*Bulletin de la Société Royale des Sciences de Liège, Vol.* 85, 2016, *p*. 1465 - 1474

# A Comparative Study of Image-In-Image Steganography Using Three Methods of Least Significant Bit, Discrete Wavelet Transform and Singular Value Decomposition

Mohammad Shahab GOLI[1,*], Alireza NAGHSH[2]

[1]M.Sc. student of Optical Telecommunications at Faculty of Electrical Engineering, Islamic Azad University, Najaf Abad Branch, Isfahan, Iran.
[2]Associate professor at Faculty of Electrical Engineering, Islamic Azad University, Najaf Abad Branch, Isfahan, Iran

[*]Corresponding author: m.shahabgoli0015@yahoo.com

**Abstract**

Today, with the growth in application of communication equipment as well as the use of Internet for information exchange, the need for data security and protection is felt more than before. Various methods have been proposed in recent years to realize this goal. One efficient, widely used method is hiding of information within data of insignificant value. An image, due to its large amount of information, may embed different data within, hence providing a decent safety margin for critical data. Three methods, including least significant bit (LSB), discrete wavelet transform (DWT) and singular value decomposition (SVD) were used in this study for image-in-image steganography. Each method has advantages and disadvantages. Advantages of LSB include high capacity and simplicity, however, as for the disadvantages, it is vulnerable against attacks such as cropping, salt and pepper noise, and compression. Therefore, the other two methods, DWT and SVD, which are robust against the mentioned attack, are used as steganography in frequency domain. Among the methods used in this study, SVD least affects the host image, making it more suitable as compared with its other two counterparts.

**Keywords:** Image, host image, watermark image, space domain, frequency domain, digital image watermarking

## 1- Introduction

Today, as a widely used communication system, the Internet is very popular among people. The goal in a communication system is transmission of information from one point to another. The information may contain sound, text, video and image, which are referred to as data [1].

Data quality and security are two main factors in delivery of information. Thanks to the development of technology, new devices are expected every day which aim to promote the quality of different data, however, security, on the other hand, is another important issue in transfer of information. Encryption and information hiding are two proposed methods for increasing data security. In encryption, the data is secured against threats and attacks by a

password. Although encryption has been used widely throughout history, it cannot guarantee the security of data once the key is revealed. Therefore, hiding of information is used as a countermeasure.

Information hiding means prevention of access to critical information by embedding them within data of insignificant value. Information hiding methods include cryptography and watermarking [1]. In cryptography, the conveyed message must remain imperceptible, while in watermarking, it can either be perceptible or imperceptible. watermarking means embedding of information within insignificant data, through which security of data transfer is increased. In watermarking, the important information which is to be protected is known as watermark information, and the data within which this information is to be embedded is known as host data. Stages of watermarking are demonstrated in Fig. 1.

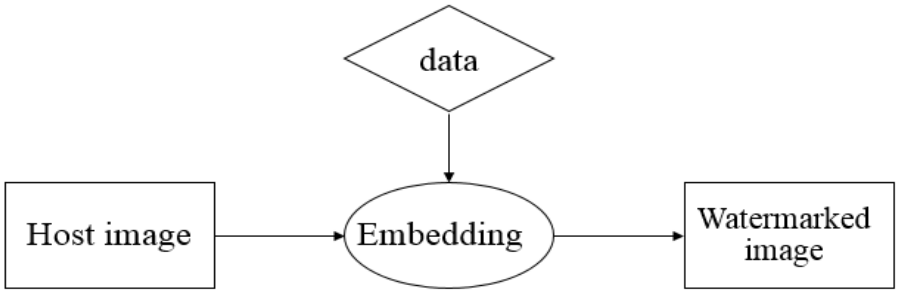



**Figure 1:** Stages of watermarking of data within an image.

Digital watermarking means embedding of critical information within binary structure of the host data [2]. The host may be in different formats such as sound, text, video and image. In case an image is used as the host, the procedure is known as image digital watermarking [3]. An image, due to its large volume size, is considered a suitable host for different information.

