American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402
© Global Society of Scientific Research and Researchers
http://asrjetsjournal.org/

A Review on Steganography Techniques

Wafaa Mustafa Abduallah[a*], Abdul Monem S. Rahma[b]

[a]*Department of Computer Science, Nawroz University, Duhok, Iraq*
[b]*Department of Computer Science, University of Technology, Baghdad, Iraq*
[a]*Email: wafaa.mustafa@nawroz.edu.krd*
[b]*Email: monem.rahm@yahoo.com*

Abstract

Steganography is the science of hiding a secret message in cover media, without any perceptual distortion of the cover media. Using steganography, information can be hidden in the carrier items such as images, videos, sounds files, text files, while performing data transmission. In image steganography field, it is a major concern of the researchers how to improve the capacity of hidden data into host image without causing any statistically significant modification. Therefore, this paper presents most of the recent works that have been conducted on image steganography field and analyzes them to clarify the strength and weakness points in each work separately in order to be taken in consideration for future works in such field.

Keywords: steganography; DCT; DWT; SVD.

1. Introduction

Internet has become significantly important in today's life. It is generally used for data transfer though currently what concerns its users the most is the security of the data transferred via the Internet. In fact, for many government organizations, business industries, and individuals, it has become increasingly important to secure the information exchanged in bulk while making use of cyber space [1]. The reason why questions of cybersecurity or those of online privacy have brought the issue of secret writing into limelight is the fact that the social, economic and professional lives of the masses today are heavily dependent on emailing, net posting, electronic banking, e-commerce, etc. [2]. Steganography does the wonder of hiding the presence of the secret information. This is unlike cryptography, where alterations are made to the message, thus rendering it unreadable to an adversary or a third party [1].

---

* Corresponding author.

Hence, it can be said that "Steganography and cryptography are cousins in the spy craft family". A message is scrambled by cryptography which makes it unintelligible. Steganography, on the other hand, makes a message invisible (i.e., that is the objective) by hiding it. The encrypted text may cause doubt in the mind of the recipient but the invisibility of text created by steganography never creates any doubt [3].

In steganography, the secret message is concealed using a cover medium (i.e., carrier) before it is transmitted on a public communication channel. It therefore, impedes the unauthorized access to the message and protects its confidentiality. Before the application of steganography for increasing the security level and reduction in the amount of data to be embedded, the secret message can be encrypted or compressed. As a result, this may minimize the perceived artifacts in the carrier image (note: the carrier object can be text, video, or audio too) [1].

This paper presents numerous steganographic techniques that have been recently proposed for hiding the secret data within the cover-images efficiently. Generally, image steganography techniques can be categorized into two main groups (depending on the domain that is used for embedding), which are: steganography methods based on spatial domain and steganography methods based on transform domain as will be explained in the following sections.

2. Spatial Domain Techniques

The concept of hiding information in spatial domain is simple and the complexity of computations is low. The secret information can be embedded simply through changing the unused Least Significant Bits (LSBs) of the cover-image. For this, numerous kinds of methods have been presented.

2.1 The Least Significant Bit

The schemes based on Least Significant Bit (LSB) can be basically classified into two main types; LSB Replacement and LSB Matching. In the first type, the secret bits are simply replaced by the LSBs of the pixels of the image. On the other hand, the second one is more complicated and difficult to detect than the first type because of its reliance upon the matching between the LSBs of the cover-image and the secret bits of the message. If there is no matching, the pixel value of the cover-image is either added or subtracted by one. Consequently, it is also called ±1embedding. In order to be able to reverse this operation, the resulted pixel value should fall within acceptable range [4].

2.1.1 The Least Significant Bit Replacement

For the LSB replacement scheme, the LSB of the image pixel is required to be changed if it differs from the value of the secret message bit therefore; the Expected Number of Modifications Per Pixel (ENMPP) is around 0.5. Hence, a modern method is proposed by [5] to reduce the ENMPP through making use of the optimization notion for the pixel selection to hide the secret bits as shown in Figure 1. The imperceptibility and the embedding efficiency have been improved noticeably but on the account of increasing time complexity and lowering embedding capacity.

A different data hiding scheme called LSB+ algorithm is developed by [6]. This algorithm is implemented for preserving some of the important image statistics besides the image histogram to avoid the detection by steganalysis technique via taking advantage of the similarity between the neighboring pixel values in all directions (up, down, left, and right). The authors proved through the experiments the ability of their method to minimize the distortion caused to the image after embedding. On the other hand, the embedding rate is decreased significantly because of the limited number of pixels that are acceptable to be used for embedding since this method only uses the pixels with same neighbor values.

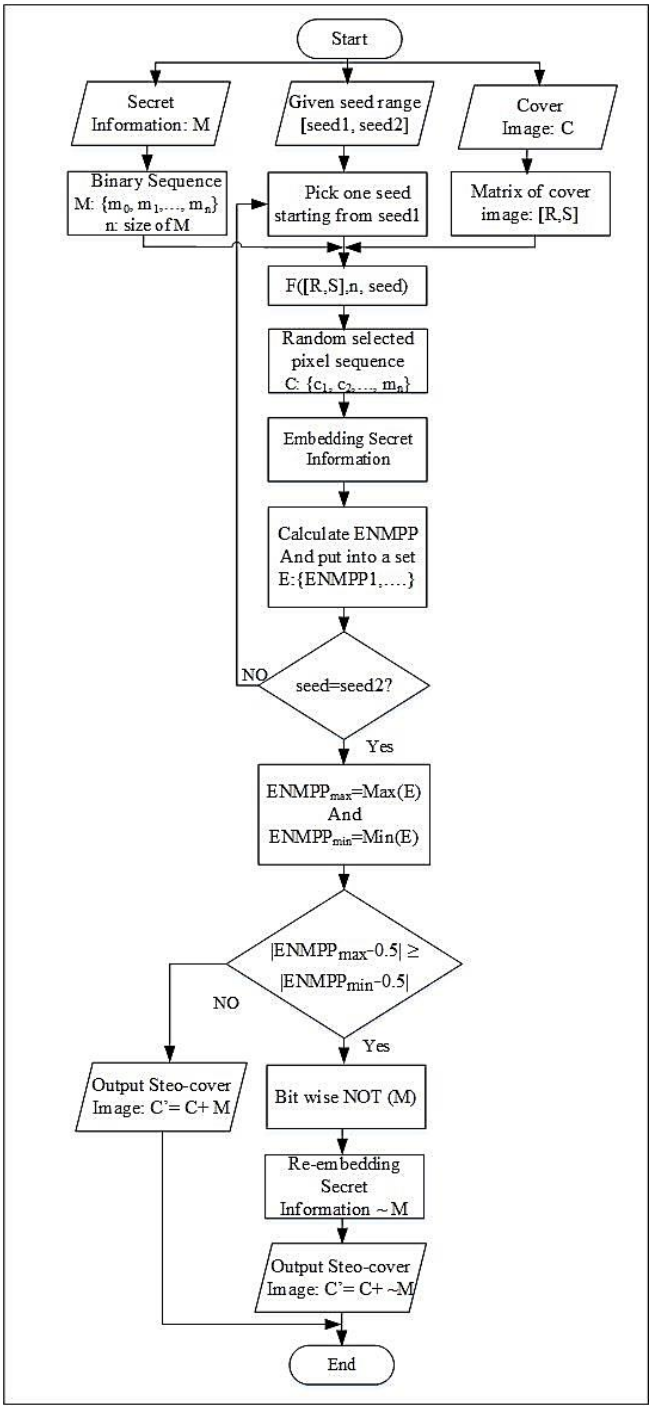

Figure 1: The flowchart of the proposed information embedding [5].

