De-Noise Steganography by Enhancing the Cover Image: A Multi-Level Security Approach

Jithesh Korothan[1], Shirivas Kishor[2], and Pradeep Butey[3]
[1]Department of Computer Science, Mahatma Gandhi College, India
[2]Department of Computer Science, Sardar Patel Mahavidyalaya, India
[3]Department of Computer Science, Kamala Nehru College, India

Abstract: *A technique that combines both logic and craft only can survive long. A multi-level security mechanism by blending steganogrpahy and visual cryptography is proposed here. Hiding already encrypted data inside an image is of immense value. Encryption is done by visual cryptography and hiding is done through the proposed de-noise Steganography With Selected Noise Bit Replacement Technique (SNBR). By and large, hiding data inside an image makes distortion to the image that leads to suspicions. Instead, this technique tries to remove disturbance or noise that is already present in the image and enhances the cover image through replacing noise bits present in the cover image with secret. In view of the fact that we replace the noise bits with the secret, it improves the quality of the cover medium and consequently the cover seems innocuous. As a result it reduces the chance of steg-analysis. The proposed method called SNBR, uses a location map to guarantee the correct extraction of the secret data. The goal of this study is to avoid degradation of the cover and improve the confidentiality of the information being communicated. Experimental results show that the new method achieves good security and a higher peak signal to noise ratio for the same number of bits per pixel of embedded image.*

Keywords: *Cover, de-noise, steganography, selected noise bit, stego-key, visual cryptography*.

Received May 5, 2014; accepted December 23, 2014

1. Introduction

Networking and digitization have become more and more evident features in the rapid development of the economic society. The convenient and timely acquisition of on-line services through accessing the Internet is a tidal current for individuals and organizations. However, the relay of sensitive information via an open Internet channel increases the risk of attacks. Thus many techniques have been proposed to deal with this issue. Data hiding plays an important role in information security for content authentication and perceptual transparency. The main aim of information hiding is to conceal the secret data into the wrappers like image, audio, video or text to avoid attracting the attention of possible attackers in the Internet channel.

The growing number of internet-based applications has made digital communication nowadays an essential part of infrastructure. In some digital communication confidentiality is necessary when sensitive information is being shared between two communicating parties over a public channel. An important sub division of information hiding is steganography [13, 16]. Cryptography [17] is the art and science of writing sensitive information in such a way that no one but the intended recipient can recover it, whereas steganography is the art and science of hiding sensitive information within innocuous documents in an undetectable way. Both provide confidentiality and protecting sensitive information. In this study we combine features of both these methods to provide multiple levels of security. The innocuous documents, also known as hosts/covers/carriers can be an image audio and video. On account of their insensitivity for the human visual system, digital images can be regarded as an excellent choice for hiding sensitive information.

One of the most commonly used data hiding approaches are the substitution technique. This approach is based on the fact that parts of the image which are regarded as redundant or noisy are replaced by the sensitive information bits. After embedding this information into the host, the resulting image is referred to as a stego-image and the file is referred to as a stego-file. The embedding algorithm may require a secret key, referred to as a stego-key.

Our primary objective here is to present a new and effective steganographic scheme that enhances the cover digital image, just opposite to the existing techniques [4] and provide a multi-level security, so as to physically and psychologically thwart steganalysis. The key issues that we have considered are the perceived quality of the stego-image and security. The blend of both steganography and visual cryptography help to accomplish this objective. Owing to the complexities in steganography and progressive power of steganalysis methods, it has turned out to be a

challenge to systematically develop techniques with much better performance. This study aims to cope with this problem by proposing a scheme that removes noises present in the cover and improves the visual quality rather than causing noises as usual. It is a substitution technique. However, not only the least significant but any bit that is part of a noise will be replaced.

The rest of this paper is organized as follows: The section 2 describes related works and the section 3 explains the proposed steganography scheme. In section 4, the cover selection for steganography based on image property is discussed. Section 5, presents the experimental results and discussion in terms of peak signal to noise ratio and finally section 6 concludes this paper.