Different classifications exist for watermarking. From an application perspective, watermarking can be divided into space and frequency domains. Least significant bit is the most well-known method in space domain. Although benefiting from advantages such as rapidity, it is not vulnerable against space domain attacks including cropping, compression, and salt and pepper noise. In order to improve the robustness of watermarking against these attacks, another domain known as frequency domain is used. Frequency domain itself includes discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) [1].

In this study, image-in-image watermarking was carried out using three methods of LSB, DWT and SVD, and the results were then compared with one another.

## 2- Watermarking in space and frequency domain

### 2-1 Watermarking in space domain

In watermarking in space domain, watermark information is directly embedded within the host data. If an image is used as the host, it is first decomposed into its forming bits, and the watermark data are embedded within the lease significant value bits. Since lower-value bits

contain a small amount of host image information, embedding of other information within does not affect the overall structure of the host data, thereby enabling us embed some information within one another [4].

Although watermarking in space domain benefits from advantages such as simplicity, high capacity and proper speed, it is vulnerable against space domain attacks such as compression, pepper and salt noise and cropping. Its vulnerability against such attacks in space domain calls for a more secure domain known as frequency domain to better improve data security [5].

### 2-2 Watermarking in frequency domain

In this domain of watermarking, watermark data are embedded within the transformed format of the host image, thereby protecting the data against space domain attacks. watermarking in this domain includes different methods, among which DCT, DWT and SVD are widely used [6]. Two of these three were used in our study.

#### 2-2-1 Discrete wavelet transform

Discrete wavelet transform (DWT) is a watermarking method used in frequency domain. By applying DWT method to an image, it can be divided into four different bands in terms of frequency. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH), respectively, which are demonstrated in Fig. 2.

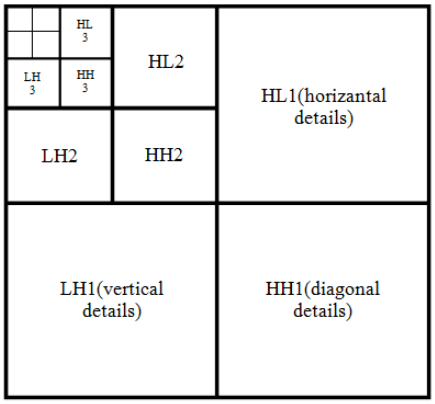



**Figure 2:** Image decomposition by applying DWT to an image.

A significant part of the energy in the original image is located in the approximate band (LL). As shown in Fig. 2, four new sub-partitions may be obtained by re-applying DWT on the approximate band, which contain lower levels of energy [6].

The watermark data may be multiplied by an alpha coefficient smaller than unit, and then be embedded within one of the above mentioned partitions to achieve watermarking. Equation 1 may be used for stepwise sub-partitioning of the image.

$$E_K = \frac{1}{M_K N_K} \sum_i \sum_j |I_K(i, j)|$$

(1)

where K is the number of decompositions, and $M_K$ and $N_K$ are the size of the sub-partition proportional to the value of K.

### 2-2-2- Singular value decomposition (SVD)

Every matrix may be expressed as multiplication of three matrices according to Equation 2.

$$A = USV^T \tag{2}$$

where U and V are orthogonal matrices, and S is a diagonal matrix of the same dimensions as A. Equation 2 may be used to conceal data within the host image to achieve watermarking. To this end, the host image should first be decomposed into three separate matrices using Equation 2, then Equation 3 is used for watermarking of the watermark data within the diagonal matrix of the host image [7, 8, 9].

$$S_N = S + \alpha \times W \tag{3}$$

where S is the resulting matrix obtained from applying SVD on the host image, $\alpha$ is value ranging from 0 to 1, and W is the watermark image. Similar to DWT, SVD is a watermarking method applicable in the frequency domain and is highly robust against different attacks. watermarking steps using SVD is shown in Fig. 3.