2.1.2 The Least Significant Bit Matching

Sharp [7] introduced the method of LSB matching for the first time but, this method has a weakness as it performs the increment or decrement to the pixel value of the cover-image in random manner. Hence, an improvement to LSB matching is presented in [4] by making use of a binary function with two pixels to be set to the desired value depending on a certain choice. A pair of two pixels has to be used for performing the embedding process, where the LSB of the first pixel holds one bit of the secret message while the second bit of the secret message has to be assigned to the binary function of two pixel values. As a consequence, this method overtook the traditional LSB matching in terms of distortion due to the significant decreasing for the number of modifications per pixel from 0.5 to 0.375 utilizing similar embedding rate that has been used with the traditional LSB matching. In addition, the experimental results demonstrated the resistance of this method against steganalysis attacks.

An adaptive technique known as Complexity Based LSB-M (CBL) is presented by [8]. A complexity measure is used to analyze the local neighborhood for finding secure locations in the cover-image that can be utilized for embedding. The embedding process involves dividing the cover-image into 3×3 overlapped blocks, and then computing the complexity of each pixel in the cover-image through checking the 8 neighboring pixels in order to determine the most suitable locations for embedding within the cover-image.

The LSB matching technique is approximately near optimal, especially when employing information from single pixel. It has the assumed shortcoming that image noise does not depend on the pixel and it may vary from pixel to pixel. Nevertheless, these assumptions have been proven wrong through some of LSB matching detectors [9,10] using natural images.

2.2 Optimal Pixel Adjustment

The basic notion behind Optimal Pixel Adjustment (OPA) is simply embedding the secret bit within the cover-image utilizing LSB substitution to generate the stego-image. Then, refining the new pixel values of the stego-image after performing the optimal LSB technique that can be done via applying addition or subtraction operation for the factor (2^z) from the embedded pixel (where, z indicates the number of hidden bits). It is noteworthy that the least z bits for the pixel values of the stego-image would not be affected by the adjustment processes [11]. Therefore, the concept of optimal pixel adjustment is adopted by the authors [11] for enhancing the quality of the stego-image under various payload capacities and numerous authentication bits conditions. Even though, this technique accomplished good results with regards to the imperceptibility and the embedding capacity but, the resistance of the system against steganalysis attacks has not been addressed.

The technique of optimum pixel embedding is typically used when the high embedding capacities are required whereas; matrix embedding (MM) technique is desirable when minimum distortion to the cover-image is essential. Therefore, a new model for data hiding is implemented by [12] based on combining both techniques to make use of their properties. Moreover, to increase the embedding capacity, the authors used Huffman coding technique for compressing the payload data before embedding as further demonstrated in Figure 2. The

experimental results proved the acceptable level of imperceptibility reached by this method though the security of the system against stegnalysis techniques was not investigated.

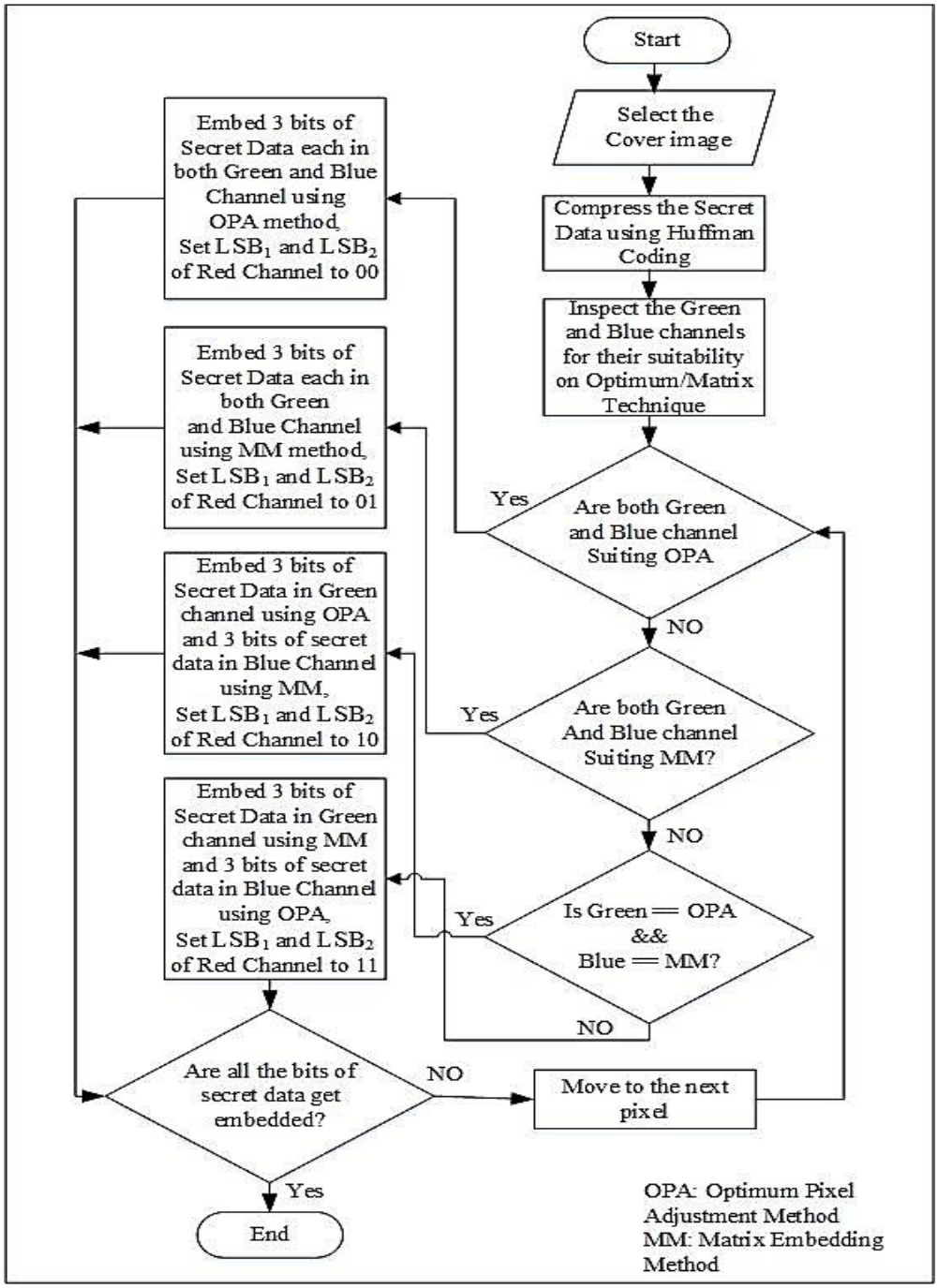

Figure 2: The process of data embedding [12].