2. Related Works

The Least Significant Bit (LSB) steganographic method [2, 9, 10] is the simplest one and is extensively used in the field of information security due to its high hiding capacity and quality. LSB replacement [2], Least Significant Bit Matching (LSBM), Least Significant Bit Matching Revisited (LSBMR) [10] and Least Significant Bit Matching-based Edge-Adaptive (LSBMR-EA) [9], image steganography are well-known LSB-like steganographic methods. The LSB-replacement embedding method replaces the LSB plane with embedded message bits, but the others do not. In LSB matching, if the embedded bit does not match the LSB of the cover image, then the pixel value of the corresponding pixel is randomly added by ±1. Unlike LSB replacement and LSBM, which embed message bits pixel by pixel, LSBMR deals with two pixels at a time and allows fewer changes to the cover image. The steganalysis resistance and image distortion of LSBMR are better than those of previous two. LSBMR-EA is anticipated to expand the LSBMR and uses an edge-adaptive scheme to select the embedding positions. Based on the size of the embedded message, LSBMR-EA embeds the message from sharper edge regions to smoother edge regions. Lou *et al.* [9], showed that LSBMR-EA can augment the security notably compared with the typical LSB-based approaches, while preserving higher visual quality of the stego-images.

Chang and Kieu [3] proposed an Optimal Pixel Adjustment Process (OPAP) to boost the quality of the stego-image by simple LSB substitution method through a raster scan. The OPAP tries to vary the value of Most Significant Bits (MSBs) next to the k^{th} bit, up to which the secret data are embedded. Yang [20] has proposed an LSB substitution method using the raster scan to improve stego-image quality by adapting an Inverted Pattern (IP) approach. In this technique, the secret message has been processed prior to embedding. The IP approach is believed to have a better image quality than that of OPAP. Provos and Honeyman [14] have proposed a hide-and-seek software technique for the random selection of pixels for embedding secret data, thereby generating the stego-image. In these random approaches, all the pixels of the cover image are not used to mask the secret data, which in turn affects the payload and the good imperceptibility. Lip *et al*. [15]. Proposed a scheme that modifies the current LSB substitution with sequential colour cycle.

It has been established that all the above stego techniques are not preferable to achieve maximum stego-image quality and greater complexity against intruders. They have computed the stego-image quality by considering a smaller amount of secret data, but they are weak when the amount of secrets is large and they do not greatly enhance the original view of the stego-image. The quality of the image can be easily analyzed by considering human vision sensitivity and the presence of secrets inside an image is realized, if the original view is disturbed.

All steganography techniques irrespective of spatial or frequency domain are not completely free from distortion. The hundred percentage imperceptibility of a secret embedded inside a cover image cannot be achieved by any known method. This fact motivated us to develop a scheme that improve the original view of the cover after embedding and maintain high visual quality. Since peak signal to noise ratio cannot be infinity, no technique is fully distortion free. However, it is possible to reduce the negative effect of embedding at the maximum. In this paper, authors proposed and demonstrated a new technique called Selected Noise Bit Replacement (SNBR) embedding that replace bits of noises already present in the digital image. It is implemented with the aim of achieving higher imperceptibility and enormous complexity against hackers as compared with the above mentioned methods.

3. Proposed Method

The proposed technique has two stages; first the secret will be partitioned into shares using visual crypto system, one of the best known cryptography techniques which have been credited to Moni Naor and Adi Shamir, who developed it in 1994. The second step involves hiding these shares into a digital image. The two stage process is proposed for accomplishing multi-level security; encryption and then embedding. Here, encryption is done through visual cryptography [11, 12] and embedding through SNBR steganography. The output of the first stage is passed to the embedding stage to enhance the security as well as the vicinity of the cover.

