

An Enhanced Steganographic System for Data Hiding in True Color Images

Saad M. Darwish¹, Shawkat K. Guirguis¹, Wesam A. Alatafy²

¹ Department of Information Technology, Institute of Graduate Studies and Researches,
Alexandria University, Egypt

² Departments of Astronomy and Space, College of Sciences, University of Baghdad, Baghdad, Iraq
Saad.saad@alexu.edu.eg, shawkat_g@yahoo.com, wesamiq@yahoo.com

ABSTRACT

The process of information propagation through the Internet may expose it to risk by discovering and stealing. Steganography is the art of hiding the existence of data in another transmission medium to get secret communication. There are several challenges facing the process of data hiding in images, such as embedding capacity, image quality, security, and computational complexity. In order to handle these challenges, this paper brings out a new data hiding system for true color images. The proposed system combines the merits of imperceptibility feature of LSB technique working in spatial domain with robust embedding policy based on salient features guided by human visual perception extracted from transform domain. The system translates the images into HSV color space that has the ability to isolate chromatic and achromatic components with the aim of increasing hiding quality. To improve security of embedding locations, the system uses secret-key for wavelet decomposition. In our case, adaptive LSB substitution method is employed to increase data hiding capacity and reduce embedding and extraction complexity. Final experimental results show the efficiency of the proposed system in terms of security, embedding capacity and the data hiding effect is quite invisible.

KEYWORDS

Steganography; LSB technique; Data hiding; Lifting wavelet; High embedding capacity.

1 INTRODUCTION

Security for data transmission is commonly very important issue in modern communication system. Steganography denotes to the art of "invisible" communication. The vital aim in steganography is to hide the very existence of the message in the

cover medium [1]. Steganography and cryptography are counterparts in digital security; the clear advantage of steganography over cryptography is that messages do not appeal attention to themselves, to messengers, or to receivers. Cryptography takes a file and transforms it, through a cryptographic algorithm, into a new encrypted file, but steganography hides a file within another file. The various applications of steganography include protected military communications, multimedia watermarking and fingerprinting applications for authentication purposes to regulate the problem of digital piracy [2].

Steganography and watermarking are two key partitions of data hiding technology. Each has its exact purposes. In the first partition, purpose of embedded data is to transmit secret communication and to avoid drawing doubt to the transmission of a hidden message. In the second division, purpose of embedded data is to supply some supplementary information about the cover media such as media owner. Furthermore, steganography pays care to the degree of hidden while watermarking pays most of its characteristic to the robustness of the message and its aptitude to combat removal attacks [3].

In general, data hiding procedure have three essential parts: the data to be hidden (secret data), the cover file (cover carrier), in which the secret data are to be embedded, and the resulting stego-file (stego-carrier) [2]. A good data hiding method should be one that can embed as much data as possible (embedding capacity), and the perceptual distortion of the digital content after the embedding process should be as miniature as

possible (invisibility). Digital images are considered good cover carriers because of their insensitivity to human visual system.

Image data hiding is an application of the steganography; its purpose is to embed a huge volume of data in images in an imperceptible way. There are many challenges facing the process of data hiding in images: (1) Embedding volume: it refers to the amount of data that can be interleaved into the image without fading its integrity; (2) Perceptual transparency: it is necessary that to avoid suspicion, the embedding should arise without significant deficiency or loss of perceptual quality of the image; (3) Robustness: it mentions to the ability of embedded data to stay undamaged if the stego-image suffers from various transformations such as scaling, rotation, cropping or compression; (4) Tamper resistance: it denotes to the difficulty to change or forge a secret message once it is embedded in a cover image; (5) Computational complexity: complexity of hiding technique employed for encoding and decoding is another issue and should be given significance [3], [4].