2.3 Pixel Value Differencing

Pixel Value Differencing (PVD) [13, 14, 15] can be considered as one of the most well-known data hiding techniques in spatial domain. This technique is used to increase the embedding capacity for the system. However, it may produce distortion to the cover-image even when using low embedding payload. Figure 3

illustrates the concept of PVD which relies on the basis of computing the difference between two successive pixels and checking the resulted value if it is large or small. Since the large value indicates that the two successive pixels belong to the edge area, consequently it also means that large amount of data can be hidden in this area. The small value refers to locating the two successive pixels in a smooth area and subsequently, less amount of data can be used for hiding in such area. This concept has been introduced by [13] which obtained good image quality with less amount of distortion as compared with those produced by LSB schemes. Nevertheless, this method has a limitation represented in the obtained original difference when it is not equal to the secret data. Then, the two successive pixels have to be adjusted and that may produce a substantial distortion to the stego-image. This limitation has been addressed and considered by [14] to present another technique that increases the quality of the stego-image via making use of modulus function for adjusting the remainder of the difference between the two successive pixels instead of changing the difference value. Furthermore, using PVD mechanism alone may arouse a problem of falling-off especially when the values of two successive pixels belong to smooth area or an extreme edge. So, the presented technique by [14] overcame this problem through revising the remainder of the difference between two successive pixels. The results obtained by [14] were much better than the results of [13] in terms of the quality of the stego-image.

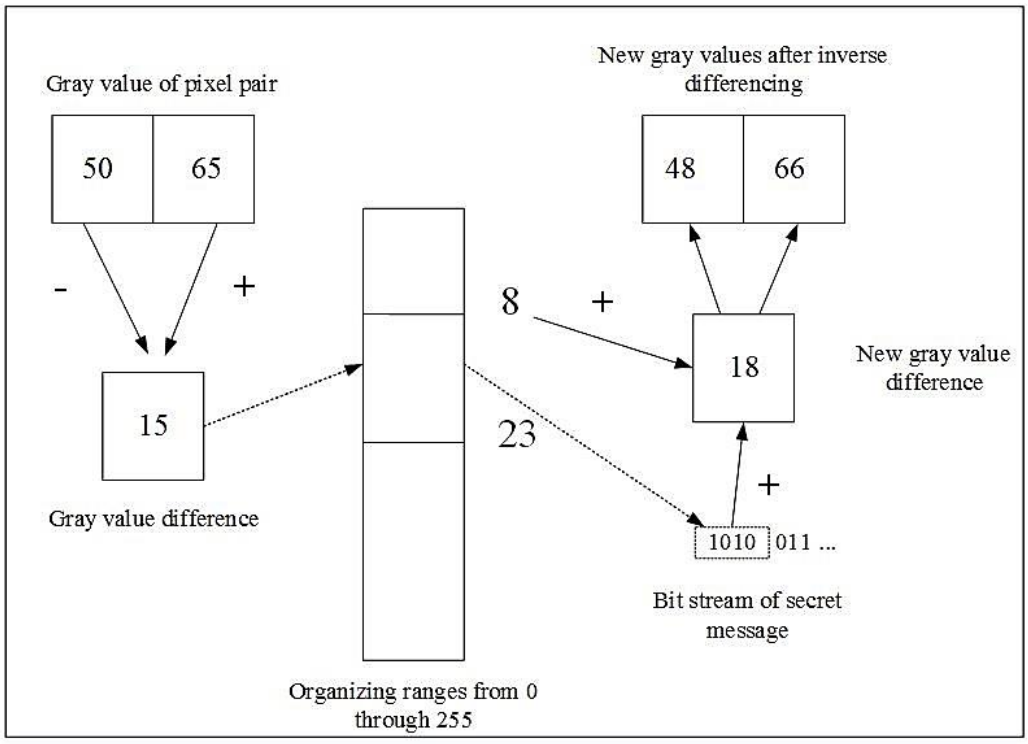

Figure 3: A clarification of the data hiding process introduced by [13].

2.4 Other Schemes Based On Spatial Domain

Achieving high embedding capacity with conserving good level of image quality is challenging in steganography field. Hence, the authors in [16] proposed a scheme for hiding color secret image within a true color image alongside preserving good image quality for both images; the stego and the extracted image, by applying color quantization technique along with their proposed method as illustrated in Figure 4. In addition,

their method provided the secret image with primitive protection via encrypting it using Data Encryption Standard (DES) cryptographic algorithm. Nevertheless, the security of the system has not been tested against staganalysis attacks.

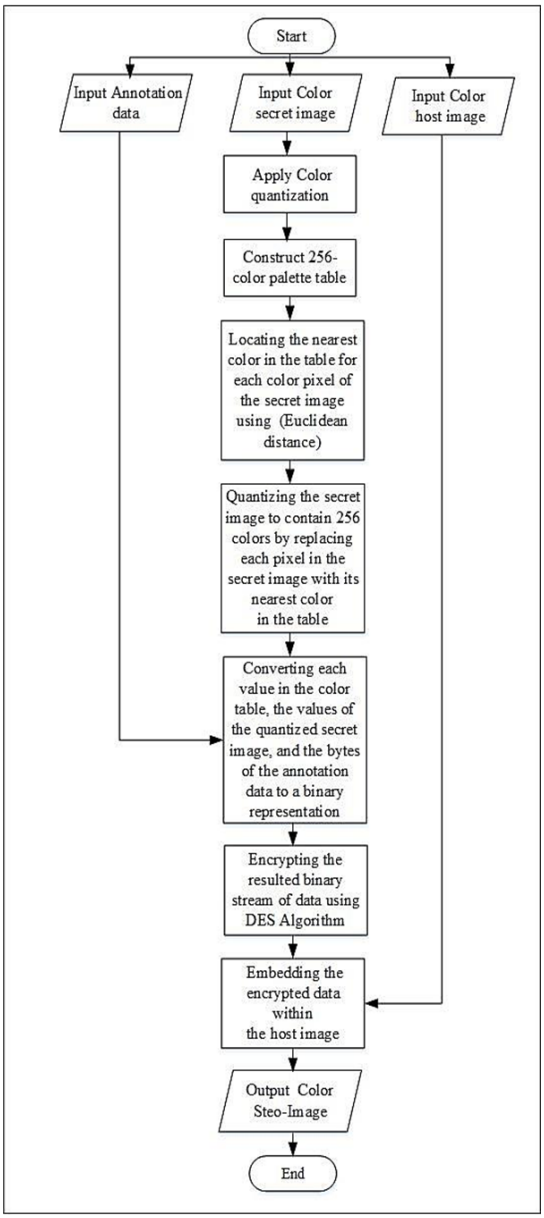

Figure 4: The steps of embedding procedure [16].

