EasyChair Preprint

№ 2177

# Steganography and its Advancements in Spatial Domain

Mallika Garg, Jagpal Singh Ubhi and Ashwani Kumar Aggarwal



December 16, 2019

# Steganography and its Current Advancements in Spatial Domain

Mallika[1], Jagpal Singh Ubhi[2] and Ashwani Kumar Aggarwal[3]

[1]Electronics and Communication Department, IIT Roorkee, India
[2]Electronics and Communication Department, SLIET, Longowal, Punjab, India
[3] Electrical and Instrumentation Department, SLIET, Longowal, Punjab, India
[1]mallikagarg49530@gmail.com
[2] js_ubhi@yahoo.com
[3]ashwani.ist@gmail.com

**Abstract- In the modern era, with the advancement of wireless communication, and Digital Signal Processing (DSP) techniques, enormous data is exchanged over the internet by many users which can be accessed worldwide that increases the possibility of attack over network. Many techniques are developed in the past that protect data from such attacks. Steganography is one of the popular techniques that protect data from unauthorized persons. It has increased to a great extent for transferring secret information by wrapping the secret data into another data for security. Generally, bits are replaced in the least significant bits and this technique is known as Least Significant Bit (LSB) steganography. The primary goal of steganography is to protect data in such a way that attackers do not know the existence of the secret content in the cover data. Also, steganography also takes care that modification in cover object should be indiscernible by the subjective testing. Steganography can be easily used along with other data security techniques to improve the performance of the system. This paper provides a review of various steganographic techniques in spatial domain. It also illustrates the different types of steganography, its applications, advantages, disadvantages and various performance evaluation parameters.**

**Keywords:** *Steganography, spatial domain, stego-image, cover image, data security.*

## 1. Introduction

The primary goal of steganography is to hide secret data within some other data. Its secondary goal is to prevent withdrawal from the cover file without devastating the host and prevent destruction of the stego-message without destroying the host. In steganography, the message itself may not be difficult to detect, but most of the people who are not intended to be recipients of the message not even detect the existence of hidden message. Steganography means not to alter the structure of the secret information, but hides it inside a cover-object (carrier object). Steganography exploits human perception for secret communication. Human senses are not taught to suspect and recognize information hidden inside them. Steganography is beneficial for securely storing secret data, such as hiding system in military communication [1].

The basic terms in steganography includes cover-object, message and stego- object as shown in fig. 1.

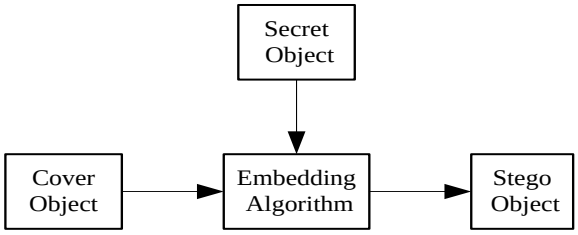


***Fig. 1.*** *Basic Terminologies.*

- Cover-object: Cover-object is basically the object in which the secret data is to be hidden. It is also called Host-object as it acts as host for the secret data.

- Message: The Secret data which is to be transmitted safely is known as Message. The secret data is nothing but the information which is hidden inside the cover-object.

- Stego-object: The cover-object carrying the secret message is known as stego-object. The resulting stego image is send to the receiver by the means of some transmission media.

## 2. Performance Evaluation Parameters and Conflicts

There are various performance evaluation parameters from which the technique can be categorized as an efficient technique.

*i) Imperceptibility:* Imperceptibility is the perceptual recognition by the human senses i.e. the alteration should not be noticed by the human vision. It should be as high as possible. The file with the embedded data and original data

source should be similar to the cover image. After embedding, perceptual quality of stego-image will degrade as compare to the cover- image.

*ii) Capacity payload:* Capacity payload refers to the maximum amount of secret information that a cover-image can hide before the distortions become observable. It can be represented in bits or bytes or kilobytes. Larger the capacity payload, better is the steganography technique. The data to be hidden in the carrier depends on the size of the carrier and the steganography method used to hide the secret information. There is always a compromise between the capacity payload and the imperceptibility that are both desirable but incompatible as with the increase in capacity payload imperceptibility decreases.