Recent methods for the embedding of data into the cover image fall into four classes [5], [6]: (1) Spatial-based scheme embeds the data into the pixels of the cover image directly. It is a simplest method for data hiding that has higher capacity but it is very weak in resisting even simple attacks such as compression; (2) Transform-based scheme embeds the data into the cover image by modifying the coefficients in a transform domain (e.g. Discrete-Cosine transform or Wavelet transform). Such technique is very secure and has certain robustness against some image processing, while its disadvantage is that it is computationally complex; (3) Spread spectrum scheme embeds the data over a wide frequency bandwidth than the minimum required bandwidth to send the information. In such technique, without destroying the cover image, it is very difficult to remove message completely. Nevertheless, this technique has a clear disadvantage in that the maximum distortion introduced by the embedding is not limited; (4) Distortion scheme embeds the data by signal distortion. The embedding process adds

sequence of changes to the image and the extraction process checks for the various differences between the original image and the distorted image to recover the secret message. This type of technique needs original image for information extraction.

In this work a specific steganographic system for hiding data in the spatial domain for true color images has been proposed. A color space mapping technique has been hired for embedding into predefined color channels to diminish degradation or damage of perceptual quality of the image. To reduce computational complexity, the system employs least significant bit (LSB) technique for embedding and extraction in predefined pixels, which corresponding to salient features that are related to some wavelet subbands' coefficients. Furthermore, to prevent illegitimate access of the data and get well embedding results, parameterized wavelet transform with an optimal LSB substitution method is utilized.

The outline of reminder of this paper is as follows. Section 2 presents a summary of the state-of-the-art image data hiding approaches. Section 3 describes the proposed system. The test results and discussion are shown in section 4. A short summary of this paper and outlook of future work are given in section 5.

2 LITERATURE REVIEW

A number of techniques have been implemented for improving image data hiding. They tried to defeat two major problems: the size of the hidden data and the security of that data against attackers. A diversity of these approaches in spatial domain has been suggested in the literature. Many of these works explicitly consider the data hiding by using LSB planes through directly replacing the LSBs of the cover-image with the message bits [7], [8]. These techniques are based on the idea that marginally modification of the pixels with a wide range of values will not cause perceptible distortion. LSB techniques usually are simple and fast to implement. They also permit for a relatively great payload and do not change the size of the image file. However there are several

disadvantages to these approaches such as the insertion is susceptible to slight image operation like cropping and compression and the hidden message can be damaged by the intruder by means of altering the LSB of all image's pixels.

Currently four different LSB-based hiding algorithms have been employed, which are: blind hide, hide seek, filter first, and battle steganography algorithms [5], [6], [7]. The first algorithm blindly hide the message since it just starts at the top left corner of the image and works across the image pixel by pixel. As it goes along, it adjusts the LBS of the image pixels to match the message. The second algorithm arbitrarily allocates the message across the image. It uses a password to create a random seed, and then utilizes this seed as a subject to the first position to hide in. It remains to randomly generate positions until it has finished hiding the message. It's still not the best method as it is not looking at the pixels used for hiding - it might be more suitable to figure out areas of the image where it is better to hide in. The third algorithm filters the image using one of the built-in filters and then hides in the highest filter values first. It has less observation on an image because using the filter guarantees that hiding is in the parts of the image that are the least visible. Finally, the fourth algorithm firstly filters the image and uses the uppermost filter values as "ships". The algorithm then randomly "shoots" at the image and when it finds a ship it groups the shots nearby that hit in the hope of sinking the ship. It is secure because you need a password to recover the message. Also, it is fairly effective because it hides the bulk of the information in the best areas.

Regarding the above classes, many researchers have developed algorithms to hide data in image. For instance, authors in [1] presented an algorithm for data hiding in binary images that assured the security and invisibility. To conceal data, no key is needed rather this algorithm that is based on the number of occurrence of 0s and 1s in data that has to hide and number of occurrence of 0s and 1s in the last bit of each pixel of binary image file. The main problem is the limited data that can be hidden because it is designed to work just on the

binary images. Mohamed M. et al. [7] suggested an approach for gray scale image that compacts with three main steganography challenges (capacity, imperceptibility, and security). This is attained by hybrid data hiding scheme that joins LSB technique with a key-permutation method. The authors also offered an optimal key permutation method using genetic algorithm for best key selection. Their experimental results showed decrement in computation time when increasing number of keys, at the same time system security improved. An improvement to the previous techniques is offered by J. M. Ahmed et al. [8] via accidentally embedding the bits of the message (instead of sequentially) in the image to yield more secured system. In this case, the embedding of message bits into the image is not only in the least bit but also in the other bits in the pixel in a random way.