Based on the models of high dimensional image, the authors in [17] designed a steganography algorithm called High Undetectable steGO (HUGO). During the implementation of the proposed algorithm, Subtractive Pixel Adjacency Matrix (SPAM) features have been considered (which was proposed by [10]). The authors also proved its effectiveness in LSB ± embedding. These features succeeded in detecting many steganography techniques that make them suitable to be used for steganalysis besides steganography techniques. The idea of SPAM features is based on calculating the probabilities of Markov transitions over various images using 8 directions of adjoining pixels. The main concept of HUGO approach can be summarized in few steps starting

from embedding set of images with a maximum payload using LSB ± embedding process through randomly increasing or decreasing the value of pixel by one. Next, using the SPAM features for originating the image model which is anticipated to be more secure since HUGO method utilizes the hardly detected parts of images for embedding. Then, optimized criteria presented in FLD are used for evaluating the weights (i.e., parts of the model) that are in charge of detecting the LSB matching. Consequently, analysis of the values of FLD criteria is used for identifying the parts of the model that are suitable for embedding. Despite this, HUGO scheme might be exposed to steganalysis attacks which are based on other models than SPAM features.

3. Transform Domain Techniques

Transform domain based steganography schemes are another choice for hiding secret data within the cover-image without being detected by humans. So, the cover-image has to be transformed using one of the transform oriented methods such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), etc. Then, secret message should be embedded by changing the coefficients. More details about these methods are given in the following sub-sections.

3.1 Discrete Cosine Transform:

Many previous works have been proposed in DCT such as [18, 19, 20, 21, 22]. The authors in [18] have presented robust steganographic scheme based on DCT that can resist JPEG image compression by utilizing only low and middle frequency coefficients for embedding the secret message. To increase the security, some of the coefficients have been used for embedding according to a secret key. In addition, to perform the embedding process; an average of surrounding coefficients to the selected coefficient would be computed, then accordingly the secret bit could be hidden. Even though, the proposed technique showed acceptable level of imperceptibility with a good level of robustness, the capacity issue was not considered.

Statistically Invisible Steganography (SIS) is another steganographic scheme that was carried out in DCT by [19] which showed robustness against steganalysis methods. The proposed technique exploits the blocks with high complexity for hiding and precludes the one with the low complexity to reduce the statistical modifications thus, provides high security. Hence, the primary focus for this work was only on security while the capacity was not considered.

To upgrade the embedding efficiency, a distinct data hiding technique called Matrix Encoding (ME) has been implemented in [23]. The concept of the matrix encoding scheme is built on the basis of Hamming code. The authors implemented an algorithm known as ‘F5’ that embeds more than one bit via modifying one coefficient. So, the image distortion has been reduced as well as the security against steganalysis attacks has been increased. Later, an improved matrix coding was introduced by [20] to ameliorate the embedding rate by using the DCT coefficients of two overlapped ME blocks as an integrated block.

The hiding process is based on the inserting or removing coefficients 1 or -1. Therefore, any insertion or removal operation will produce various results for the improved matrix encoding. The proposed algorithm selects the best option with the least distortion among all potential results. The authors could prove the

efficiency of the proposed algorithm in terms of less detectability by steganalysis attacks but the capacity of payload for both methods, [23, 20] does not exceed 0.25 bpp, which is very low.

Two reversible steganographic techniques were presented by [22, 21] to increase the capacity of embedding in transform domain using DCT.

The core idea of [22] was based on the changing of the quantization table and the quantized coefficients of DCT. In this scheme, to provide a space for hiding the secret data, the entries of quantization table would be lowered by dividing some components of the quantization table by an integer number and at the same time, multiplying the quantized coefficients of DCT by the same number, then adding an adjustment value as shown in Figure 5.

On the other hand, the steganographic scheme that was presented by [21] made use of integer mapping for implementing the two dimensional DCT which decomposes the cover-image into various frequencies where only the high frequency components are used for embedding the secret message. Due to the similarity between the distribution of the coefficients for the two dimensional DCT and the Gaussian distribution, this makes the former suitable for hiding the secret message via utilizing histogram shifting technique. Therefore, to make a space for hiding the secret message, the positive coefficients are shifted to the right while the negative coefficients are shifted to the left. Both [22, 21] have reached approximately the same level of embedding capacity but, on the account of image quality, which has been significantly decreased. The drawback is that none of these schemes addressed the issue of security properly.

3.2 Fourier Transform:

Another frequency domain that has been adopted in steganography field is the Fourier Transform which makes use of spectral characteristics of the natural images such as Fourier magnitude and phase to be used for embedding secret data. Some of the previous works exploited the phase for hiding such as [24, 25], while others like [26,27] utilized the magnitude for embedding. On the other hand, other researchers like in [28] used the property of zero padding for image steganography based on Fourier transform domain. More specifically, the proposed algorithm used Nyquist rate for padding the cover-image with zeros, then applied Discrete Fourier Transform (DFT) on each plane separately. The DFT produces up to 75% zeros as mathematically proved by the author. These zeros can be slightly modified to embed the secret data without making any noticeable effect on the image. However, the capacity of embedding is limited to using only these coefficients with zero values.

Two works [24,25] proposed color image steganography frameworks that use DFT based on adaptive phase modulation (APM) to preserve image quality after embedding. Both works utilized the Lempel–Ziv–Welch (LZW) method for compressing the secret image to get low bit rate. In addition, both works adopted DES cryptographic algorithm for enhancing the security of the system. However, there is a slight difference between the two works in the steps of applying embedding process. Moreover, the work presented by [25] used hardware element of Linear Feedback Shift Register (LFSR) to overcome the shortage of high complexity that is involved in the work of [24] as shown in Figure 6.

