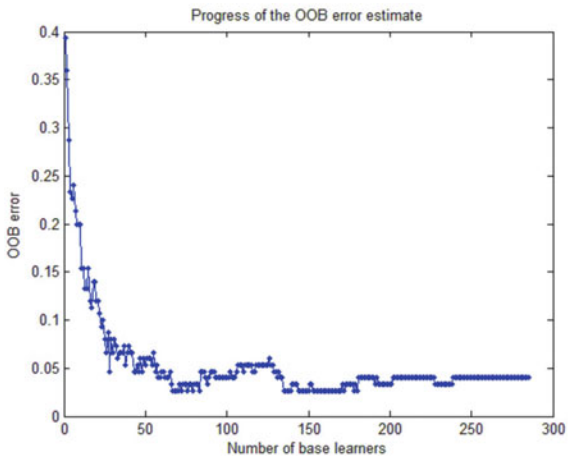


Fig. 6 OOB error estimates

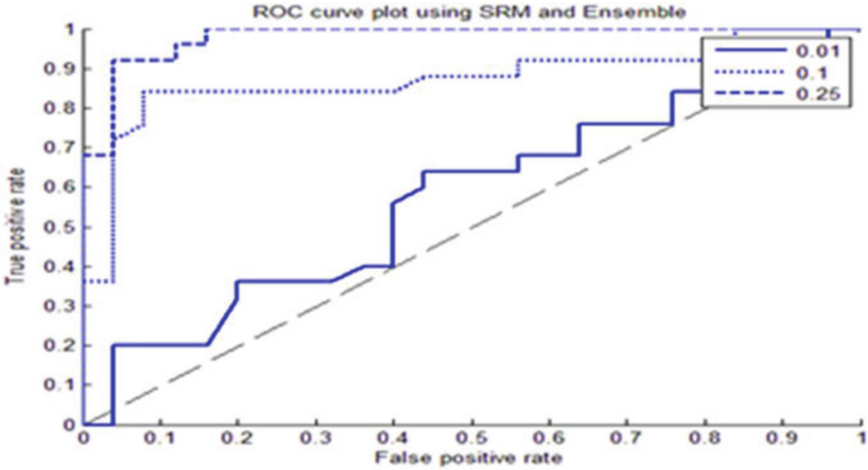
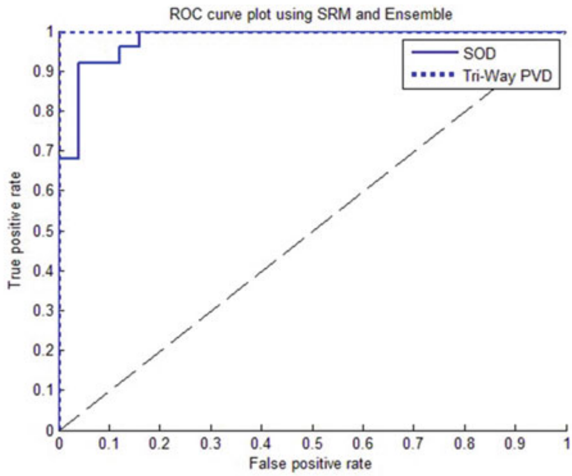


Fig. 7 ROC curve embedding at 0.01, 0.1, and 0.25 bpp

Fig. 8 ROC curve comparison at 0.25 bpp



5 Conclusions

With the help of algorithms, figures, and examples, this proposed method has shed light on the various techniques available for implementing Steganography and has narrowed its focus to our own devised method of Image Steganography, which explains how to embed a message into any cover image in a clear and understandable manner. Because it has been tested and run several times, the novel technique is one-of-a-kind and has shown to be quite reliable thus far. The results of the steganalysis are pretty satisfactory and comparable to those of other models. Moreover, the application of SRM steganalysis is investigated, and it is discovered that the embedding is pretty acceptable below 0.25 bpp when displaying its ROC curve with an ensemble classifier.