*iii) Computational complexity:* Computational complexity refers to the computational cost of embedding and extraction. It should be as low as possible.

*iv) Robustness:* After embedding, data should withstand changes if stego-image goes into some transformations such as cropping, sharpening, blurring, scaling, rotation, compression, filtering and the addition of different types of noise.

*v) Undetectability:* Undetectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed.

*vi) Accuracy:* The state of hidden information being correct or precise when extracted from the medium is called accuracy.

*vii) Secrecy:* Security of a steganographic system is defined in terms of undetectability, which is assured when the statistical tests cannot distinguish between the cover and the stego-image [2].

### *Conflicts among Parameters*

The main purpose of enhancing any steganographic method is to enhance its requirements or parameters in terms of undetectability, imperceptibility and capacity. Often, improving a certain parameter may affect the other parameter negatively. For example, the imperceptibility and capacity cannot be maximized at the same time. The amount of changes that occurs in the cover image by embedding are directly influenced by the amount and the content of the confidential information. As a result, there should be a compromise between these requirements. According to the requirement or application, the desired performance parameters of the Steganographic systems must be high. For example, digital watermarking requires high robustness.

## 3. Classification of Steganography

Steganography can be classified into various types depending on the host and the domain used for transmission of the secret information which are given below:

### *3.1. Based on Host*

According to host used, steganography is classified as text steganography, audio steganography, video steganography and protocol steganography.

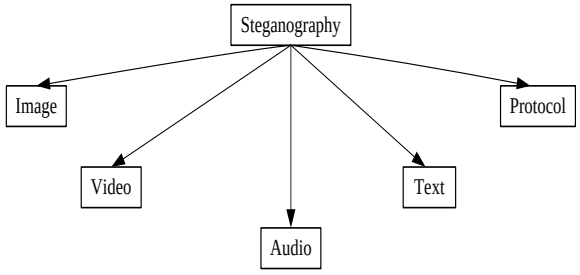


***Fig 2*** *Classification of steganography based on host*

*i). Image steganography:* If the data is hidden in the image then it is called image steganography. This is the most popular form of steganography. The images are represented in terms of the pixel where the value represents the color and intensity of the pixel.

*ii). Video steganography:* If secret data is hidden in the video then it is called video steganography without disturbing the original quality of the cover file.

*iii). Text steganography:* If steganography uses text to hide the data then it is called text steganography. It is the earliest and the most complex form of steganography. It can be applied in the digital format such as PDF.

- The following message was actually sent by a spy in WW I

"APparently nEutral's pRotest iS tHoroughly dIscounted aNd iGnored.
ISman hArd hIt. BLockade iSsue aFfects pRetext fOr eMbargo oN bYproducts,
eJecting sUets aNd vEgetable oIls."

- Taking the second letter in each word the following message emerges:

"Pershing sails from NY June 1."

***Fig 3** Example of Text steganography*

*iv). Audio steganography:* If the secret data is hidden in audio signal then it is called audio steganography. It can embed messages in WAV, H.264, Mp4, AU, and even MP3 sound files. Sampling and quantization are used for Audio Steganography. The secret audio information is embedded in the cover audio such that it is imperceptible to the human ears.

*v). Protocol steganography:* If steganography uses network protocols such as TCP, IP, UDP, ICMP, to embedding information then it is called as network steganography. We hide information in the header of a TCP/IP packet in some fields that are either optional or are never used.

