Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.10, September 2016 – www.caeaccess.org

Steganography Literature Survey, Classification and Comparative Study

Alaa Fkirin
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Gamal Attiya
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Ayman El-Sayed
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

ABSTRACT

Transmitting confidential images between two channels suffer from hacking. Therefore, protecting confidentiality has become a very essential issue. Recently, several methods are developed to protect important information. The main idea is based on embedding important information in multimedia carrier such as: text, image, audio, and video. The developed methods may be classified as steganography and watermarking. Steganography aims to embed huge amount of secret data in multimedia carrier while watermarking aims to hid small amount of secret data in multimedia carrier. This paper first presents a literature survey of information hiding, then classifies the proposed methods, and finally introduces a comparative study between the different methods.

General Terms

Algorithms, Steganography.

Keywords

Information Hiding, Steganography, Encryption, Stego, Cover, grafia

1. INTRODUCTION

Recently, several methods are developed to protect important information. The developed methods may be classified into two categories: steganography and watermarking. Both steganography and watermarking are data embedding methods. Steganography aims to embedding huge amount of secret data in multimedia carrier such as text, image, audio, and video. On the other hand, watermarking, that may be mainly used for proving copyright, aims to hiding small amount of secret data in multimedia carrier. Although steganography and cryptography have a common goal and are related concepts, the usage and the way of both are somewhat different. Steganography is hiding the message existence completely whereas cryptography is securing the sent message. Steganography's main factors are un-detectability, robustness, and capacity. These factors separate steganography from other related techniques e.g. cryptography and watermarking. Figure 1 presents different branches of information hiding [1]. More details and comparisons are discussed in [1][2]. This paper concerns with steganography based information hiding. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. In other words, steganography is the process of embedding a file, message, image, or video within another file, message, image, or video. The expression steganography combines the Greek word "stego" which means "cover" and the Greek word "grafia" which means "writing", resulting "covered writing"[3].

Steganography has various useful applications. Secret Communications: secret information can be transmitted without being afraid of alerting danger from potential attackers [4]. Feature Tagging Elements: secret data can be embedded beyond an image, such as names of individuals tagged in a photo some locations in a map [5]. Copyright Protection: Aims to prevent data from being copied [5]. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden[6].

The idea of steganography was first presented in [7] at 1983. Figure 2 presents the scenario of steganography system [8]. Steganography scenario can be summarized in two different phases: encoding (embedding) phase with the help of secret key and decoding (extracting) secret data phase with the manner of preserving information invisible. In the embedding phase, the secret message is embedded in an actual/original multimedia carrier (cover message) by using an embedding algorithm and a secret key. The key is used to aid in encryption and to decide where the information should be hidden in the multimedia carrier. After hiding the secret message, one can call it stegomedium and the key which is used for hiding process is called stego-key. In the extracting phase, the secret message is extracted from the multimedia carrier by using an extracting algorithm and the same secret key.

The idea of steganography was first presented in [7] at 1983. Figure 2 presents the scenario of steganography system [8]. Steganography scenario can be summarized in two different phases: encoding (embedding) phase with the help of secret key and decoding (extracting) secret data phase with the manner of preserving information invisible.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.10, September 2016 – www.caeaccess.org

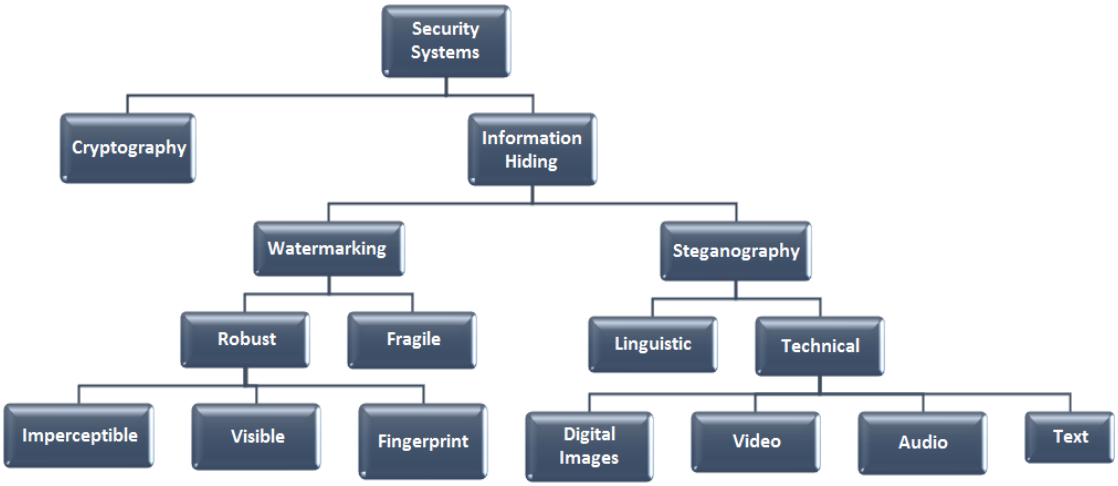

Figure 1: Branches of information hiding [1]