In the same direction the authors in [9] presented a new method to embed a gray image into a grayscale cover image (data hiding by gray level modification). The method was designed in such a way that the gray value of every pixel of the secret image is conserved, i.e. no alteration will be generated in the secret image when it is extracted out from the cover-image. On the other hand, because the resulting cover-image usually holds a large quantity of embedded data, it may extremely be corrupted. Their method is faster and makes a little variation to the cover image that is indistinguishable by human eyes. From another perspective, the pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. In the extraction phase, the original range table is necessary to divide the stego-image by the same way as used to the cover image. This method can successfully bring both high embedding capacity and outstanding imperceptibility for stego-image but it is blind [9].

On the topic of transform-based data hiding methods, in the literature, the most used transformation functions include discrete cosine transform (DCT) and discrete wavelet transform

(DWT) [10-12]. The basic approach for hiding information with DCT and DWT is to transform the cover image, pull the coefficients, and then upturn the transformation. If the choice of coefficients is good and the size of the changes is controlled, then the result is appealing near to the original. For example, the work presented in [10] proposed a novel high capacity data hiding method based on JPEG. The proposed method employs a capacity table to guess the number of bits that can be hidden in each DCT component so that substantial alterations in the stego-image can be escaped. This method does not embed the secret data in the high-frequency components in order not to enlarge the size of the stego-image. Their algorithm allows users to regulate the level of embedding capacity by using a capacity factor.

Another related work in [4] where the authors recommended high-capacity image steganography technique in gray scale images that uses pixel mapping method in integer wavelet domain with tolerable levels of imperceptibility and distortion in the cover image and high level of total security. This method prepared for extracting the secret message without the cover image. The work in [12] offered a two stage (stego-based-crypto) invertible technique based on cryptography and steganography algorithms. In order to increase the security, their technique used RSA cryptographic algorithm in the first stage for encrypting the secret message, and Integer Wavelet Transform (IWT) based lifting scheme in the second stage as a steganography algorithm to hide the secret message. This algorithm affords good security, but the embedding capacity is restricted and the computational complexity is high. In recent times, many schemes unify both of spatial and frequency domain in a unified diagram to attain the advantages of both them. In this case the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels, see [4] for more details.

Surprisingly, in the literature, data hiding techniques that deal with the true color image are few and vary in their security, robustness and performance [13][14]. For instance, the authors in [13] considered an algorithm for data hiding in

RGB color images using LSB technique for red color channel only. Disadvantages of their method are mainly in the fact that it needs a fairly large cover image to create a practical amount of hiding space. Another work in [14], where an overlapping color palette partition based data hiding with improved secret embedding procedure has been presented. In their approach, a mapping function is considered to process color embedding for color that belongs to three color sub-palettes. The similarity of colors in palette is explored to produce any size of sub-palettes with large size to increase hiding capacity. Disadvantages of their method are mainly in the fact that it requires original image for the recovery of secret message.