References

1. Holub V, Fridrich J, Denemark T (2014) Universal distortion function for steganography in an arbitrary domain. EURASIP J Inf Secur 2014(1):1
2. Balasubramanian C, Selvakumar S, Geetha S (2014) High payload image steganography with reduced distortion using octonary pixel pairing scheme. Multimed Tools Appl 73(3):2223–2245
3. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):781–783
4. Liao X, Qin Z, Ding L (2017) Data embedding in digital images using critical functions. Signal Process: Image Commun 58:146–156
5. Sun H-M et al (2011) Anti-forensics with steganographic data embedding in digital images. IEEE J Sel Areas Commun 29(7):1392–1403
6. Kieu TD, Chang C-C (2011) A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 38(8):10648–10657
7. Kuo W-C, Kuo S-H, Huang Y-C (2013) Data hiding schemes based on the formal improved exploiting modification direction method. Appl Math Inf Sci Lett 1(3):1–8
8. Tsai P, Hu Y-C, Yeh H-L (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89(6):1129–1143
9. Chen N-K et al (2016) Reversible watermarking for medical images using histogram shifting with location map reduction. In: 2016 IEEE international conference on industrial technology (ICIT). IEEE
10. Pan Z et al (2015) Reversible data hiding based on local histogram shifting with multilayer embedding. J Vis Commun Image Represent 31:64–74
11. Al-Dmour H, Al-Ani A (2016) A steganography embedding method based on edge identification and XOR coding. Expert Syst Appl 46:293–306
12. Qazanfari K, Safabakhsh R (2014) A new steganography method which preserves histogram: generalization of LSB++. Inf Sci 277:90–101
13. Tavares JRC, Junior FMB (2016) Word-hunt: a LSB steganography method with low expected number of modifications per pixel. IEEE Lat Am Trans 14(2):1058–1064
14. Tseng H-W, Leng H-S (2014) High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion. IET Image Proc 8(11):647–654
15. Nguyen TD, Arch-Int S, Arch-Int N (2016) An adaptive multi bit-plane image steganography using block data-hiding. Multimed Tools Appl 75(14):8319–8345
16. Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24(9–10):1613–1626
17. Yang C-H, Wang S-J, Weng C-Y (2010) Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations. Fundam Inform 98
18. Pan F, Li J, Yang X (2011) Image steganography method based on PVD and modulus function. In: 2011 international conference on electronics, communications and control (ICECC). IEEE
19. Liao X, Wen Q, Zhang J (2013) Improving the adaptive steganographic methods based on modulus function. IEICE Trans Fundam Electron Commun Comput Sci 96(12):2731–2734
20. Wu H-C et al (2005) Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE Proc-Vis, Image Signal Process 152(5):611–615
21. Jung K-H (2010) High-capacity steganographic method based on pixel-value differencing and LSB replacement methods. Imaging Sci J 58(4):213–221

22. Yang C-H et al (2011) A data hiding scheme using the varieties of pixel-value differencing in multimedia images. J Syst Softw 84(4):669–678
23. Hussain M et al (2015) Pixel value differencing steganography techniques: analysis and open challenge. In: 2015 IEEE international conference on consumer electronics-Taiwan. IEEE
24. Hussain M et al (2017) A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Process: Image Commun 50:44–57
25. Chang K-C et al (2008) A novel image steganographic method using tri-way pixel-value differencing. J Multimed 3(2)
26. Wang C-M et al (2008) A high quality steganographic method with pixel-value differencing and modulus function. J Syst Softw 81(1):150–158
27. Chang K-C et al (2007) Image steganographic scheme using tri-way pixel-value differencing and adaptive rules. In: Third international conference on intelligent information hiding and multimedia signal processing (IIH-MSP 2007), vol 2. IEEE
28. Kodovsky J, Fridrich J, Holub V (2011) Ensemble classifiers for steganalysis of digital media. IEEE Trans Inf Forensics Secur 7(2):432–444
29. Fridrich J et al (2011) Steganalysis of content-adaptive steganography in spatial domain. In: International workshop on information hiding. Springer, Berlin, Heidelberg
30. Kodovský J, Fridrich J (2011) Steganalysis in high dimensions: fusing classifiers built on random subspaces. In: Media watermarking, security, and forensics III, vol 7880. International Society for Optics and Photonics
31. Fridrich J, Kodovsky J (2012) Rich models for steganalysis of digital images. IEEE Trans Inf Forensics Secur 7(3):868–882