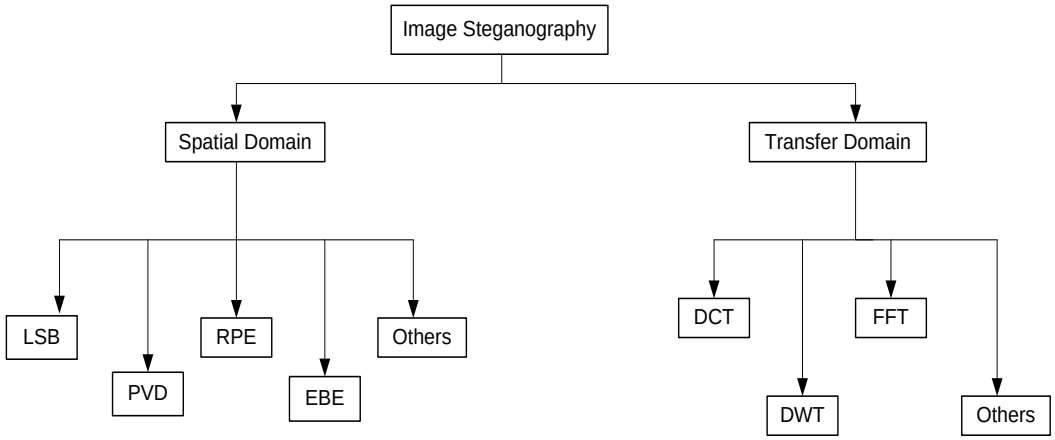


***Fig.4.** Classification of spatial domain image steganography techniques*

### *B. Based on Domain*

Based on domain, steganography is classified into two main types:

*i). Spatial domain:* In spatial domain, pixels of secret image are directly embedded in the intensity of the pixels of cover image. Spatial domain techniques encompass bit-wise methods that apply bit insertion and manipulation of secret or cover bits.

*ii). Transform domain:* In transform domain, also known as frequency domain, images are first transformed in other domain by applying transformation, then the secret image is embedded in the cover image in the transform domain. After embedding, the embedded image is again transformed. Steganography in the transform domain involves the manipulation of algorithms and image in the transform domain. The advantage of this technique over spatial domain techniques is that it hides information in areas of the image that are less exposed to compression, cropping, and image processing but it is complex as compared to spatial domain techniques. The various transform domain steganographic techniques are:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method.
5. Embedding in coefficient bits.

Data embedding in the frequency domain is more robust than in the spatial domain. However, when such techniques are used in which embedding capacity is higher, spatial domain schemes are used rather than frequency domain.

## 4. Spatial Domain Steganographic Techniques

There are many versions of spatial steganography, all directly alter bits in the image pixel values in hiding the data. Spatial domain techniques are broadly classified into:

*i). Least significant bit (LSB) steganography:* One of the simplest and very popular technique of steganography is Least Significant Bit (LSB) replacement. In this technique, least significant bit or bits of a pixel of the cover data are replaced by the bits of data to be hidden [1]. LSB can be extended up to 4 least significant positions of a byte, i.e. we can replace four bits of hidden data with the original value of a pixel, whose binary value is of 8 bits. As replacing four bits may cause distortion in an image due to noticeable change in its color and its pixel intensity, so replacing 2 bits is preferred in most of the applications. Least significant bit (LSB) based

steganography conceals the confidential information in the LSBs of pixels of the cover image without noticeable distortions. Changes in the values of the LSB are imperceptible to subjective analysis. The last bits of each byte is of least importance, as any modification in LSB has least effect on the content of byte which is not noticed by the human eye. The hiding capacity can be increased by using up to moderate bit least significant bits in each pixel.

LSB steganography has a weak point that its sample value changes asymmetrically [2]. When the LSB of cover image is same as that of the message bit to be embedded, no change is made in the LSB of the cover image. Otherwise the value 2n is changed to 2n+1 or 2n+1 is changed to 2n. But the changes from 2n to 2n-1 or 2n+1 to 2n+2 will never happen. Increment or decrement in the values of the pixels by modifying the LSB of the cover image do not affect the intensity value of colors of the cover image, so much that the changes are visible to the human eyes. This implies that odd pixel intensity is always decreased by 1 whereas even pixels intensity is always increased by 1. So the resultant stego image resembles with the cover image. This asymmetry can be detected by simple steganalytic techniques. There are a lot of improvements and modifications proposed to strengthen this technique [3].

A new method "Enhanced Least Significant Bit (ELSB)" has been proposed for color images [4]. As the bits of the secret information are embedded only in the BLUE channel of the RGB cover image, ELSB method has less distortion than that in simple LSB method. However, the main weakness of this technique is that it has less capacity payload and is slow.