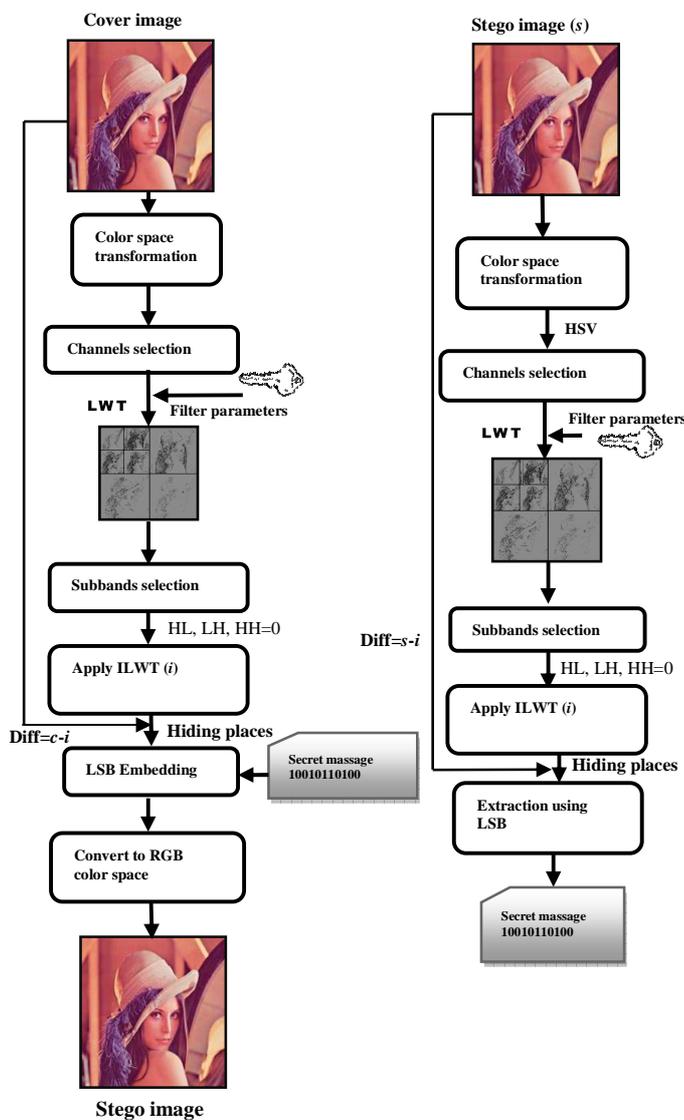


Figure 1. Proposed Data Hiding system.

The contribution of this paper is to develop a system for hiding information in true color images that tries to overcome the obstacles facing the previous techniques. The idea is that changing in the salient image pixels in specific image's color channels will not perceptually degrade the image. The robustness of the created system is realized by employing LSB substitution technique in various color channels and different least significant bits to increase hidden data capacity, whereas security is achieved by adapting a wavelet filter parameterization technique. Furthermore, this system requires no knowledge of the original image for the recovery of the secret image, yet yields high signal-to-noise ratios for the recovered output.

3 PROPOSED METHODOLOGY

To get a well balance between invisibility and hiding capacity, the suggested system exploits adaptive LSB substitution and human visual system features to develop a lossless data hiding system for color images. This system works in spatial-domain with the help of some information extracted from transform domain to choose the image's locations that will be used for embedding. This comes from our observation that different subbands of frequency domain coefficients give significant information about where salient and non-salient pixels of image reside.

The most important differences that distinguish the proposed system from existing state-of-the-art approaches are: (1) it works at a true color image and embedding process can be carried out in multi-color channel, thus increasing the hiding capacity; (2) more secure- it can battle a range of attacks (tamper resistance) by exploiting the concept of parametric wavelet filter; (3) the computational complexity is reduced because of working at spatial domain instead of transform domain, which is very complex, takes more time and makes more changes in the cover image; (4) the ability to support low invisible degradation because of utilizing color space mapping technique; (5) adaptive- the system takes statistical global features of the image before attempting to

interact with its LSB pixels. The system is driven by separate functions: adaptive excerpction of the place to conceal; adaptive excerpction of number of bits per pixel to conceal.

At first color conversion is applied on the input image through HSV color space. Secondly cover image is converted to transform domain. This is attained by applying parameterized DWT on cover image leading to four subbands. Then payload locations are determined depending on wavelet based salient points coefficients. Finally secret data embedding is performed in image pixels directly by locating those pixels corresponding to salient subbands' coefficients. The systematic block diagram of the proposed scheme is shown in Fig.1 and the following subsections briefly outline each step.