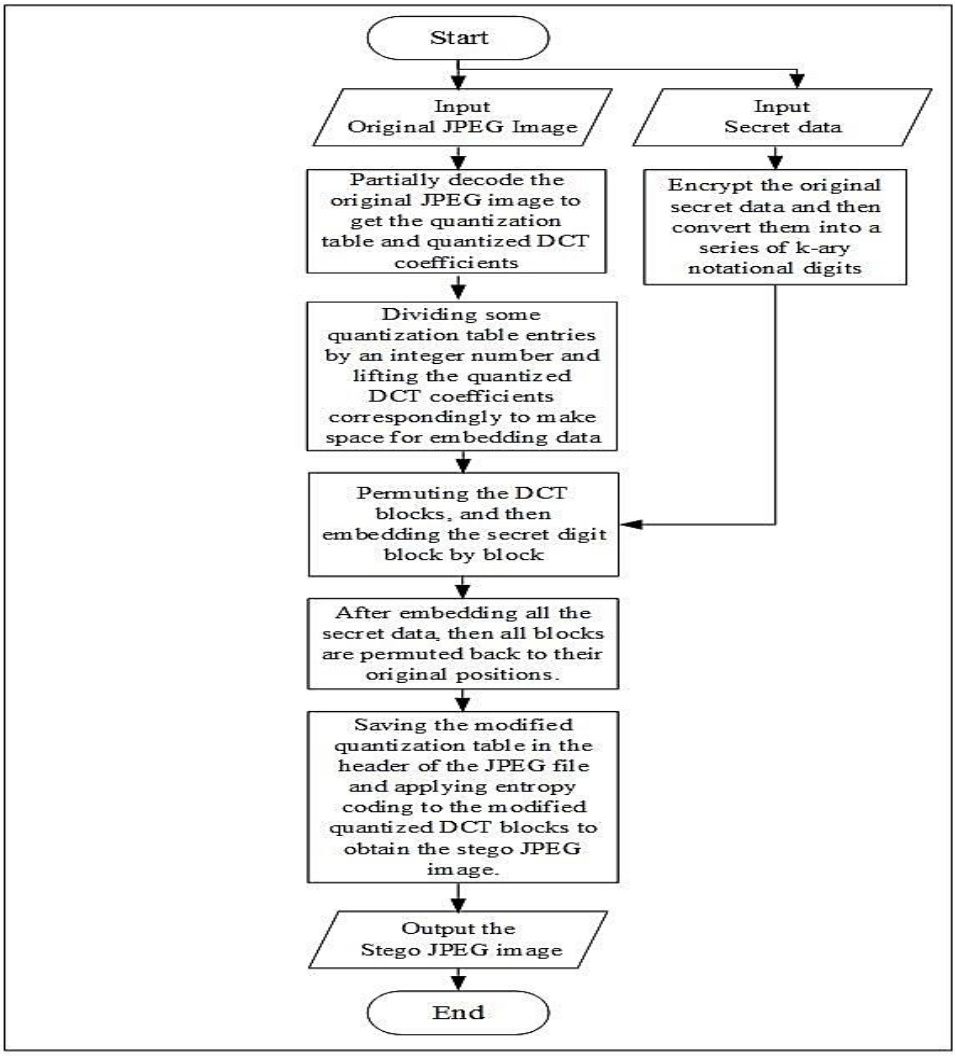

Figure 5: The proposed data embedding phase [22].

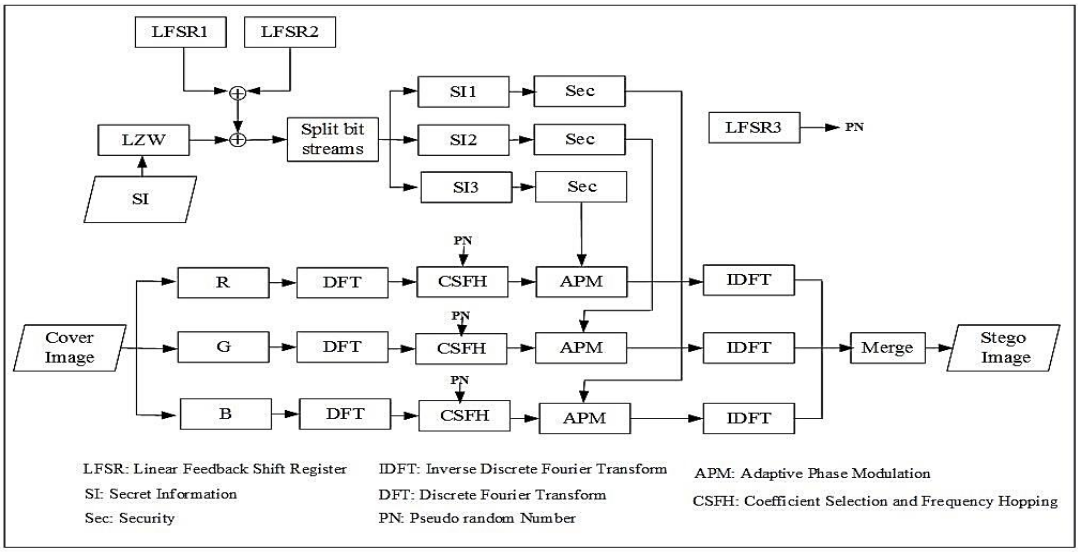

Figure 6: The conceptual model of the optimized algorithm [25].

The classical Fourier Transform has been generalized to another form called Fractional Fourier Transform (FRFT) that has an advantage over DFT in terms of combining both spatial and frequency domains. This transform is able to indicate the spectral components of the image or the signal besides the time location of these spectral contents. This feature has been espoused for image steganography, by two works [29, 30]. More precisely, the authors in [30] illustrated an advanced image steganography technique using Weighted Fractional Fourier Transform (WFRFT) that provides an intermediate domain amidst spatial and frequency domain for hiding the secret data. So, firstly the cover-image is divided into blocks of size 2*2, and then WFRFT is applied to each block. The secret bits are embedded within the LSB of the real components of the transformed cover-image. The experimental results showed an obvious similarity between the histogram of the original and stego-images. Albeit with this, the proposed mechanism is limited in the capacity of embedding since it can only hide the secret image with size up to the half of the cover-image size.

3.3 Wavelet Transform

Another type of transform domain that can be adopted for steganography is, DWT. Unlike DCT that can be applied to blocks of the image which affects the continuity between blocks, DWT is applied to the entire image and it produces better energy than that of DCT [31]. But, in general, wavelet filters output coefficients with floating point; thus, in the case of using an image that consists of integer data, the resultant filtered data produce floating point, subsequently, the original image is difficult to be reconstructed perfectly. Nevertheless, wavelet transforms based on lifting scheme that maps integer to integer can deal with integer data and is able to reconstruct the original data completely without any loss [32]. In spite of this, some steganographic frameworks are implemented using DWT such as [31, 33, 34]. Many other researchers used Integer Wavelet Transform (IWT) like [35, 36, 37, 32] to avert the troubles of floating point with wavelet filter.

A different data hiding method is provided by [34] to embed two secret grayscale images within a color image using DWT. To perform the hiding procedure, DWT is applied on the secret images as well as the cover-image after converting the last one to YCbCr color space (where, Y is the Luminance, Cb is the Chroma Blue and Cr is Chroma Red). The proposed algorithm utilized the low frequency sub bands for Cb to hide one of the secret images and for Cr to hide the other secret image according to a secret key. Finally, the secret key has to be embedded also within the cover-image using LSB to get the resultant stego-image. The proposed scheme did not produce any distortion within the stego-image. Besides that, the secret images can be extracted successfully. However, the resistance against steganalysis attacks has not been reflected by methods [33] and [34].

Another study for image steganography based on IWT is proposed by [35] where the wavelet transform is applied to both cover and secret image. Then, an embedding operation is performed using an algorithm of assignment called Munkres algorithm that is used to find best embedding locations based on the matching between blocks to be used for embedding. During the experiments, different types of sub bands have been used for embedding such as the horizontal, vertical and diagonal. However, the results showed that the diagonal coefficients offered better results than other sub bands in terms of image quality.