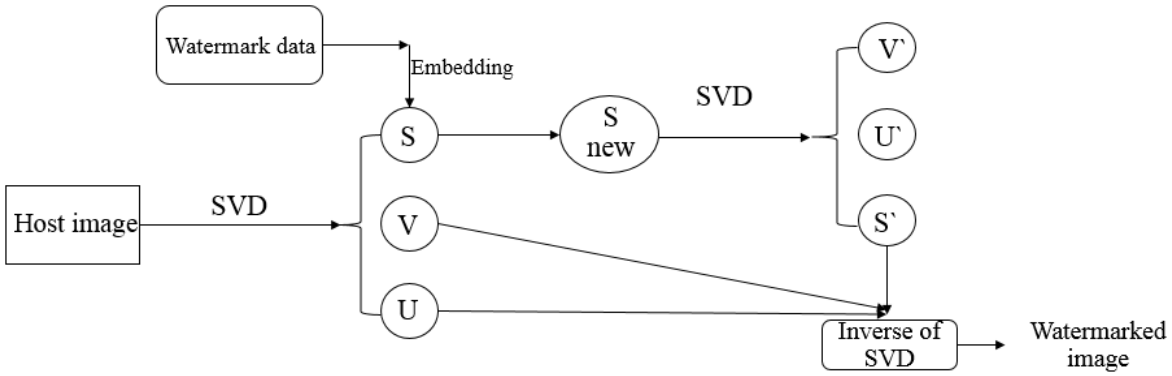
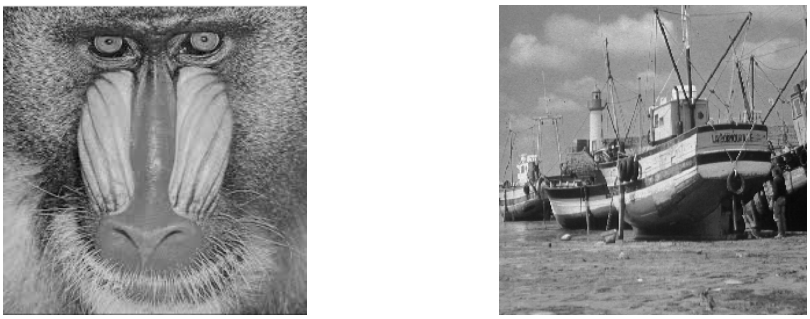



**Figure 3:** Stages of watermarking using SVD.

## 3- Image as a watermark

Image is one of the various data types. An image may be concealed within another using watermarking to be transmitted. Depending on the watermarking method of the origin, extraction procedure is carried out to retrieve the watermark image at the destination. In our study, a standard image was selected in MATLAB as the watermark image, and attempts were made for watermarking of this watermark image within another standard image, i.e. host image, using

LSB in the space domain and DWT and SVD in the frequency domain. Images of a baboon and a boat were used as the watermark and host image respectively. Each method is described in details in the following sections.

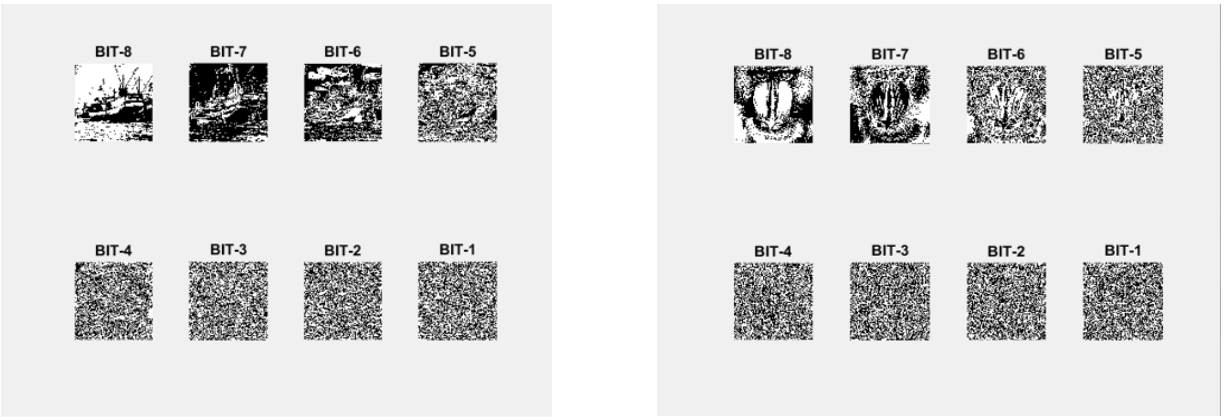


a **b**

**Figure 4:** a) Image of a baboon (watermark image), b) Image of the boat (host image).

### 4-1 Image-in-image watermarking using LSB method

There are columns and rows in each image in the form of a matrix, the arrays of which are called pixels. Each pixel is made up of 8 bits or 1 byte. As zeros and ones fill in each bit, the value of a bit is formed as a binary value. In LSB, the watermark image as well as the host image are decomposed into their forming bits. Figs. 5 demonstrate the decomposed images of the watermark and the host.