SNBR, as the name implies removes noises present in the cover medium by embedding shares of the secret information at selected noise pixels. Care is taken to avoid any distortion that may happen during

embedding. Selection is done through analyzing statistical features [5, 18]. Also it is done by considering the Human Vision Sensitivity (HVS). After selecting a particular position or finding a noise of the image the pixel values of that particular point is fetched. The details are explained in the following paragraphs.

Often, embedding makes distortion, but here it causes no distortion and gives enhancement to the original view of the cover. After embedding phase, if needed the image can further be processed to enhance by considering HVS without affecting the secrets inside. Here the algorithm takes the advantage of human psychology and human vision sensitivity. For this purpose it may use the image enhancement techniques. Human psychology is oriented in such a way that an intruder often anticipates a blurred or distorted stego-image due to hidden secret. As said the proposed system makes no distortion and improves its visual quality; the cover seems innocuous as far as an attacker is concerned.

To select the values of required pixels in an image using mouse click and return the values in a variable, here authors used the impixel function of MATLAB. We can select a pixel point from an image using mouse click in the MATLAB workspace. Impixel function returns the value of specified pixels in a variable in the MATLAB workspace. These values will be converted into binary. The x, y coordinates of the pixel value will be stored using the impixelinfo function in MATLAB. These pixel coordinates will act as the location map to guarantee the correct extraction of the secret. Noise pixels can be selected in this manner and embedding is done by replacing all or part of bits of these selected pixels so that it will improves the visual quality of the cover image without affecting its original view. The advantage of this scheme is that it enhances the noisy image and tries to avoid disturbances caused during embedding. The cover image first of all must seem casual. So it must be chosen from a set of subjects that can have a reason to be exchanged between the sender and the receiver. The image must be "noisy", so the embedded data in the noise bits can de-noise the image and accomplishes the task. Selection of a suitable image with noise is done carefully. Authors tried to have similarity between secret shares and noises while selecting images. The following subsection outlines the procedure for the proposed technique.

3.1. Visual Cryptography Shares

The secret data is made into shares using (2, 2) visual cryptography methods. Using advanced algorithm the security can be improved. This is the first level of hiding. These shares will be treated as information to be embedded inside an Image. The embedding process consists of choosing a subset of cover-elements and performing the substitution operation on them, which exchanges the SNBR of cover by the secret.

3.2. Encoding Process

1. Take the secret to be encrypted.
2. Create shares of the secret data with the help of visual cryptography. [first level of hiding]
3. Select an appropriate image to embed shares of the original message.
4. The selection of a suitable image is done carefully [19].
5. The image should comprise enough noises to be replaced.
6. Click noise pixel point in the image using mouse from MATLAB workspace.
7. Use impixel and impixelinfo functions of MATLAB to select the most suitable pixel values and its coordinates respectively.
8. Suitable pixels means, noise pixels that are easy to be replaced in the cover image.
9. Selection is done by statistical analysis (histogram, co-occurrence, run-length matrices or filtering) and HVS.
10. Coordinates will be kept as location map.
11. Pixel values will be converted into its binary.
12. Shares of secret will be embedded in selected pixels in the image.
13. The entire bytes in a pixel or few bits of a selected pixel can be replaced by considering the HVS.
14. The replacing bits positions within the selected pixel will also be noted.
15. If entire bytes within a selected pixel are replaced only its location map[x, y coordinates] is required to be noted.
16. The location map with bit positions together form stego-key.
17. Embedding is done using the SNBR steganography technique. (Here we get second level of hiding).

3.3. Decoding Process

1. Take the stego-image.
2. Using the stego-key, extract the embedded secret.
3. SNBR-steg decoding process extracts the secret from the cover image.
4. After decoding the secret from the cover medium [here the image], the receiver will get visual cryptographic shares of the original message.
5. These shares can be super imposed and produce the original message.