To make a tradeoff between imperceptibility and capacity, a distinct steganographic technique based on Integer

Wavelet Transform is proposed by [36]. The implemented algorithm used color image as a cover that first should be divided into three planes: Red, Green and Blue, and then, IWT should be applied on each plane separately. Finally, the secret data are to be hidden in the wavelet coefficients in random style using graph theory. Furthermore, the proposed work utilized three keys for hiding and extracting the secret message, where the first key was used for selecting sub band for hiding, the second key was used for selecting the coefficients at random, and the third key was used for selecting the number of bits to be hidden within the chosen coefficients. The proposed system achieved reasonable image quality with high capacity as well as robustness against Chi-square steganalysis attack.

3.4 Contourlet Transform

The wavelet transform has been extended to a new recent transform called Contourlet transform which is proposed by [38]. Contourlet transform is similar to wavelet transform in conforming the multi-resolution quality of the human visual system. This new transform offers different representation for the image using multi scale and multi directional filter banks. Hence, it surpasses the wavelet transform in analyzing the image and detecting the smooth contours as well as the directional details [38, 39]. In addition, changing the values of Contourlet transform coefficients produces less amount of distortion to image quality as compared to wavelet domain [40]. Therefore, Contourlet transform has been utilized in the steganography field by some researchers like [41, 40].

Another adaptive steganographic scheme based on Contourlet transform is presented in [42] to hide the secret data within chosen cover-image. The proposed technique decomposes the cover-image into sub bands by applying Contourlet transform. Then, the secret data are embedded by modifying the coefficient values in either increasing or decreasing them where only one coefficient within the block should be used for embedding one bit. On the other hand, many criteria have been used for choosing the suitable cover-image for embedding. The authors proved through the experiments that selecting the appropriate cover-image can help reduce image detectability by steganalysis methods. So, the security is increased; but again, at the expense of capacity, which was up to 0.06 bit per pixel.

Another steganographic technique based on Contourlet transform and cover selection is proposed by [43]. The contrast measurement is utilized as a criterion for selecting a suitable cover for hiding. The most appropriate cover is the one with highest contrast value since such cover affects on the steganalyzer in wrongly classifying the stego-image. The embedding algorithm is achieved by applying one level of Contourlet transform on the selected cover. Then, the sub bands are divided into blocks of 8*8 and the secret data are hidden within the blocks that have an energy value greater than the value of mean energy which represents the mean energy of all blocks. The proposed method obtained efficient results in terms of image quality but the capacity was limited to 24,927 bits only. Furthermore, the security against steganalysis attacks also needs to be investigated to prove the assumption of affecting cover selection mechanism on the security.

3.5 Other Types of Transform Methods

There are other types of Transform techniques that are not famous like the previously mentioned methods, but they also have been used in the field of data hiding such as Discrete Hadamard Transform (DHT) [44, 45], Curvelet Transform [46], and Singular Value Decomposition (SVD) Transform [47, 48, 49]. Another type of transform similar to wavelet transform known as Stantlet transform is utilized for image steganography by [45] for having properties better than conventional DWT and DCT in terms of signal compression and time localization. To obtain good embedding rate and increase the security as well, the secret message is encoded using T-codes before embedding. The resulted secret data are embedded within the coefficients of the high frequency sub bands of the transformed cover-image using LSB scheme. The experimental results of the proposed method showed high undetectability and the results were approximately comparable to results of Haar wavelet Transform scheme. One more transform scheme is known as SVD that is widely utilized in the applications of signal processing. The basic idea behind SVD is to decompose the matrix into three matrices; U and V are two orthogonal matrices and S is a diagonal matrix that is usually exploited for hiding the secret data [47]. Three of the previous works [47, 48, 49] proposed color image steganography based on SVD transform domain. Precisely, the authors in [47] applied SVD transform on the cover-image then, used the nonzero Singular Values (SV) for embedding the secret data since slight modification to SV values may not affect the visual discrimination of the resulted image. The proposed method achieved good embedding rate with acceptable level of imperceptibility whereas the robustness against attacks has not been investigated through the experiments. On the other hand, the work presented by [48] concentrated on the fidelity of the image rather than other requirements of data hiding. So, instead of using singular values of the transformed cover-image, the values of U matrix have been used for embedding the secret data through changing the sign of some entries for the U matrix. Accordingly, the capacity of embedding has been reduced. However, the ratio of recovering the secret message accurately is increased due to enlarging the visual fidelity between the stego-image and cover-image.

3.6 Combination of Transform Methods

Some of the researchers suggested using two or more transform methods, for instance the authors [50, 51, 52, 53] utilized DCT with DWT. While, others like [54, 55, 56] proposed SVD watermarking technique based on Wavelet Transform domain. Another mixture between SVD and DCT is proposed by [57] to build impervious watermarking system against different types of attacks. The authors of [58] (Das & Kundu, 2011) accomplished robust watermarking system via applying successive transforms of Contourlet Transform and DCT. The work presented by [51] described a combination of DCT with DWT to improve the performance of the steganographic method in terms of visual quality for the stego-image and the extracted secret image. The core idea behind the proposed scheme was applying the DCT to the secret image then, extracting the features from both the cover-image as well as the transformed secret image via applying DWT on both separately. The embedding procedure utilized two keys for hiding the features of the secret image within the features of the cover-image. The authors demonstrated the effectiveness of using two transform methods through the experiments which showed good imperceptibility for the stego-image. In addition, the proposed method resists eight types of image processing attacks. Hence, the authors recommended the proposed scheme for the application of copyright protection.

4. Analysis

Table 1: Gaps in the Previous Studies

Researcher Name and Year	**Method Name**	**Method Domain**	**Imperceptibility**	**Capacity**	**Security Against Steganalysis attacks**
1- (Sun et al.,2012), [5]	LSB Replacement	Spatial Domain	Good	Low	Not Approved
2- (Wu et al., 2011), [11]	Optimal Pixel Adjustment (OPA)	Spatial Domain	Good	Good	Not Approved
3-(wang et al., 2008), [14]	Pixel Value Differencing (PVD)	Spatial Domain	Good	High	Secure against Rs- detection attacks
4-(Schnev & Kim, 2012), [20]	Improved Matrix Encoding Scheme based on DCT	Transform Domain	Good	Low	Secure
5-(Keshari & Modani, 2011), [30]	Weighted Fractional Fourier Transform (WFRFT)	Transform Domain	Good	Reasonable (up to the half of cover image size)	Not Approved
6-(Raftari & Moghadam, 2012), [35]	Steganography Based on Integer Wavelet Transform (IWT)	Transform Domain	High	The size of secret image is half the size of cover image	Not Approved
7-(Sajedi & Jamzad, 2010), [42]	adaptive contourlet-based steganography method	Transform Domain	Good	low	Secure

The summary of explanation for the previous methods that have been illustrated in the preceding sections can be shown in Table 1. From the table, it is easy to discover the gaps that have been found in these methods in terms of capacity and security since most of the methods that are implemented in spatial domain provide high capacity of embedding but, on the expense of security. On the contrary, most of the methods that are carried out in transform domain suffered from the low capacity and are provided with good level of security.