In the embedding phase, the secret message is embedded in an actual/original multimedia carrier (cover message) by using an embedding algorithm and a secret key. The key is used to aid in encryption and to decide where the information should be hidden in the multimedia carrier. After hiding the secret message, one can call it stegomedium and the key which is used for hiding process is called stego-key. In the extracting phase, the secret message is extracted from the multimedia carrier by using an extracting algorithm and the same secret key.

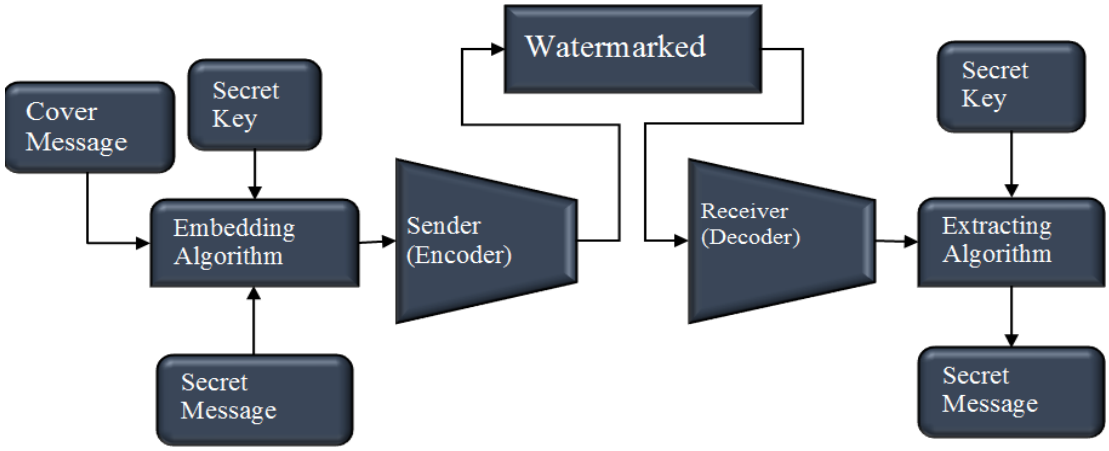

Figure 2: Scenario of a steganography system [5].

Multimedia carriers that may be used in steganography are text, image, video and audio. Text steganography can be achieved by many ways like: using nth text character, altering some rules like spaces, or including a code consisting of page numbers, character or line. However, text steganography lacks security. Audio steganography can be achieved by embedding information into audio signal by using inaudible frequencies to human ear.

Video steganography can be achieved by hiding secret information into a video (stream of moving images and sounds). In this type, any trivial distortions could be unnoticed because of information continuous flow and

the payload capacity will be high which a great advantage is really. Image steganography can be achieved by hiding secret information in a digital image such that someone cannot know the presence or contents of the hidden message.

Although many different carrier file formats can be used, digital images are the most popular because of their frequency on the Internet. Image steganography has its own advantages and is most popular among the others as it has better payload capacity and imperceptibility. This paper focuses on hiding information in digital images. It provides a state-of-the-art review of the different existing methods of image steganography, its uses and techniques along with some common standards and guidelines drawn from the literature. It also attempts to identify the requirements of a good steganographic algorithm. The main purpose is to help future researcher

on this field by providing a simple review of the existing techniques.

The rest of this paper is organized as follows. Section 2 presents brief classification of image steganography techniques. Section 3 describes spatial domain techniques. Section 4 explains transform domain techniques. Section 5 discuss spread spectrum steganography and its characteristics Section 6 introduces briefly the model based steganography Section 7 discuss the hybrid techniques and declare its benefits, also shows recent most effective researches using hybrid techniques. Section 8 presents standard quality measure factors. Section 9 shows comparative study that includes Comparison between spatial and

transform domain techniques, also Comparison between data hiding methods. Finally, the conclusions are presented in section 10.