4. Cover Selection Based on Traits

The cover object in steganography acts only as a carrier for secret messages. Therefore, the client is allowed to choose any cover images from the database using a cover selection strategy. A cover selection

technique for hiding a secret image in a cover image was first introduced in Kermani and Jamzad [7]. This method operates on image texture similarity and replaces some blocks of a cover image with identical secret image shares; then, locations of confidential image blocks are kept in the cover medium. In Kharrazi *et al*. [8], the cover selection problem was studied by investigating three state of affairs in which the embedder has either complete knowledge, partial knowledge, or no knowledge of the steganalysis method.

In wrapper selection methods, a batch process determines the value of wrapper selection measure for each image in a database and the results are stored in a measure value database. When the steganographer wants to select a cover image, he can refer to this database and choose a proper image to hold his secret data. In this proposed scheme, apart from noises, the following properties like contrast, brightness, and darkness are also used as a measure for cover selection. In this way, to have a secure covert communication one can select a cover image with more noises, high contrast, brightness, or darkness from the database. The reason behind such selection, as will be explained in the following section, is that, in general, images with more noises, higher contrast, brightness, and darkness provide more embedding capacity.

5. Experimental Results and Discussions

The results of our experiments illustrate that stego-images, which are obtained by hiding secret data in cover images with disturbances, are less detectable by steganalysis. The proposed method begins with visual cryptography. It encrypts the secret into 2 shares. Visual cryptography requires no computation to decrypt the secret from its shares. Subsequently, these secret shares will be embedded into the cover image using the proposed SNBR steganography.

The reason behind using visual cryptography is, even if an intruder is success in steganalysis, he is not able to read the secret and might not thing about the act of encryption of the secret. Experiments have been done with plenty of images. Two among them are shown in Figures 3 and 4. First of all create shares of the secret. Figure 1 is the secret. Figure 2 shows its visual cryptographic shares. This is the first level of hiding. These shares are inserted into an image using proposed steganography. The steganography algorithm used here is a new one of its kind. As mentioned earlier, Figures 3 and 4 are two cover medium used for experiments in which some noises are seen. The shares of the Figure 1 are embedded into these two images. Figures 5 and 6 are their corresponding stego-images, where data (shares) are stored. Here, accomplishes the second level of hiding. From the human perception and PSNR values shown in Table 1, it is sure that this new technique has significantly improved the cover mediums. In addition to this, as stated earlier, a multi level security is also achieved.

Figure 1. Secret data.

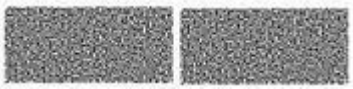

Figure 2.Visual cryptography shares.

Figure 3. Original image 1 with noise.

Figure 4. Original image 2 with noises.

Figure 5. Hiding using steganography (stego-image 1).

Figure 6. Hiding using steganography (stego-image 2).

Figure 7-a. Cropped and enlarged area of cover image [Figure 3].

Figure 7-b. Cropped and elarged area of stego image 1.

Table1. MSE and PSNR of cover and stego-images (the unit of PSNR is db).

Cover Image with noise		**Noise removed Stego Image PSNR**	
MSE	**PSNR**	**MSE**	**PSNR**
5.44	40.78	0.59	50.4
5.02	41.13	0.62	50.2

In order to verify the method, the PSNR values of the original noisy cover images are compared with the values of their respective stego-images. Peak Signal To Noise Ratio (PSNR) is a statistical measure commonly used in image steganography for indicating the quality difference between the stego-image and the cover image. PSNR is estimated (in decibel) by the following formula:

$$PSNR=10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (1)$$

Where MSE is the mean square error which is defined as:

$$MSE=\frac{1}{wh}\sum_{i=1}^{w}\sum_{j=1}^{h}\left(C_{ij}-S_{ij}\right)^2 \quad (2)$$

Where 'w' and 'h' are the width and height of the images and C_{ij}, S_{ij} are the value of the pixel (i, j) in the cover and stego image, respectively. Higher the PSNR value, better the quality. Table 1 shows the MSE and PSNR values of two images before and after steganography. Results show that the visual quality of the cover image has been enhanced after embedding secret inside.