5. Conclusions

A general idea about various steganography techniques that have been presented in the literature for the duration of last few years, along with their main types and categorization of steganography technique is presented in this paper. As well as, a significant analysis for the most important aspects of steganographic systems which are the embedding capacity, the imperceptibility (i.e. stego-image quality) and security have been illustrated for each method. Hence, there occurs a tradeoff between the embedding capacity and imperceptibility. Where, increasing embedding capacity without affecting the security and quality of the stago-image can be considered as a challenging mission. Furthermore, this study presented some problems related to the previous methods; First, Spatial domain techniques have low level of security. Second, transform domain schemes restricted with low embedding capacity. Third. the quality of the stego-image is an essential aspect which is constrained with the embedding capacity. So, there is a need for new methods that can take the benefits of two domains to overcome these gaps and make a balance among the three requirements of steganographic system which are capacity, imperceptibility and security.

References

[1] E.-S. M. El-Alfy and A. A. Al-Sadi. “High-capacity image steganography based on overlapped pixel differences and modulus function”. in Proc. of International Conference on Networked Digital Technologies, Springer Berlin Heidelberg, vol. 294, 2012, pp. 243-252.

[2] M. Conway. “Code wars: steganography, signals intelligence, and terrorism”, Technology & Policy, Springer Netherlands, vol. 16 (2), pp. 45-62, 2003.

[3] N. F. Johnson and S. Jajodia. “Exploring steganography: Seeing the unseen”. Computer, IEEE, vol. 31(2), pp. 26-34, 1998.

[4] J. Mielikainen. “LSB matching revisited”. IEEE signal processing letters, vol. 31(5), pp. 285-287, 2006.

[5] J. Sun, Y. Li, X. Zhong, and J. Li. “A Scheme of LSB Steganography Based on Concept of Finding Optimization Pixels Selection”. In Software Engineering and Knowledge Engineering: Theory and Practice, 1st ed., vol. 115, Y. Wu, Springer Berlin Heidelberg, 2012, pp. 155-160.

[6] H. T. Wu, J. L. Dugelay, Y. M. Cheung. “A data mapping method for steganography and its application to images”. In Information Hiding, 1st ed., K. Solanki, K. Sullivan and U. Madhow, Springer Berlin Heidelberg, 2008, pp. 236-250.

[7] T. Sharp "An implementation of key-based digital signal steganography", in Information Hiding Workshop, vol. 2137, 2001, pp. 13-26.

[8] V. Sabeti, S. Samavi, and S. Shirani. "An adaptive LSB matching steganography based on octonary complexity measure". Multimedia tools and applications, Springer, vol. 64(3), pp. 777-793, 2013.

[9] M. Goljan, J. Fridrich, and T. Holotyak ." New blind steganalysis and its implications". In proc. Security, Steganography, and Watermarking of Multimedia Contents VIII, vol. 6072, 2006, pp. 607201-607201.

[10] T. Pevny, P. Bas, and J. Fridrich. "Steganalysis by subtractive pixel adjacency matrix". Information Forensics and Security, IEEE Transactions, vol.5(2), pp. 215-224, 2010.

[11] C.-C. Wu, S.-J. Kao, and M.-S. Hwang. "A high quality image sharing with steganography and adaptive authentication scheme". Journal of Systems and Software, vol. 84(12), pp. 2196-2207, 2011.

[12] N. Pandian, and R. Thangavel."A hybrid embedded steganography technique: optimum pixel method and matrix embedding", in proc. of the International Conference on Advances in Computing, Communications and Informatics, ACM., 2012, pp. 1123-1130.

[13] D.-C. Wu, and W.-H. Tsai. "A steganographic method for images by pixel-value differencing". Pattern Recognition Letters, vol. 24(9), pp. 1613-1626. 2003.

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

[15] W., Luo, F. Huang, and J. Huang. "A more secure steganography based on adaptive pixel-value differencing scheme". Multimedia tools and applications, vol. 52(2-3), pp. 407-430, 2011.

[16] Y.-H. Yu, C.-C. Chang, and I.-C. Lin, (2007). "A new steganographic method for color and grayscale image hiding". Computer Vision and Image Understanding, vol. 107(3), pp. 183-194, 2007.

[17] T. Pevny, T. Filler, and P. Bas. "Using high-dimensional image models to perform highly undetectable steganography". in Information Hiding Workshop, vol.6387, 2010, (pp. 161-177).

[18] Z. Sun, and Z. Ji. "A security steganography method for lossy compression gray scale image". In Proc. Of International Conference on Intelligent Computing, Springer, vol. 4681, 2007, pp. 636-645

[19] Q. Liu, A. H. Sung, Z. Chen, and X. Huang. "A JPEG-based statistically invisible steganography".in Proc. of the Third International Conference on Internet Multimedia Computing and Service, ACM, 2011, pp. 78-81.

[20] V. Sachnev, and H. J. Kim. "An improved matrix encoding scheme for JPEG steganography". In International Workshop on Digital Watermarking, Springer, vol. 7128 ,2012, pp. 3-15.

[21] Y.-K. Lin. "High capacity reversible data hiding scheme based upon discrete cosine transformation". Journal of Systems and Software, vol. 85(10), pp. 2395-2404, 2012.

[22] K. Wang, Z.-M. Lu, and Y.-J. Hu. "A high capacity lossless data hiding scheme for JPEG images". Journal of Systems and Software, vol. 86(7), pp. 1965-1975, 2013.

[23] A. Westfeld. "F5—a steganographic algorithm". International workshop on information hiding, Springer, vol. 2137,2001, pp. 289-302.

[24] A. S. Khashandarag, N. Ebrahimian. "a new method for color image steganography using SPIHT and DFT, sending with jpeg format". In proc. Of International Conference on Computer Technology and Development, IEEE, 2009, pp. 582-586.

[25] A. S. Khashandarag, A. H. Navin, M. K. Mirnia, and H. H. A. Mohammadi, "An optimized color image steganography using LFSR and DFT techniques". In Advanced Research on Computer Education, Simulation and Modeling, Springer Berlin Heidelberg, vol. 176, 2011, pp. 247-253.

[26] T. Rabie. "Digital Image Steganography: An FFT Approach". In Networked Digital Technologies, Springer Berlin Heidelberg, vol. 294 ,2012, pp. 217-230.

[27] F. Alturki, and R. Mersereau. "Secure blind image steganographic technique using discrete fourier transformation". In proc. of International Conference of Image Processing, IEEE, vol. 2 ,2001. pp. 542-545.

[28] R. T. McKeon. "Steganography Using the Fourier Transform and Zero-Padding Aliasing Properties". In proc. of International Conference of Electro/information Technology, IEEE, 2006, pp. 492-497.

[29] A. Soni, J. Jain, and R. Roshan. "Image steganography using discrete fractional Fourier transform". In proc. of International Conference of the Intelligent Systems and Signal Processing (ISSP), IEEE, 2013 pp. 97-100.