2. IMAGE STEGANOGRAPHY

Image steganography concerns with hiding secret information in digital images. There exists a large variety of image steganography techniques. Some of these techniques are more complex than the others, and all of them have respective strong and weak points. Image steganography techniques can be classified into spatial domain (image domain) steganography, transform domain (frequency domain) steganography, spread spectrum steganography and model based steganography. Figure 3 shows a classification tree of image steganography techniques. The following sections describe the different methods of image steganography.

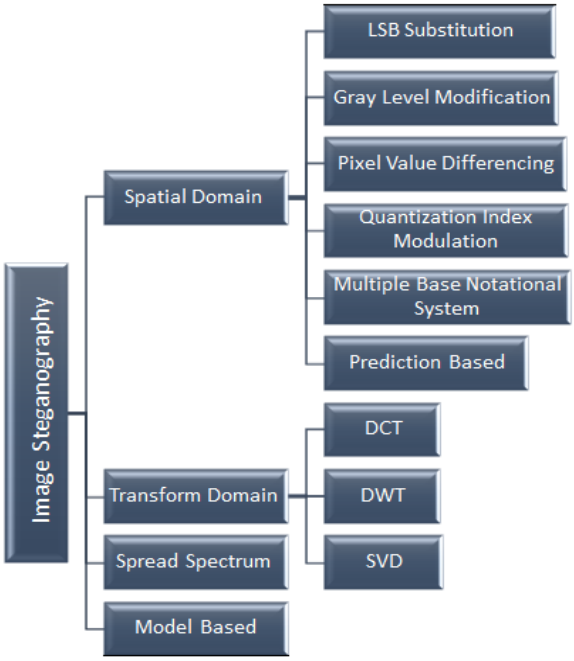

Figure 3: Classification of image steganography techniques [9]

3. SPATIAL DOMAIN METHODS

Image domain applies bit insertion and noise manipulation of a covered image. In spatial domain steganography, embedding the secret message will be done to the pixels directly [10], for example, Least Significant Bit (LSB), gray level modification, pixel value differencing, quantization index modulation, multiple base notational system, and prediction based.

3.1 Least Significant Bit

LSB is a simple and common method for burying information on cover image [11]. Digital images can be classified as grayscale (8-bit-planes) or colored (24 bit-planes) which depends on each pixel intensity levels, i.e., each pixel can be represented by 24-bits, 8-bits or even only one bit. If every pixel of the digital image is assumed as n bits then the digital image can be composed of n numbers of 1-bit planes in the range from bit-plane zero to bit-plane n-1 [12]. For example, in a gray scale image each pixel is represented by eight bits, so the image can be sliced onto eight slices (bit planes) from bit-plane zero to bit-plane 7. These eight slices are divided onto two parts: Most Significant Bits (MSE) and Least Significant Bits (LSB) [13]. LSB do not hold visually important data, so that is the perfect environment for embedding watermark bits. In this method, the process of embedding depends on choosing a subset of cover image and applying the substitution operation on them. That exchanges the LSB of cover image by the watermark [14]. The LSB method is characterized by simplicity, high capacity, easy to understand and implement, and can't be noticed by the naked eye [15]. However, the drawbacks of this methods are that lacks robustness (Easy manipulation by attackers), susceptible to noise, scaling and cropping.

3.2 Image Downgrading and Covert Channels

Image downgrading is considered as substitution system where images act as both covers and secret messages. This case had been discussed in [16], where the authors had fears about security threats which face operating systems with high-security which is called image downgrading because it could help on exchanging images secretly.

The main idea of image downgrading depends on making the cover-image and the secret image equal in dimensions. Then, the sender exchanges the four least significant bits values of the cover image (grayscale or color) with the four most significant bits of the chosen secret image. In extraction, the receiver extracts the four least significant bits out of the watermarked image, and then it gets to the most significant bits of the secret image. In many cases, the degradation of the cover image is not noticeable by naked eye, as four bits are enough for transmitting rough approximation of the secret image. In the multilevel security systems, like the system used by the army, sometimes it is necessary to declassify the form of some information. For example, if they want to change it from 'top secret' onto 'confidential'' or from 'confidential' onto 'public' or even from 'top secret' to 'public'. This is not easy specially if they need to downgrade images [17].

3.3 Gray Level Modification

In 2004, Potdar et al. [18] discussed a technique based on a mathematical function. This technique maps data by altering gray levels of the pixels without embedding or hiding it and uses the conception of even and odd numbers in mapping the data in the cover image. For example, even values are mapped with zero and odd values are mapped with one. The gray level modification method is characterized by low computational complexity and high capacity.