3.1 Embedding Steps

1. *Convert into HSV color space:* Change RGB color image into HSV color space. The HSV model separates out the luminance component (Intensity) of a pixel color from its chrominance components (Hue and Saturation). This representation is more similar to the human perception of color through eye cells [13]. In computer vision anyone often wants to separate color components from intensity for many reasons, such as robustness to lighting changes, or removing shadows. HSV is often used simply because code for conversion between RGB and HSV is commonly available and can be executed easily. In this research and through experiments, the proposed system can determine the best color channels that can be used in the process of concealment, and that do not result in any deformation regarding cover image visibility and quality of secret image after extraction.

2. *Apply wavelet filter parameterization:* Robustness of data hiding technique can be enhanced if properties of the cover image could be exploited. Taking this facet into consideration, working in transform domain becomes more attractive. The use of wavelet in image steganographic model lies in the fact that the wavelet transform clearly splits the high frequency

information (LH, HL, HH subbands) that hold the edges and textures of the image in different directions and low frequency information (LL subbands) that comprises the supreme energy of the image on a pixel by pixel basis[11].

The wavelet lifting scheme is a method for decomposing wavelet transform into a set of stages. The advantage of lifting scheme is that they do not need temporary storage in the calculation steps and has required less number of computation steps [15]. Filter parameterization is a technique that utilizes a secret-key for the wavelet decomposition of image. Introducing secret filter parameterization in wavelet based hiding algorithms has advantages of vast key-space that expands the hiding security, and also an adaptive way of building coefficients that raises the hiding robustness against specific attacks. In the proposed system, a secret wavelet filter is chosen in order to protect the location of the embedding information. Formally, given N parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$ the recursion

$$c_0^0 = \frac{1}{\sqrt{2}} \quad \text{and} \quad c_1^0 = \frac{1}{\sqrt{2}},$$

$$c_k^n = \frac{1}{2} \left(\begin{array}{l} (c_{k-2}^{n-1} + c_k^{n-1})(1 + \cos \alpha_{n-1}) + \\ (c_{2(n+1)-k-1}^{n-1} + c_{2(n+1)-k-3}^{n-1})(-1)^k \sin \alpha_{n-1} \end{array} \right) \quad (1)$$

can be used to determine the filter coefficients c_k^N , $0 \leq k < 2N + 2$ and $c_k = 0$ for $2N + 2 \leq k < 0$. The parameter values used for construction and the resulting wavelet filter coefficients are kept secret. For implement lifting wavelet transform, the Cohen-Daubechies-Feauvean (CDF9/7) wavelet filter is selected due to its best performance.

Since human eyes are much more sensitive to the low frequency part, the proposed system can hide secret message in image's pixels that are related to the salient features placed in the high frequency's portions without making any alteration in the approximation (LL) subbands [11]. By doing this, the system can easily make variations in image data with low perceptibility. As shown in Fig.1, firstly the selected color channel for the

cover image is transformed into wavelet coefficients by one-level parametric lifting wavelet transform with a secret-key. Then, the three high-frequencies subbands are set to zero. The reference image is obtained by inverse lifting wavelet transform. By computing the difference between the original image and its reference image, the hiding locations are acquired. In summary, exploiting the spatial-frequency properties of the wavelet transform can help the system to define the best locations for data hiding, so that significant distortions in the stego-image can be avoided.

3. *Use LSB to embed data:* After choosing the places of concealment (pixel indicator) with the help of wavelet theory, LSB technique is used for embedding data. LSB insertion method is simple and the most well-known Steganography technique. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision when applying LSB technique to each byte of an 8-bit image. For adaptive-ness, the proposed system uses 1, 2, or 3 least significant bits of the cover image to increase the storage capacity of the concealed data. In the LSB, according to the bits 0 or 1 in message LSB is being changed. If message bit is 0 then LSB is remained the same and if message bit is 1 then LSB is changed to 1. By doing this change, the image becomes a bit different than the original version. The decision of whether to use the 2nd or 3rd bit is based on the experiments. Readers looking for more information about LSB methodology can refer to [16].

