Hybrid Selective Steganography

Sushma R B, Dr. Manjula G R, Sayyed Johar

Sushma R B, JNN college of Engineering,
Shimoga, Karnataka, India PH-+91 9008023838
sushmarb@jnnce.ac.in

Dr. Manjula G R, , JNN college of Engineering,
Shimoga, Karnataka, India PH-+91 9164300521
grmanjula@jnnce.ac.in

Sayyed Johar, , JNN college of Engineering,
Shimoga, Karnataka, India PH-+91 9886164756
syedjohar@jnnce.ac.in

Abstract: The dream of our Prime Minister "Digital India" will be successful only if there is reliable security for the digital data Majority of the sensitive information which passes through the communication channel is vulnerable to attackers. Hence we need to develop algorithms that will help protect the integrity of digital media element and intellectual property rights of its owners. So it is necessary to develop methods which not only involves hiding of sensitive information but also the fact that communication is taking place. To achieve these requirements we are using the concept of Steganography which is the art of secret. There are several types of steganography depending on which is the carrier. Here we have used Image as the carrier. Here we are using a combination of 2 algorithms, which is selected based on the data that is being communicated. The proposed scheme aims to provide better performances in terms of time, robustness and perceptual quality than other embedding algorithms.

Keywords: Image Steganography, Random Index Channel, Pixel Pattern Based, PSNR, MSE

1. Introduction

Information and communication technology has evolved in a greater manner recently. All the data needed is just fingertips away. Each and every person has access to majority of the data. Even though this seems as an advantage, there are several disadvantages too. Sensitive data present on the network becomes vulnerable as many people can access it. Now a days, ecommerce is a major trend which involves highly sensitive and confidential information to communicate. For exchanging of data, everyone relies on computer networks which is unprotected. So there is a need for information security to avoid unauthorized access of the data and also secure transmission of data. There are various technologies present to satisfy these norms. Mainly the technologies which are having information security as primary concern are Cryptography, Steganography and Watermarking. So this area has drawn attention of many researchers, government agencies, law makers, military, intelligence agencies who require uninterrupted communications. The key areas of concern in information security are confidentiality, integrity and availability. Confidentiality refers to avoiding the disclosure of information to unauthorized persons. Data sent by the sender should be consistent throughout its life cycle which is referred to as data integrity. Availability means, information should be available for the receiver whenever necessary. Cryptography is a technology which is used when the data is sensitive and should be read by the receiver itself. Cryptography algorithms converts plain text or sensitive information of the sender to unreadable cipher text using encryption key. The receiver decrypts it using the decryption key. The idea is to change the text into format which is not easy to read or analyse without decryption key. Modern cryptographic algorithms heavily based on mathematical theory and involves high computation. A digital watermark deals with patterns of bits inserted into a digital file, image audio or video. They are mainly used for copyright purposes. Steganography is a term got by combining two words, Stego means covered graphy means writing. Hence Steganography is the art of secret writing.

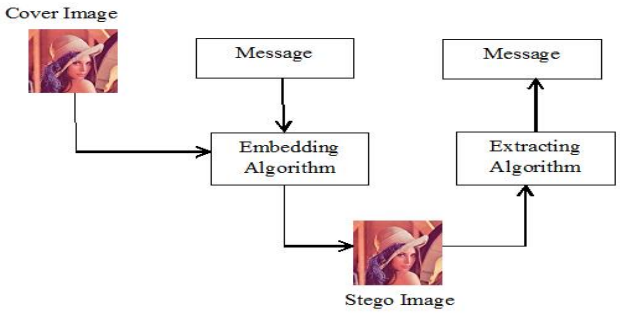


Fig1: *Image Steganography*

Image steganography terminologies are as follows:-

1. Cover-Image: Original image which is used as a carrier for hidden information.
2. Message: Actual information which is used to hide into images. Message could be a plain text or some other image.
3. Stego-Image: After embedding message into cover image is known as stego-image.
4. Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.

Properties of Image Steganography algorithms:

1. High Capacity: amount of information that can be put into the image.
2. Perceptual Transparency: even after embedding data into cover image, the change should not be noticeable.
3. Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
4. Tamper Resistance: It should be difficult to alter the message once it has been embedded into stego-image.

5. Computation Complexity: How much expensive it is computationally for embedding and extracting a hidden message is of major concern.