3.4 Pixel Value Differencing

In 2003, Da-Chun et al. [19] developed a new embedding method, called Pixel Value Differencing (PVD), based on the difference between pixel values.

First, they divide the cover image into non-overlapping blocks having two connecting pixels. Then, they modify each block difference. They found that the larger the difference into original pixel value, the greater the modification will be. They also found that the embedded secret bits number depends on the pixel case that will be in smooth area or in edge area. In smooth area, the difference between adjacent pixels is less whereas in edge area it is more. Therefore, the data that is embedded into edge area pixels is more than embedded into smooth area. This technique is better than LSB in watermarked image quality and imperceptibility [19].

In [20], the authors discuss how to secure communication and overcome attacks using the PVD. They proposed many approaches like: "PVD method vulnerable to histogram analysis". In [21], the authors discussed how to get benefit from combination between modulus function and PVD in order to do data hiding. In [22] and [23] many types of PVD are developed like: four pixel PVD. In [24], a scheme uses two, three and four pixels (neighbor) for embedding decision is established.

3.5 Quantization Index Modulation

Quantization Index Modulation (QIM) technique is considered host interference rejection method, as there is no need to the host signals in decoding process. QIM can be used for steganography purposes and also for digital watermarking. QIM is based on embedding information in the cover medium by first modulating an index or (sequence of indices) through the embedded information. Then, quantizing host signal with quantizer or (sequence of quantizes) [25]. The quantization index modulation technique is characterized by the ability to control robustness and high embedding capacity [25].

3.6 Multiple Base Notational System

Multiple Base Notational System (MBNS) steganography is based on converting secret data into symbols in a notational system that has multiple bases. Then, modifying the pixels of the host image, in which the remainders of values of the pixel, which are divided by bases, will be equal to symbols. Briefly, it is known that binary number system (base 2) is the main basis of computer. In most cases, secret message is binary stream, and the quantity of data enclosed into each symbol is one bit. Therefore, to embed additional data into the busy areas, the message will appear as an integer number (by using variable base system). That means, the message can be converted into series of symbols which have different information carrying abilities depends on different bases used. Greater base will lead to extra information in corresponding symbol [9]. In [26], the authors introduced (2n + 1) base system using a method called Exploiting Modification Direction (EMD). In [27] a novel strategy to hide data is established based on using combination between VQ and MBNS. The MBNS technique is characterized by high payload capacity is achieved, better invisibility than PVD and better PSNR than PVD.

3.7 Prediction Based Steganography

In [28], a scheme based on prediction based steganography is developed. The predictive coding approach is introduced as a solution to the problem of stego image distortion (which came from embedding data by modifying the values of the pixel directly), as 'prediction based steganography' predicts pixel values using a predictor which estimates input image pixel values [9]. The prediction based steganography technique is characterized by high payload capacity. This scheme hide tree proved superior with nearly 99.85% capacity of embedding.

4. TRANSFORM DOMAIN TECHNIQUES

Transform Domain applies image transformation and manipulation of algorithm. In transform domain steganography, embedding the secret requires transforming the image from the spatial domain to the frequency domain by using any of the transforms, for example, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Single Value Decomposition (SVD). After the transformation process, the embedding process will be done in proper transform coefficients.

4.1 Discrete Cosine Transformation

Discrete Cosine Transform (DCT) is based on transforming signal or image from spatial domain to frequency domain. The DCT split the image as shown in figure 4 up to spectral sub-bands (parts) of different significance with respect to the visual quality of the image [29]. Embedding positions Choices: (i) Low-frequency coefficients: Bad invisibility, because human eye is sensitive to noise on it, as it contains the image visual parts, (ii) High-frequency coefficients: bad robustness, as the image could be corrupted through noise attacks or compression, and (iii) Middle-frequency coefficients: good invisibility and robustness, so it is the best choice.

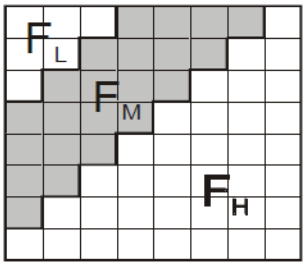

Figure 4: Discrete Cosine Transform[30].

Assume that X is the original gray scale image with size N1XN2, and the watermark W with size M1XM2. In W, the value of the marked pixels is ones, and the value of others are zeros [31]. The original image is represented as:

$$X = \{x(i,j), 0 \le i < N1\ , 0 \le j < N2\}$$

Where, $x(i,j) \in \{0, \dots, 2^L - 1\}$ represents intensity of the pixel $x(i,j)$ and L represents the bits number of each pixel.