[30] S. Keshari, & S. G. Modani. "Weighted Fractional Fourier Transform based Image Steganography". In proc. of International Conference of the Recent Trends in Information Systems (ReTIS), IEEE, 2011, pp. 214-217.

[31] A. A. Shejul, & U. L. Kulkarni. "A DWT based approach for steganography using biometrics". In proc. of International Conference of the Data Storage and Data Engineering (DSDE), IEEE, 2010, pp. 39-43.

[32] A. H. Yajurvedi, & S. Kulkarni. "An Adaptive Image Steganography Algorithm Using Successive

Pixel Difference Embedding and Integer Wavelet Transform". In Proc. of the Fourth International Conference on Signal and Image Processing (ICSIP 2012), Springer India, vol. 221, 2013, pp. 203-212.

[33] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi. "High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform". In Proc. of the International Conference in Intelligent Control and Innovative Computing, Springer US, vol.110, 2012, pp. 395-404.

[34] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath. "A Secure Image Steganography Technique to Hide Multiple Secret Images". In Proc. of the International Conference in Computer Networks & Communications (NetCom), Springer New York, vol.131, 2013, pp. 613-620.

[35] N. Raftari, & A. M. E. Moghadam. "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm". In Proc. of the International Conference of the Modelling Symposium (AMS), IEEE,2012, pp. 87-92.

[36] V. Thanikaiselvan, & P. Arulmozhivarman. "High security image steganography using IWT and graph theory". In Proc. of the International Conference of the Signal and Image Processing Applications (ICSIPA), IEEE, 2013, pp. 337-342.

[37] G. Prabakaran, R. Bhavani, and K. Kanimozhi. "Dual transform based steganography using wavelet families and statistical methods". In Proc. of the International Conference of the Pattern Recognition, Informatics and Mobile Engineering (PRIME), IEEE, 2013, pp. 287-293.

[38] M. N. Do, & M. Vetterli. "Contourlets: a directional multiresolution image representation". In Proc. of the International Conference of the Image Processing, IEEE, vol. 1, 2002, pp. 357-360.

[39] M. N. Do, and M. Vetterli. "The contourlet transform: an efficient directional multiresolution image representation". IEEE Transactions on Image Processing, vol. 14(12), pp. 2091-2106, 2005.

[40] M. Mohan, & P. Anurenjan. "A new algorithm for data hiding in images using contourlet transform". In Proc. of the International Conference of the Recent Advances in Intelligent Computational Systems (RAICS), IEEE, 2011, pp. 411-415.

[41] H. Sajedi, and M. Jamzad. "Adaptive steganography method based on contourlet transform". In Proc. of the 9th International Conference of the Signal Processing, IEEE, 2008, pp. 745-748.

[42] H. Sajedi, & M. Jamza. "Using contourlet transform and cover selection for secure steganography". International Journal of Information Security, Springer, vol. 9(5), pp. 337-352, 2010.

[43] M. S. Subhedar, & V. H. Mankar. "Performance Evaluation of Image Steganography based on Cover Selection and Contourlet Transform". In Proc. of the International Conference of the Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), IEEE, 2013 pp. 172-177.

[44] S. Pal, P. Saxena, & S. Muttoo. “Image steganography for wireless networks using the hadamard transform”. In Proc. of the International Conference of the Signal Processing and Communications (SPCOM'04), IEEE, 2004, pp. 131-135.

[45] S. Mutt & S. Kumar. “Secure image Steganography based on Slantlet transform”. In Proc. of the International Conference of the Methods and Models in Computer Science (ICM2CS), IEEE, 2009, pp. 1-7.

[46] A. A. Al-Ataby, & F. M. Al-Naima. “High Capacity Image Steganography Based on Curvelet Transform”. In Proc. of the International Conference of the Developments in E-systems Engineering (DeSE), IEEE, 2011, pp. 191-196.

[47] K. S. Babu, K., Raja, K. Rao, K. Rashmi, K. Venugopal, & L. Patnaik. “Robust and high capacity image steganography using SVD”. In Proc. of the International Conference of the Information and Communication Technology in Electrical Sciences (ICTES 2007), 2007, pp. 718 – 723.

[48] H. Abdallah, M. Hadhoud, & A. Shaalan. “An efficient SVD image steganographic approach”. Paper presented at the Computer Engineering & Systems (ICCES), IEEE, 2009. pp. 257-262.

[49] R. K. Lama, S.-J. Han, & G.-R. Kwon, “SVD based improved secret fragment visible mosaic image generation for information hiding”. Multimedia tools and applications, Springer, vol. 73(2), pp. 1-14, 2013.

[50] K. Raja, K. Kumar, S. Kumar, M. Lakshmi, H. Preeti, K. Venugopal, & L. M. Patnaik. “Genetic algorithm based steganography using wavelets”. In Proc. of the International Conference of the Information Systems Security, Springer Berlin Heidelberg, 2007, pp. 51-63.

[51] V. Kumar, & D. Kumar. “Digital Image Steganography Based on Combination of DCT and DWT”. In Proc. of the International Conference of the Information and Communication Technologies, Springer Berlin Heidelberg, 2010, pp. 596-601.

[52] R. Smko, A. Almarimi, & K. Negrat. “Payload Encoding for Secure Extraction Process in Multiple Frequency Domain Steganography”. In Proc. of the International Conference of the Networked Digital Technologies, Springer Berlin Heidelberg, 2010, pp. 306-313.

[53] S. B., A. Saejung, J. Preechasuk, C. Chantrapornchai. “On the comparison of digital image steganography algorithm based on DCT and wavelet”. In Proc. of the International Conference of the Computer Science and Engineering Conference (ICSEC), IEEE, 2013, pp. 328-333.

[54] A. Mansouri, A. M. Aznaveh, & F. T. Azar. “SVD-based digital image watermarking using complex wavelet transform”. Sadhana, vol. 34(3), pp. 393-406, 2009.

[55] S. KapreBhagyashri, & M. Y. Joshi. "All frequency band DWT-SVD robust watermarking technique for color images in YUV color space". In Proc. of the International Conference of the Computer Science and Automation Engineering (CSAE), IEEE, vol. 3, 2011, pp. 295-299.

[56] N. M. Makbol, & B. E. Khoo. "A Hybrid Robust Image Watermarking Scheme Using Integer Wavelet Transform, Singular Value Decomposition and Arnold Transform". In Proc. of the International Conference in Advances in Visual Informatics, Springer Berlin Heidelberg, 2013, pp. 36-47.

[57] E. Yavuz, & Z. Telatar. "SVD adapted DCT domain DC subband image watermarking against watermark ambiguity". In Proc. of the International Conference in Multimedia Content Representation, Classification and Security, Springer Berlin Heidelberg, 2006, pp. 66-73.

[58] S. Das, & M. K. Kundu. "Hybrid contourlet-DCT based robust image watermarking technique applied to medical data management". In Proc. of the International Conference in Pattern Recognition and Machine Intelligence, Springer Berlin Heidelberg, 2011, pp. 286-292.