3.2 Extraction Steps

By doing the same sequences of steps required to determine the embedding locations, the secret image will be extracted. As shown in Fig.1 the received stego image, which may be attacked is firstly converted to HSV color space and then the predefined color channel is transformed into wavelet coefficients by one-level parametric integer lifting wavelet transform with a suggested secret-key α , in embedding process, to deal with the correct location of the secret message.

Then, the three high frequency vertical, horizontal, and diagonal subbands are set to zero. Perform the inverse wavelet transform and obtain the reference image. As in embedding process, the computed difference between the color channel's image and its reference image is utilized to achieve blindness of the proposed system. According to the sequence of embedding locations, the hidden data is gained by the LSB extraction process.

4 RESULTS

In this section the authors present the experimental results of the proposed system based on two benchmarks to evaluate the hiding performance. First one is the capacity of data hiding and another one is the imperceptibility of the stego image, also called the quality of stego image. The stego-image should be acceptable by human eyes (qualitative) and by peak signal to noise ratio PSNR in decibels (quantitative). Experimental results are shown based on many well-known images that have different features as shown in Fig. 2

Table 1 shows PSNR results that measure the percentage of the stego data (see Fig.3) to the image data. Results show high PSNR values, which range from 56 to 64 dB and verify that the proposed system is unimpaired according to secret images with different sizes. In the literature, PSNR values above 50 dB consider good quantity for the quality of the image after embedding [4][5]. Fig. 4 shows stego-image produced by the proposed system. Human eyes cannot notice any visual distortion from the stego-image, which indicates that our system can obtain good transparency.

To clarify the most important HSV color channels that can be used in the process of data hiding, we embedded different secret images inside different color space channels of different cover images and observed average PSNR values for the resulted stego-images. As shown in Table 2, the system achieves high values for different channels (imperceptibility) but regarding the quality of the extracted secret image; we can observe that

V color channel still get the best extraction's quality (about 64dB) as shown in Fig. 5 .



Figure 2. Set of the cover images used in the process of embedding (512x512).

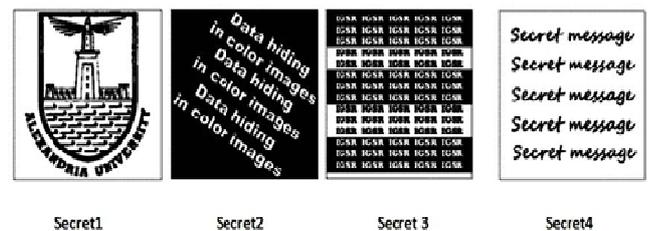


Figure 3. Set of the secret images used in the process of embedding (binary).

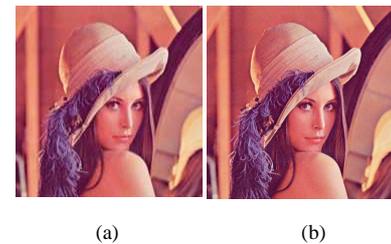


Figure 4. (a) Cover Lena image; (b) Stego-image after embedding secret image

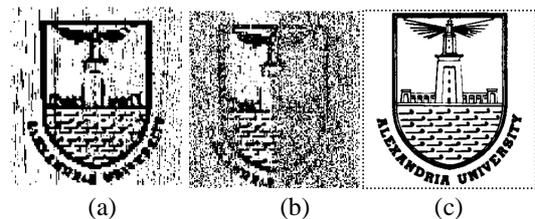


Figure 5. Secret image extracted from (a) H; (b) S; and (c) V channels.