The watermark is represented as:

$$W = \{w(i,j), 0 \le i < M1\ , 0 \le j < M2\}$$

Where, $w(i,j) \in \{0,1\}$.

For each 8x8 image block for watermark embedding only $(64x\frac{M1XM2}{N1XN2})$ coefficients is used. Where, the amount of embedded information into the image is determined by the ratio $\frac{M1XM2}{N1XN2}$.

Generally, in order to achieve more robustness, the amount of embedded information should be reduced [31].

During embedding process, the sender first splits image into 8×8 blocks. Then, performing DCT on each block of these blocks where every block encodes one secret message bit. Next, select a pseudorandom block which will code the message bit. After that, the watermark is embedded in the coefficients of middle band frequencies [32] [30], as shown in the figure. Finally, apply inverse DCT (IDCT) in order to map back the coefficients to the space domain.

During extraction process, first apply DCT to both watermarked image and original image. Then, extract permuted data by at last apply IDCT.

The DCT is characterized by the most robust technique to lossy compression and Image visibility is protected [33]. However, the drawbacks of this method are that Block effect Picture cropping effect.

4.2 Discrete Wavelet Transformation

Wavelet transform is used in a wide range in signal processing applications and image compression. It separates the signal to set of basic functions which are called wavelets. Discrete Wavelet Transform (DWT) is described as an efficient and very flexible method for decomposing signals sub bands. In recent years, JPEG committee releases a new standard of image coding is called 'JPEG-2000' which is based on DWT [34].

DWT is used in a wide range in signal processing applications for example audio, video and image compression. In case of one-dimensional DWT, image is decomposed into 4 bands denoted by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level [35], as shown in Figure 5 (a). Where, H symbolizes high-pass filter (High frequency) and L symbolizes low-pass filter (Low frequency). In case of Multi-Level Discrete Wavelet Transform, as shown in Figure 5 (b). This represents the image after applying three times of DWT. The image consists of frequency areas of LL1, LH1, HL1, HH1. The LL1 (low-frequency area) is decomposed onto sub-level frequency area information of LL2, LH2, HL2, HH2. By applying previous decomposition again and again the image can be decomposed onto N level wavelet transformation [36]. When N decomposition is reached, as shown in Figure 5 (c), it will be 3N+1 sub-bands containing the multi-resolution sub-bands (LLN) and HLx, LHx and HHx, where, x ranges from one to N [37].

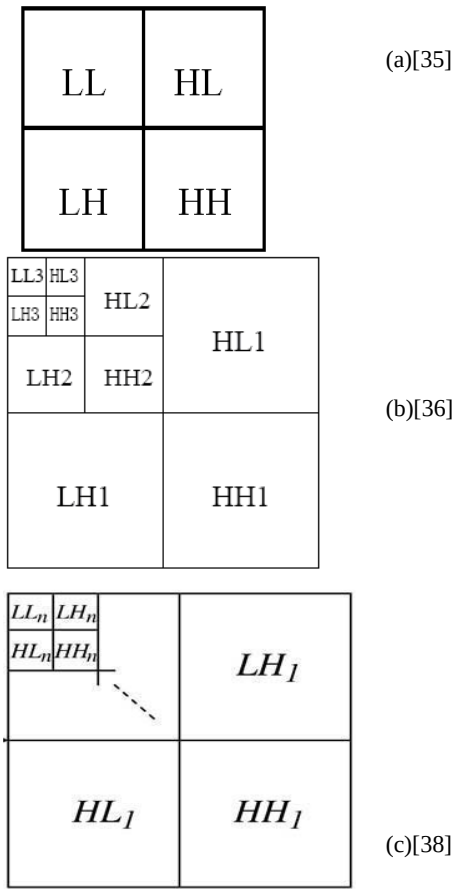

Figure 5: Discrete Wavelet Transform (DWT)

As the most essential part of image is concentrated at LLx (lower frequency sub-bands), the embedding of the watermark in this sub-bands will cause a problem because this may reduce the quality of the image significantly. Otherwise, HHx (high frequency sub-bands) contain the textures and edges of the image and the changes on such sub-bands cannot be noticed by human naked eyes. So, The embedding process will be done on the coefficients of high frequency sub-bands [39]. After embedding watermark, perform inverse Discrete Wavelet Transformations (IDWT). These transformations are applied in order to obtain the watermarked image [29].