The proposed scheme is compared with three other currently popular steganographic schemes namely LSB based Substitution, Bit Plane Complexity Segmentation (BPCS) [1] and adaptive depth varying [6] scheme. The default optimal parameter settings suggested in the respective works are adapted for experimentation. The results are shown in the following subsection.

Figure 8-a. Cropped and enlarged area of cover image [Figure 4].

Figure 8-b. Cropped and enlarged area of stego image 2.

5.1. Visual Quality Analysis

The visual quality of the stego images generated is measured in metrics like Average Absolute Difference (AAD), PSNR, and the Structural Similarity Index Measure (SSIM). The results are reported in Table 2. It may be noted that the proposed method produces stego images with high image quality. To evaluate the visual quality of stego-images using the human eye, we enlarged the partial area of original cover images and corresponding stego-images, as shown in Figures 7-a and 8-a as well as Figures 7-b and 8-b respectively. Figures 7-a and 8-a show the cropped area from the two original noisy images (Figures 3 and 4) and Figures 7-b and 8-b show the cropped area from their corresponding stego-images (Figures 5 and 6). The difference between original cover images and stego-images show the proposed method enhances the noisy image and gives better picture perception than the original noise cover images.

Table.2. Visual quality analysis of the proposed method.

Steganograpy Algorithm	**AAD×10^{-2}**	**PSNR**	**SSIM**
LSB	0.29941	45.4	0.9999
BPCS	0.29878	45.8	0.9999
AE-Depth Varying	0.15075	49.0	1
Proposed SNSB	0.15030	50.4	1

5.2. Security Analysis

Most of the works associated with information hiding suggest single level of security. So the secret can be easily read, once it is extracted. This is a trouble associated with these approaches. In the light of this, authors blended steganography with visual cryptography to provide multiple levels of security. Here, if the security is breached at one level it can be preserved at the next level.

Evaluating the security of the proposed approach, we test the proposed scheme with plenty of images, which are collected from some sets of images with different resolutions. We cropped the images to size of 512X512 and converted them to grayscale. These covers have not shown to the steganalyzers that determine the embedding capacity. Then to construct cover image dataset, a secret share (random binary string) is embedded in each image in the dataset so as the size of secret data is equal or smaller than the embedding capacity of the cover image. Then the detection rate of these images is evaluated against the state-of-the-art steganalyzers. The efficient and famous steganalysis methods like Wavelet-Based Steganalysis method (WBS) proposed by Lyu and Farid (2002) and Markov-DCT based steganalysis method (274-dim), which has a 274-dimensional feature vector that

merges Markov and DCT features (Pevny and Fridrich, 2007) are used for the evaluation. First we evaluated the detection rate of each original image with the state of the art PQ steganalyser with three different payloads. Then the same cover is tested after de-noising them with the proposed SNBR steganography. The results in Table.3 show that the proposed method embeds secret data with high security without attracting the attention of the attackers.

Table 3. Detection accuracy (%) of images with classical steganography and the proposed approach.

	Classical PQ Stego Method steganalyser		Proposed SNBR using PQ Stego Method steganalyser	
Payload In bits	WBS	274-dim	WBS	274-dim
2000	70	72	50	54
6000	73	74	53	50
10,000	76	76	55	59

6. Conclusions

A novel spatial steganography scheme realized with SNBR paradigm is introduced. Most suitable noise significant pixel is modified to an extent decided by the HVS of the image. The generated stego images possessed less perceptual distortion compared with highly noised cover image. They also prove to be secured against RS steganalysis. The experimental results evaluated on natural images using different kinds of steganographic algorithms show both visual quality and security of our stego-images are significantly better compared to typical LSB-based approaches and their edge adaptive versions. In addition to this the proposed method provides a multi level security through associating visual cryptography and steganography. This study has also taken the advantage of human psychology. Often steganography makes distortion to the cover medium. Instead, this method improves its original view. So an intruder may not think that the image is a cover medium. However, our method is not strong against filtering, cropping, and lossy compression or any such active modifications. Hence, our future work will focus on modifying our approach so that the secret message may be preserved even in the presence of intermediate image manipulations.