*Ankita Gangwar, Vishal Shrivastava, (2013)* in [5], provide an improved RGB-LSB based image steganography. The third party cannot extract the hidden information without knowing the secret key. A secret key is used to hide secret information in the cover image in the LSB of RGB cover image pixels. The bits of secret information and secret key are XORed to determine which color channel need to be used for LSB replacement. This adds double security to the secret information, one due to secret key and another due to LSB steganography.

*Moustafa M. Kurdi, Akram M. Zeki, Imad A. Elzein, (2016)* in [6], used Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in digital watermarking. The random right circular shifts are used to change the order of bit sequences for improving the security. This ensures that hidden watermark text is not predicted by the unauthorized user. The advantage of this technique is its high-capacity payload.

*ii). Pixel-value differencing (PVD):* The pixel-value differencing (PVD) scheme provides high imperceptibility to the stego object by the human eyes as compared to the cover object. *Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang 2008* in [7], proposed a PVD scheme in which, two consecutive pixels are selected and a quantization range table is designed. This range table determines the payload by the difference value between the consecutive pixels. The consecutive pixel values having relatively more difference has larger payload than that of the pixels having less difference. This means that in smoother areas, less information can be embedded than at the edges. This is how the imperceptibility of the stego image is high.

*Gandharba Swain, 2017* in [8], developed a steganographic method combining LSB substitution and PVD in non-overlapping image blocks of size 2×2 by scanning the image in a raster scan order. For every image block, the upper-left pixel is embedded with k-bits of data using LSB substitution. Then the new value of this pixel is used to calculate three pixel value differences with the upper-right, bottom-left, and bottom-right pixels of the block. This paper proposes two variants of the method viz., variant-1 and variant-2. A higher PSNR value is obtained using variant-1 whereas the variant-2 provides both higher PSNR and higher capacity payload.

*Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun* (2010) in [9], also combine LSB and PVD approaches not only to enhance the capacity payload and imperceptibility, but also to reduce the risk of the RS-steganalysis detection.

*iii). Edge based embedding (EBE):* In Edge based embedding method, all the edge pixels in the cover image are used for embedding the bits of the secret data. The edge pixels are used because such pixels are more capable of hiding the secret data with the minimal perceptibility in the stego image. *BrahmaTeja, K.N., Madhumati, D.G. and Rao, K.R.K*. 2012 in [10], proposed a method in which first the masked image is formed by masking some LSB of the cover image. Thereafter, edge pixels are detected from the masked cover image using Canny edge detector or Sobel edge detector. After obtaining the edge pixels, the data is hidden in the LSB bits of the edge pixels only. This algorithm hides data in the edge pixels and thus ensures better security against attackers.

*Junlan Bai, Chin-Chen Chang, Thai-Son Nguyen, Ce Zhu, Yanjun Liu* in [11], a novel steganography approach based on the combination of LSB substitution mechanism and edge detection is proposed. To avoid the excavation of human visual system (HVS) when the payload increases, the cover pixels are classified into edge areas and non-edge areas. Then, pixels that belong to the edge areas are used to carry more bits of secret information than that of non-edge areas to increase the capacity payload. The principle based on the fact that edge areas can tolerate more number of embedding bits than smooth areas is used. The proposed scheme achieves a much higher payload and a better visual quality than those of state of the art schemes.

*iv). Random pixel embedding (RPE):* Random pixels are used for embedding bits of secret information in the cover data. *Laskar, S.A. and Hemachandran, K.* (2013) in [12], proposed a method in which the secret bits are placed in the randomly selected pixels on the basis of the random sequence generated by the pseudorandom number generator (PRNG). So, the secret bits are embedded randomly which makes it difficult for the intruder to recover the secret bits.

*Rupali Bhardwaj, Vaishali Sharma (2016)* in [13], present a technique for providing three levels of security. First level of security is provided by complementing the bits of the secret message, second level by hiding the complemented bits of the secret image in the cover image pixels that are selected randomly and third by using inverted bit LSB method. This increases the security of the secret message manifold.