Table 1 shows PSNR results that measure the percentage of the stego data (see Fig.3) to the image data. Results show high PSNR values, which ranges from 56 to 64 and verify that the proposed system is unimpaired according to secret images with different sizes. In the literature, PSNR values above 50 consider good quantity for the quality of the image after embedding [4][5]. Fig. 4 shows stego-image produced by the proposed system. Human eyes cannot notice any visual distortion from the stego-image, which indicates that our system can obtain good transparency.

To clarify the most important HSV color channels that can be used in the process of data hiding, we embedded different secret images inside different color space channels of different cover images and observed average PSNR values for the resulted stego-images. As shown in Table 2, the system achieves high values for different channels (impressibility) but regarding the quality of the extracted secret image; we can observe that V color channel still get the best extraction's quality (about 64 dB) as shown in Fig. 5 .

To test the ability of the proposed system for increasing the hiding capacity based on the number of bits per pixel to conceal; we embedded two different secret images with the same size within one cover image. Two secret images are embedded into two different LSB up to the third bit because there is little change of the pixels' values at this point. From the results listed in Table 3; we can notice that, embedding in 1st bit and 2nd bit respectively yields the best PSNR results. Still, other LSBs also can achieve considerable PSNR values when compared to existing systems but with the difference that the suggested system can achieve an increase in the capacity of concealment at a rate of up to 50% increase for other methods.

Table 4 shows the average value of the computation time for embedding and extraction of different secret image with different size over ten runs. As expected, by increasing embedding capacity, the computation time is increased with trivial values. This is due to the simplicity and

high computational speed of the employed lifting wavelet transform. These results reveal the ability of the proposed system to be implemented in real-time applications. The whole software component is implemented using MATLAB[®] release R2011b on HP Pavilion dv6 Notebook PC with Intel Core™ i7 CPU @ 2.20 GHz @2.20 GHz processors, 8 GB memory and 40 GB HD running Microsoft Windows 7 home premium SP1.

Table 1. PSNR Results for Different Secret Images within Different Cover Images (dB).

Cover / Secret Images	secret images of size (150x150)				secret images (200x200)				secret images (250x250)				secret images (300x300)			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Lena	64	64	64	64	61	61	61	61	59	59	59	59	57	57	57	57
Baboon	62	62	62	62	59	59	59	59	58	58	58	58	56	56	56	56
Peppers	64	64	64	64	61	61	61	61	59	59	59	59	57	57	57	57
Jet	62	61	62	62	59	59	59	59	57	57	57	57	55	55	55	55
Boat	62	62	62	62	60	60	60	60	58	58	58	58	56	56	56	56
Football	63	63	63	63	60	60	60	60	58	58	58	58	56	56	56	56

Table 2. Average PSNR(dB) Results for Different Color Space Channels.

HSV color space	PSNR
H	54
S	64
V	65

Table 3. Average PSNR (dB) Results for Different 3- LSBs.

Selected bits	PSNR(dB)
1bit +2bit	58
1bit +3bit	52
2bit +3bit	52

Table 4. Average time (Sec) for Embedding and Extraction of Different Secret Images with Different Size.

Size of the secret image	Time(Sec)
150	1.3
200	1.4
250	1.4
300	1.6

Regarding system security, steganography that uses a key has a better security than non-key steganography. This is so because without the knowledge of the valid key of wavelet parameterization, it is difficult for third party or invaders to recover the embedding locations of the message. Hence, the system represents the more secure communication way compared to original

LSB. In other words, by embedding data in only certain region (salient features) and not in whole image the security is enhanced (tamper resistance).

5 CONCLUSION AND FUTURE WORKS

In this paper, an efficient steganographic system for embedding secret messages into true color image without producing any major change has been proposed. To increase the system performance in terms of both capacity and security; the method of optimal LSB substitution is presented in combination with parameterization-based lifting wavelet transform. The proposed system allows complete recovery of the original host image with small visual distortion in stego-images because of consideration of human perceptual factor that is inherited from HSV color space of image. In addition, the system is able to extract the secret message without the cover image.