References

[1] Bui C., Lee H-Y., Joo J., and Lee H-K., "Secure Bit-Plane Based Steganography for Secret Communication," *IEICE Transactions on Information and Systems*, vol. E93-D, no. 1, pp. 79-86, 2010.

[2] Chan C. and Chen L., "Hiding Data in Images by Simple LSB Substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469-474, 2004.

[3] Chang C. and Kieu T., "A Reversible Data Hiding Scheme Using Complementary Embedding Strategy," *Information Sciences*, vol. 180, no. 16, pp.3045-3058, 2010.

[4] Cheddad A., Kevitt P., Curran K., and Condell J., "Digital Image Steganography: Survey and Analysis of Current Methods," *Science Direct*, vol. 90, no. 3, pp. 727-752, 2010.

[5] Gonzalez R., and Woods R., *Digital Image Processing*, Amazon, 2008.

[6] He J., Tang S. and Wu T., "An Adaptive Image Steganography Based on Depth-Varying Embedding," *in Proceeding of Image and Signal Processing*, Sanya, pp. 660-663, 2008.

[7] Kermani Z. and Jamzad M., "A Robust Steganography Algorithm Based on Texture Similarity Using Gabor Filter," *in Proceeding of IEEE International Symposium Signal Processing and Information Technology*, Athens, pp. 578-582, 2005.

[8] Kharrazi M., Sencar H., and Memon N, "Cover Selection for Steganograpic Embedding," *In Proceeding of Image Processing*, USA, pp. 117-121, 2006.

[9] Luo W., Huang F., and Huang J., "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, 2010.

[10] Mielikainen J., "LSB Matching Revisited," *IEEE Signal Process*, vol. 13, no. 5, pp. 285-287, 2006.

[11] Naor M. and Shamir A., *Visual Cryptography, Advances in Cryptology*, Springer-Verlag, 1995.

[12] Naor M. and Shamir A., "Visual Cryptography II: Improving the Contrast via the Cover Base," *Security in Communication Networks*, vol. 1189, no. 2, pp. 197-202, 1996.

[13] Peticolas F. and Katzenbeisser S., *Information Hiding Techniques for Steganography and Digital Water Marking*, Artech House, 2000.

[14] Provos N. and Honeyman P., "Hide and Seek: an Introduction to Steganography," *IEEE Security and Privacy Magazine*, vol. 99, no. 3, pp. 32-44, 2003.

[15] Por L., Beh D., Ang T., and Ong S., "An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm," *The International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 51-60, 2013.

[16] Shih F., *Digital Watermarking and Steganography Fundamentals and Techniques*, CRC Press, 2007.

[17] St alling W., *Cryptography and Network Security-Principles and Practices*, Pearson Prentice Hall, 2006.

[18] Salivahanan S., *Digital Signal Processing, Tata McGraw-Hill*, 2000.

[19] Sajedi H. and Jamzad M., *Secure Cover Selection Steganography*, Springer Link, 2009.

[20] Yang C., "Inverted Pattern Approach to Improve Image Quality of Information Hiding by LSB Substitution," *Pattern Recognition*, vol. 41, no. 8, pp. 2674-2683, 2008.

Jithesh Korothan has been working as assistant professor in Computer Science, Mahatma Gandhi College, Iritty,Kerala,India. He is currently pursuing his PhD at RTM Nagpur University, Maharashtra, India.

Shirivas Kishore has been working as an assistant Professor and HOD in Computer Science in Sardar Patel Mahavidyalaya, Chandrapur since 1997. He has been awarded Ph.D. in Management by R.T.M. Nagpur University and Ph.D. in Computer Science by JJT University, Rajasthan, India.

Pradeep Butey Research supervisor and HOD, Dept.of Computer Science, Kamala Nehru College, Sakkardara Square, Nagpur-09. He has got 25 years of teaching experience. He has been awarded PhD in Computer Science.