2. Hybrid Selective Steganography

Each pixel is a combination of RGB i.e. (Red, Green, and Blue). Any image will have 8 bits representing each of the three color values (red, green, and blue) at each pixel. Cover image is chosen such that small changes in it is not generally noticable. Even peoples eye is not so sensitive to identify those minute variations. Maintaining the quality of the image is important for protection of the message. Enhancing this we use different techniques. The proposed technique is a combination of two algorithms, Pixel pattern based [7] and randomized Index channel method [6]. Based on the pixel values of secret image the choice of the technique differs. Since the combination and usage of algorithm varies based on secret data, it becomes almost impossible to identify the technique correctly. Hence making the algorithm more secure. According to Pixel pattern based technique, for each pixel in the Secret Image matching pixel in the cover image is searched. When the matching pixel is found, the corresponding position of both cover and secret images are stored. This is repeated for all the pixels, which has matching pixel in cover image. The rest of the pixels are embedded using random index channel based algorithm. In Index channel method, any image with RGB combination can be used as cover image to store secret data. If it's highly color variant then it will be easier to store more data. Each pixel by itself identifies whether it stores any secret data or not. The last 2 bits are used as indicator of whether there is any data stored or not, therefore as the cover image changes, the possibility of storing data also changes making it more secure. The rule used to identify whether or not the data is stored is represented by M variable as illustrated in table 1. This M variable identifies in which channel we are storing data. If M has a value 01 then we are storing data in one of the channels. How much of data is stored is given by 5, 6, 7 bits of that pixel. The detailed illustration is given in table 1

Table 1: *Meaning of bits in index channel algorithm*

M=bit 0 and bit 1	Channel 1	Channel 2
00	No data stored	No data stored
01	Data stored= H	No data stored
10	No data stored	Data stored= H
11	Data stored =H	Data stored = H

According to index channel algorithm, first any one of the channels among red green and blue is chosen and assigned as index channel. This random selection makes this algorithm more secure. Once channel is selected, for each iteration of for loop the index channel changes according to algorithm specified. The number of bits stored is given by the last two bits of cover image. If the last 2 bits is 00 then no bits are embedded in the cover image. All the possibilities is given in table 1. This process continues until all the 24 bits in secret image is embedded. Then next pixel of secret image is considered. The algorithm first checks each pixel of cover image, whether that is used by pixel pattern based algorithm If it is not used then the corresponding picture in the cover image is used to embed, else skipped. The value of 5,6 or 7 bits is recorded to determine number of secret bits to be stored in other than the index channel based on the bits 1 and 2. The remaining secret bits of that pixel is stored in next pixel of cover image until all 24 bits of the pixel is stored. This is repeated for all the pixel in secret image which were not embedded using pixel pattern based method. Now the modified cover image is called 'stego image'. The secret data can be any text, binary image or colored image and Cover medium used is colored image.

2.1 Algorithm:

Algorithm for embedding:

Step 1: Read the cover image.
Step 2: Read the secret image.
Step 3: Read the size of the cover image.
Step 4: Read the size of the secret image.
Step 5: Embed according to the pixel pattern based for all the pixels of secret image whose value is equal to the value of pixels in cover image.
Step 6: For the rest of the pixels in the secret image, embed according to the randomized index channel algorithm.

Pixel pattern based algorithm.

Step 1: Consider two arrays of size cover image.
Step 2: for each pixel in secret image.
Step 3: for each pixel in cover image.
Step 4: If the value of pixel in secret image is equal to the value of pixel in cover image,
Step 5: set array1 (coverrow, covercol)=0
Step 6: set array2 (secretrow,secretcol)=value of matched pixel
Step 7: Repeat steps 4-6 until, all the pixels of seceret image is checked for matching.

Randomized index channel algorithm

Step 1: using random number generation select any one channel and assign it to index channel.
Step 2: In every pixel present in secret image
Step 3: If numofbits available>0
Consider the selection of channels as:
If already selected channel is red, then channel=green.
Otherwise if selected channel is green then channel =blue.
Otherwise if selected channel is blue, then index channel=red.
Step 4: If array1(coverrow ,covercol)==1
Step 5: start from first pixel of coverimage
Step 6: consider the bits 5,6,7 and store it in H
Step 7: Fetch the 7 and 8 bit and store it in variable leastsignificantbit.
Step 8: If leastsignificantbit.=00, none of the data is hidden in that pixel.
Step 9: If leastsignificantbit=01 or 10 or 11 store the number of bits according to table 1
Step 10: The bits stored subtract it from numofbits. Continue the same until all 24 bits of secret image is completed and go to next pixel of secret image

Algorithm for extraction

Pixel pattern based extraction algorithm.

Step 1: for each pixel in secret image.
Step 2: for each pixel in cover image.

Step 3: If the value of pixel in array2 is equal to the value of pixel in cover image,
Step 4: Extract that pixel from the cover image.
Step 5: Insert that pixel in the recovered image at specified position.
Step 6: Repeat steps 4-6 until,all the pixels which are used by this algorithm are extracted

Randomized index channel extraction algorithm
Step 1: if array1 (coverrow ,covercol)==1
Step 2: Select the stego image
Step 3: Read the values from the arrays used in the pixel value based algorithm.
Step 4: Extract the pixels and insert in the recovered image at respective positions.
Step 5: Repeat the step 4 until the arrays become empty.
Step 6: .consider the first channel which was selected randomly while embedding
Step 7: until every pixel in secret image is considered Numofbits is assigned to 24
Step 8: until all the bits in one pixel of secret image Index channel is chosen as follows
If already selected channel is red, then channel=green.
Otherwise if selected channel is green then channel =blue.
Otherwise if selected channel is blue, then index channel=red.
Step 9: consider the bits 5,6,7 and store it in H.
Step 10: Fetch the 7 and 8 bit and store it in variable leastsignificantbit
Step 11: If leastsignificantbit=00, neglect that pixel as no data stored
Step 12: If leastsignificantbit =01 or 10 or 11 etract the number of bits as in table 1.
Step 13: Perform this until all the bits in the pixel are extracted
Step 14: loop the steps from 7 to 14 until all the pixels are extracted from received image.