a b

**Figure 5:** a) Decomposed watermark image, b) Decomposed watermark image

Significant bits of the watermark image are then embedded within insignificant bits of the host image, as depicted in Fig. 6.

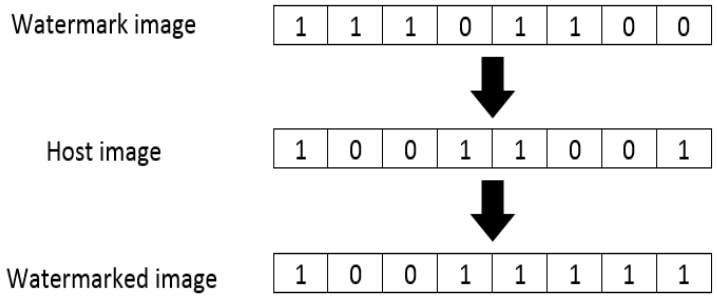



**Figure 6:** Embedded watermark image high-value bits in the host image

Least significant bits have little contribution in formation of an image, therefore, changes in them does not damage the overall structure of an image. 3 or 4 bits of the watermark image may be embedded within the host image. It should be noted that as the number of embedded bits increases, the quality of the extracted image also increases. On the other hand, this increase may also damage the host image. 3 embedded bits were considered in our study. Fig. 7 demonstrates the procedure of embedding 3 most significant bits of the watermark image into the host image.

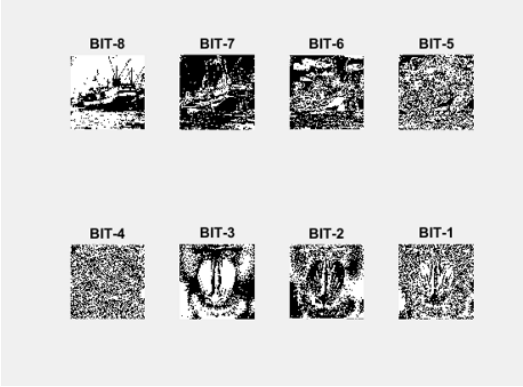



**Figure 7:** Embedding of 3 bits of the watermark image into the host image.

The watermarked image is sent to the destination after watermarking is performed. The watermarked image using LSB is demonstrated in Fig. 8. At the destination, the watermark image is decomposed into its forming bits, then its three least insignificant values, which are in fact the three significant values of the watermark image, are extracted. The extracted image is illustrated in Fig. 9.

**Figure 8:** The watermarked image using LSB.

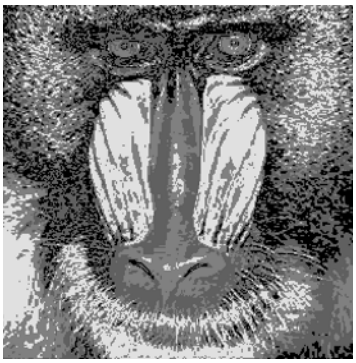


**Figure 9:** The extracted image using LSB method

As illustrated by the Fig. 9, the quality of the extracted image is lower than that of the watermark image, since only 3 bits of the watermark image are used.

### 4-2 Image-in-image watermarking using DWT method

The image of the boat is first partitioned into four different bands in terms of frequency by applying DWT. By re-applying DWT on the obtained approximate image (band), it is sub-partitioned into 4 new bands. The watermark image is then multiplied by a coefficient smaller than unit and is placed within the horizontal band. At the destination, the watermarked image is partitioned by twice application of the DWT method. The watermark image is then multiplied by the inverse of alpha and is extracted. The watermarked image and the extracted image are shown in Figs. 10 and 11 respectively.