*v). Pixel mapping method (PMM):* In this method, cover image pixels are selected for embedding by using some mathematical functions which are dependent on its pixel intensities [14]. The bits of the secret data are embedded in the selected pixels and the number of bits embedded in each pixel depends on its intensity as well as intensity of its neighboring 8 pixels.

*Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin* (2001) in [15], hide the secret image by using optimal LSB substitution and genetic algorithm. This method embeds secret data by replacing rightmost k -LSBs of a pixel value with secret bits directly. Genetic algorithm in which chromosomes are created by three kinds: crossover, mutation, and reproduction, is used to find the optimal result for hiding important information. This results in high-quality embedding of the secret image in the cover image. However, major disadvantage of this work is that "approximately" optimal solutions are obtained instead of optimal solutions.

*Chang, C.C., Hsiao, J.Y. and Chan, C.S* (2003) in [16], find the optimal solution of LSB substitution which is computationally faster than [16]. Optimal solutions are obtained by redefining the matrix using dynamic programming which is the square of the difference between the redefined matrix and the substitution matrix.

*Chin-Chen Changa, Ju-Yuan Hsiaob, Huan Xu, Jianjun Wang, Hyoung Joong Kim* (2010) in [17], proposed a novel strategy to find a near-optimal solution for the pair-wise least-significant-bit (LSB) matching scheme. It involves the change of two cover pixels and two bits of secret data at the same time and also changes the matching order between the secret bits and cover pixels to decrease the distortion of the cover image. The proposed three-tier score system reduces the distortion of the stego image, decreases the probability of detection, and at the same time improves the visual quality.

## 5. Comparative analysis

The comparative analysis of various spatial domain techniques are shown in Table 1 "see Appendix 1 for table of results".

## 6. Applications of Steganography

Steganographic methods could be used by any two parties that might wish to protect the secrecy of their communication. Also, there are numerous reasons why people or agents want their communication to be secret. For example, they could be forbidden political organizations that want to communicate among themselves, or even criminals who want to organize a crime or a terrorist operation. There are other specific uses of steganography methods like controlling copyright protection, improving the robustness of image search engines, and smart identity cards. Moreover, steganography methods could be used for embedding checksums and error correction codes. Another application of steganography methods is to maintain the link between image data and the patients' information, whereby the separation is considered necessary for confidentiality purposes, by embedding patients' information into the image. Some other methods of steganography have been discussed in relation to patient records and data concealment in digital images. Secret communication may be used in the business sector as well, and in the modern economic climate the security of corporations is no less important than the security of countries, all large organizations must protect their online information using steganography and other security methods.

## 7. Summary

This paper gave an overview of different steganographic techniques, its major types and classification of steganography which have been proposed in the literature during past few years. As this field of research is a sound topic and gaining importance rapidly, this detail and comprehensive review will be a best tool for quick understanding of the recent projected techniques and will help to present the new and better methodology. These techniques are reliable in one or the other way which is determined on the parameters according to the requirement. Future contribution will focus on the experimental review of steganographic schemes.

## References

[1] Pfitzmann, B., 1996, May. Information hiding terminology-results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding* (pp. 347-350). Springer-Verlag.

[2] Dr. Rajkumar L Biradar, Ambika Umashetty, A Survey Paper on Steganography Techniques. *International Journal of Innovative Research in Computer and Communication Engineering*, January 2016.

[3] Swain, G. and Lenka, S.K., 2014. Classification of image steganography techniques in spatial domain: a study. *Int. J. Comput. Sci. Eng. Tech (IJCSET)*, *5*(3), pp.219-232.

[4] Gupta, S., Gujral, G. and Aggarwal, N., 2012. Enhanced least significant bit algorithm for image steganography. *IJCEM International Journal of Computational Engineering & Management*, *15*(4), pp.40-42.

[5]Gangwar, A., 2013. Improved RGB-LSB steganography using secret key. *International Journal of Computer Trends & Technology*, *1*(4), pp.85-89.

[6] Kurdi, M.M., Elzein, I.A. and Zeki, A.M., 2016, December. Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in digital watermarking. In *Computer Engineering Conference (ICENCO), 2016 12th International* (pp. 111-116). IEEE.