3. Experimental Results and Analysis:

The proposed method is implemented for hiding several JPEG images as shown in Table 3. The column Cover Image specifies all images that are used as cover images and Secret Image column contains all images used as secret image. These images are in JPEG format, but can be applied to any other image format. The secret data can be any text, binary image or colored image and Cover medium used is colored image. The stego images that are obtained after embedding secret image in cover image are compared with corresponding cover images to get MSE and PSNR values. The results obtained is better than the previous method and the comparison is shown Table 2. MSE and PSNR identifies the difference between cover image and its corresponding stego image. If the difference is minimal then MSE value will be close to 0. And average PSNR value should be more than 40.As tabulated the values of MSE and PSNR are better than the previous method compared.

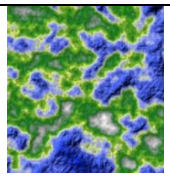
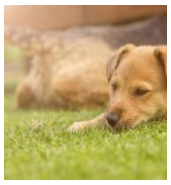
Table 2: *Comparison of MSE values.*

Cover image	Secret image	MSE of proposed method	MSE of Index Channel [6]
Coverpic1	secretlena	2.5118	3.1215
Coverpic1	secretdoll	2.1806	2.7847
Coverpic2	secretlena	2.8598	3.2642
Coverpic2	secretdoll	1.7413	2.5341
Coverpic3	secretlena	2.9583	3.4654
Coverpic3	secretdoll	1.8847	2.5123

Table 3: *Comparison of PSNR values*

Cover image	Secret image	PSNR of proposed method	PSNR of Index Channel [6]
Coverpic1	secretlena	44.7095	42.3417
Coverpic1	secretdoll	44.7791	41.2856
Coverpic2	secretlena	43.6015	41.7614
Coverpic2	secretdoll	45.7561	42.1498
Coverpic3	secretlena	43.4544	41.2639
Coverpic3	secretdoll	45.4213	42.7821

Table 4: *Test bed of images used for performance analysis*

Cover image	Secret image
 Coverpic1	 secretlena
 Coverpic2	 Secretdoll
 Coverpic3	 Secret3

4. Conclusion

Hybrid steganography presents complex method of steganography since it is the combination of two different steganography algorithm. In this, the pixel value will be changed only for the randomized index based method hence the stego image looks almost like original cover image. This makes it more secure because it almost becomes impossible

to identify the existence of any other form of data. Randomized index based method uses one channel as an indicator for the existence of hided secret color image in the other one or two channels. . This algorithm works better if there is minimal color differentiation between cover and secret images. The proposed algorithm shows promising results compared to other existing methods.

6. References

[1]. Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub,"RGB Intensity Based Variable-Bits Image Steganography" , IEEE Asia-Pacific Services Computing Conference , pp. 1322-1327, 2008.

[2]. Namita Tiwaril and Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal Of Security and its Applications, Vol. 4, No. 4, October 2010.

[3]. Mamta Juneja and Parvinder S. Sandhu, "An Improved LSBbased Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies, pp. 10-14, 2013.

[4]. Koyi Lakshmi Prasad and T. Ch. Malleswara Rao, "A Novel Secured RGB LSB Steganography with Enhanced Stego-Image Quality", International Journal of Engineering Research and Applications , Vol. 3, No. 6, pp. 1299-1303, 2013.

[5]. Babita and Ayushi, "Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique",International Journal of Computer Science and Engineering Technology, Vol. 4, No. 6, pp. 758-762 , 2013

[6]. Ajit Danti, G. R. Manjula and R. B. Sushma , " Steganography using Randomized Index Channel with Arnold Cat Map Encryption ", Proceedings of the Second International Conference On "Emerging Research in Computing , Information and Communication and Application " 2014

[7]. R.Rejani , D. Murugan and Deepu V.Krishnan ," Pixel Pattern Based Steganography On Images " Ictact Journal on Image and Video Processing, February 2015, volume: 05, issue: 03

Author Profile

Mrs Sushma R B

Sushma R B received the B E degree from BNM Institute Of Technology, Bangalore and M.Tech from Bapuji Institute Of Technology Davangere. Currently working in Jawaharlal Nehru National College Of Engineering, Shimoga. Author has 8 years of experience in teaching. Area of interest includes Image Processing and specifically steganography.