Extensive experiments show advantages of our lossless color image data hiding system for providing good image quality and large message capacity as well as increasing in the system immunity to specific range of attacks. The proposed system is very practical for most image files that are stored and transmitted in the PNG and BMP format. In the future, we intended to extend our system to hide gray scale and color images as secret message and to increase the system ability to deal with geometric and processing attacks.

6 REFERENCES

1. Bhattacharyya, D., Roy, A., Roy, P., Kim, T.: Receiver Compatible Data Hiding in Color Image. *International Journal of Advanced Science and Technology*, Vol. 6, No. 1, pp. 15 - 24, (2009).
2. Jiang, M.: A High-Capacity Lossless Data Hiding Scheme for Binary Images. *International Journal of Digital Content Technology and its Applications*, Vol. 5, No. 12, pp. 43- 50, (2011).
3. Bedi, S.S., Verma, S., Tomar, G.: An Adaptive Data Hiding Technique for Digital Image Authentication", *International Journal of Computer Theory and Engineering*, Vol. 2, No. 3, pp. 338- 344, (2010).
4. Bhattacharyya, S., Sanyal G.: Data Hiding in Images in Discrete Wavelet Domain Using PMM. *International Journal of Electrical and Computer Engineering*, Vol. 5, No. 6, pp. 359-367, (2010).
5. Umamaheswari, M., Sivasubramanian S., Pandiarajan S.: Analysis of Different Steganographic Algorithms for Secured Data Hiding. *International Journal of Computer Science and Network Security*, Vol. 10, No .8, pp. 154 - 160,(2010).
6. Akeem, A.O., Olatunji, J.O., Latifat B.A.: A Framework for Multimedia Data Hiding Security. *International Journal of Computer Science and Network Security*, Vol. 11, No. 12, pp. 99- 104, (2011).
7. Mohamed, M., Al-Afari, F., Bamatraf, M.: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. *International Arab Journal of e-technology*, Vol. 2, No. 1, pp. 11-17, (2011).
8. Ahmed, M.J., Ali, M. Z.: Information Hiding using LSB Technique. *International Journal of Computer Science and Network Security*, Vol. 11, No. 4, pp. 18-25, (2011).
9. Ahmadi K.: A New Method for Image Security and Data Hiding in Image. *American Journal of Scientific Research*, Vol. 24, No. 38, pp. 41-49, (2011).
10. Hsien-Wen, T., Chin-Chen, C.: High Capacity Data Hiding in JPEG-Compressed Images. *International Journal of Informatics*, Vol. 15, No. 1, pp. 127–142, (2004).
11. Anjali, A.S., Umesh, L.K.: A Secure Skin Tone based Steganography Using Wavelet Transform. *International Journal of Computer Theory and Engineering*, Vol. 3, No. 1, pp.16-22, (2011).
12. Adnan, M. A., Brifcani, W.M.: Stego-Based-Crypto Technique for High Security Applications. *International Journal of Computer Theory and Engineering*, Vol. 2, No. 6, pp. 835-841, (2010).
13. Du, X. L. ,Li, W., Lu, P.: Multi-Channel Data Hiding Scheme for Color Images. In: *Proc. International Conference on Information Technology: Coding and Computing (ITCC 2003)*, pp. 569 – 573, USA, 28-30 April (2003).
14. Li, Y.-C., Sai, P., Lin, C.-H., Yeh, H. -L.: Palette Partition Based Data Hiding for Color Images. In: *Proc. Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '09)*, pp. 620 – 623, Japan, 12-14 Sept. (2009).
15. Saad, S.M.: Design of a Robust and Secure Digital Signature Scheme for Image Authentication over Wireless Channels. *IET Information Security*, Vol. 3, No.1, pp. 1– 8, (2009).
16. Gupta, S., Handa, A., Sandhu, P.: Implementing Adaptive Steganography by Exploring the Ycbr Color Model Characteristics. *World Academy of Science, Engineering and Technology* 46, pp. 765-768(2010).