[7] Wang, C.M., Wu, N.I., Tsai, C.S. and Hwang, M.S., 2008. A high quality steganographic method with pixel-value differencing and modulus function. *Journal of Systems and Software*, *81*(1), pp.150-158.

[8] Swain, G., 2016. A Steganographic Method Combining LSB Substitution and PVD in a Block. *Procedia Computer Science*, *85*, pp.39-44.

[9] Yang, C.H., Weng, C.Y., Wang, S.J. and Sun, H.M., 2010. Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. *Journal of Systems and Software*, *83*(10), pp.1635-1643

[10] BrahmaTeja, K.N., Madhumati, D.G. and Rao, K.R.K., 2012. Data hiding using EDGE based steganography. *International journal of Emerging Technology and advanced Engineering*, *2*(11), pp.285-290.

[11] Bai, J., Chang, C.C., Nguyen, T.S., Zhu, C. and Liu, Y., 2017. A high payload steganographic algorithm based on edge detection. *Displays*, *46*, pp.42-51.

[12] Laskar, S.A. and Hemachandran, K., 2013. Steganography based on random pixel selection for efficient data hiding. *International Journal of Computer Engineering and Technology*, *4*(2), pp.31-44.

[13] Bhardwaj, R. and Sharma, V., 2016. Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution. *Procedia Computer Science*, *93*, pp.832-838.

[14] Bhattacharyya, S., Khan, A., Nandi, A., Dasmalakar, A., Roy, S. and Sanyal, G., 2011, December. Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography. In *Information and Communication Technologies (WICT), 2011 World Congress on* (pp. 36-41). IEEE.

[15] Wang, R.Z., Lin, C.F. and Lin, J.C., 2001. Image hiding by optimal LSB substitution and genetic algorithm. *Pattern recognition*, *34*(3), pp.671-683.

[16] Chang, C.C., Hsiao, J.Y. and Chan, C.S., 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, *36*(7), pp.1583-1595.

[17] Xu, H., Wang, J. and Kim, H.J., 2010. Near-optimal solution to pair-wise LSB matching via an immune programming strategy. *Information Sciences*, *180*(8), pp.1201-1217.

**Appendix 1**

**Table 1.** Comparison of Various Spatial Domain Techniques

| S.No. | Authors | Year | Technique used | Target Parameters | | Remarks |
|---|---|---|---|---|---|---|
| | | | | Imperceptibility | Capacity Payload | |
| 1. | Shilpa Gupta, Geeta Gujral and Neha Aggarwal | 2012 | LSB | Yes | No | Less distortion |
| 2. | Ankita Gangwar, Vishal Shrivastava | 2013 | LSB with secret key | Yes | No | Secure and complex |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3. | Moustafa M. Kurdi, Akram M. Zeki, Imad A. Elzein | 2016 | LSB and RRCF | Yes | Yes | Secure, less complex |
| 4. | Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang | 2007 | PVD | No | Yes | High hidden capacity |
| 5. | Gandharba Swain | 2017 | LSB and PVD | No | Yes | High hidden capacity and high PSNR |
| 6. | Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun | 2010 | LSB and PVD | Yes | Yes | Robustness |
| 7. | Saiful Islam, Mangat R Modi and Phalguni Gupta | 2014 | EBD | Yes | Yes | Increased Security and less distortion |
| 8. | Junlan Bai, Chin-Chen Chang, Thai-Son Nguyen, Ce Zhu, Yanjun Liu | 2017 | EBD | Yes | Yes | Less Distortions |
| 9. | Laskar, S.A. and Hemachandran, K. | 2013 | RPE | Yes | No | Security |
| 10. | Rupali Bhardwaj, Vaishali Sharma | 2016 | RPE | Yes | No | Higher Security |
| 11. | Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin | 2001 | PMM | Yes | Yes | Not an optimal mapping |
| 12. | Chi-Shiang Chan | 2003 | PMM | Yes | No | Optimal mapping and fast |
| 13. | Chin-Chen Changa, Ju-Yuan Hsiaob, Huan Xu, Jianjun Wang, Hyoung Joong Kim | 2010 | PMM | Yes | No | Data cannot be easily extracted |