**Figure 10:** The watermarked image using DWT method.

**Figure 11:** The extracted image using DWT method

### 4-3 Image-in-image watermarking using SVD

In this method, the host image is decomposed into three matrices using SVD method. The watermark image is then embedded into the diagonal matrix using Equation 3. The watermarked image is then created using the inverse of the SVD method. In order to extract the watermark image, first SVD method is applied on the watermarked image, then the desired image is extracted using the resulting diagonal matrix as well as Equation 3. Figs. 12 and 13 show the results of this watermarking method.

**Figure 12:** The watermarked image using SVD method

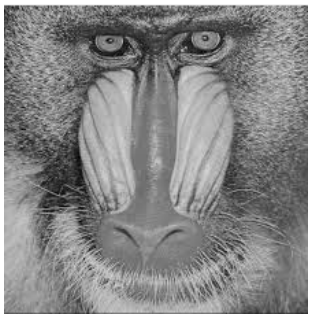


**Figure 13:** The extracted image using SVD method

## 5. Conclusion

There are metrics available to assess performance of watermarking methods, enabling us to compare different methods. Peak signal-to-noise ratio (PSNR) is one of these metrics.

**Table 1:** PSNR metric and its mathematical relations.

| Assessment metric | Mathematical relation |
|---|---|
| PSNR | $10 \times LOG_{10} \frac{\left(MAX_I{}^2\right)}{MSE}$ |

Comparison results of the three watermarking methods used in this study with respect to PSNR metric are given in Table 2.

**Table 2**: Comparison of different watermarking methods with respect to PSNR metric.

| Watermarking methods | PSNR |
|---|---|
| LSB | 38.2717 dB |
| DWT | 30.2722 dB |
| SVD | 66.6591 dB |

Three image-in-image watermarking methods were investigated in this study. LSB method is a watermarking method applicable in space domain, the implementation of which is very easy. In addition to its simplicity, although the method presents high capacity as well as speed, it is vulnerable to spatial domain attacks. Frequency domain was then proposed to address this issue, and two of its widely used methods were investigated. These two methods are robust against cropping, compression and salt and pepper noise attacks, and can protect critical data against attacks of such type. The mentioned three methods are widely used. According to the results in Table 2, the value of PSNR metric for SVD method was higher than those of the other two

methods, showing that watermarking using this method imposes less damage to the host image, i.e. the host image is altered less as compared with the other two methods. Therefore, use of SVD for watermarking delivers better performance as compared with the other two methods, as PSNR metric shows.

**References**

1. Seyed Mojtaba Mousavi, Alireza Naghsh, "Watermarking Techniques used in Medical Image:a survey", Journal of Digital Imaging, Volume 27, Issue 6, pp 714-729, December 2014.
2. Pan W, Coatrieux G, Cuppens-Boulahia N, Cuppens F, Roux C,"Medical image integrity control combining digital signature andlossless watermarking, in Data Privacy Management andAutonomous Spontaneous Security In"Garcia-Alfaro J, et al Eds.Springer Berlin: Heidelberg, 2010, pp 153–162.
3. Vinita Gupta, Atul Barve, " A Review on Image Watermarking and Its Techniques",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 1, January 2014.
4. Wu N-I, Hwang M-S "Data hiding current status and key issues" Int JNetw Secur 4(1):1–9, 2007
5. Muralikrishna Nangedda, Reddy A Sudharsan, " Medical Image Steganography with Digital Water Marking", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 7, July 2014.
6. Heylena K, Dams T"An image watermarking tutorial tool usingmatlab" Mathematics of Data/Image Pattern Recognition,Compression, and Encryption with Applications XI, Proc. of SPIE2008. 7075, 70750D: p. 1–12.
7. Ali M, Ahn CW, Pant M" A robust image watermarking techniqueusing SVD and differential evolution in DCT domain". Opt Int J LightElectron Opt 125(1):428–434, 2014
8. Arsalan M, Malik SA, Khan A" Intelligent reversible watermarking ininteger wavelet domain for medical images". J Syst Softw 85(4):883–894, 2012
9. Agreste S, Puccio L"Wavelet-based watermarking algorithms" theory,applications and critical aspects. Int J Comput Math 88(9):1885–1895, 2011