In order to extract the watermark, first, execute N-level DWT on the watermarked image. Then, find the embedding locations. Finally, perform comparison between watermarked image and cover image in order to obtain the watermark [38].

The DWT is characterized by Imperceptibility and Robustness. However, the drawbacks of this method are that Long compression time, High computational cost, Noise/blur close to edges of images

4.3 Singular Value Decomposition

Singular Value Decomposition (SVD) is a mathematical technique based on a linear algebra theorem which declares that the rectangular matrix (A) can be analyzed into three matrices [40]: U (Orthogonal matrix), S

(Diagonal matrix), and V (Transpose of an orthogonal matrix). The theorem is presented usually like: $A = USV^T$

For Embedding [33]:

- Apply SVD to the original image: $\boldsymbol{A = USV^T}$
- Add watermark to the SVs of the diagonal matrix of the original image: $\mathbf{D = S + kW}$
- Apply SVD to the modified new matrix resultant from step2: $\mathbf{D = U_W S_W V_W^T}$
- Get the watermarked image by using the modified matrix: $\mathbf{A_W = US_W V^T}$

Where, A is the original image, W is the watermark image, A_W is the watermarked image, k is a factor which controls the watermark strength.

For Extraction [33]:

- Apply SVD to the watermarked image. $\boldsymbol{A_W^* = U^* S_W^* V^{*T}}$
- Compute the matrix that contains the watermark. $\boldsymbol{D^* = U_W S_W^* V_W^T}$
- Obtain the watermark.$\boldsymbol{W^* = \frac{D^* - S}{K}}$

Where, * is a mark of possible corruption owing to attacks.

The SVD is characterized by resultant matrices size from SVD is not fixed (square or rectangle) and Image singular values (SVs) which preserve image most energy, resist against attacks and having intrinsic algebraic image properties. However, the drawback of this method is diagonal that will appear in the extracted watermark.

5. SPREAD SPECTRUM STEGANOGRAPHY

In [41], the authors proposed a spread spectrum method based on spreading the narrowband bandwidth of a signal across wideband of frequencies. In [42], an approach depends on spread spectrum is presented. In this approach, the secret data was embedded in GF(2m) Galois Field. In [43], the authors presented correlation in addition to bit aware concept with spread spectrum steganography. They proposed two enhanced data hiding approaches. The spread spectrum method is characterized by robustness versus statistical attacks.

6. MODEL BASED STEGANOGRAPHY

Model based steganography is a model which is presented in order to overcome the weaknesses in the data hiding embedding process such as: problems that faces spatial domain, Stego image distortions and modifications [9]. In [44] the authors proposed 'model based steganography' based on statistical properties of cover medium. This model is considered as statistics aware steganography or adaptive steganography. This new method helps to embed secret message taking care of overcoming previous drawbacks. In this method, the embedding process works as follows. The cover image was divided into two parts: part that was not altered during embedding and the other part were used to carry secret message without modifying the cover statistical properties. The hidden message is supposed to be a random uniform stream of bits. By using an entropy decoder (which is chosen according to probability conditional distribution), the hidden message was processed. For extracting, first, entropy encoder was used. Then, the stego message was separated into two parts. After that, Probability distribution was calculated, finally, the secret message is obtained. An adaptive steganography survey is introduced in [45].

7. HYBRID TECHNIQUE

Some researchers combine two or more approaches of the previous techniques to procedure a new technique. Due to this combination, the disadvantages of one method will be removed because of the effect the other used technique. Therefore, the hybrid techniques are better than individual previous techniques.

In [46], a hybrid watermarking technique combined fragile and robust techniques is introduced to improve authentication, verification, integrity and copyright protection at the same time. In [47], a hybrid DWT-SVD technique is proposed by using human Visual System Model and compared with SVD only [48]. The comparison proved that the hybrid method is better in PSNR and BCR (Bit Correlation Rate). In [49] a hybrid DCT-SVD technique is proposed for copyright protection. This method is more robust, also achieves better PSNR and correlation. In [50] a hybrid method combined of DWT, DCT and SVD is Proposed and compared with [51] that used only DWT and [52] that used DCT and SVD. The comparison proved that the hybrid method [50] is better in PSNR and correlation. In [53], a hybrid method combines the three techniques DCT,DWT and SVD is presented and found that the results are improved. In [54] a hybrid technique combines DWT and DCT is proposed while a hybrid technique which combines DWT and SVD is developed in [55]. In these methods, the PSNR value was improved and the robustness was high. In [56] a hybrid technique combines DWT, DCT and SVD is proposed. The experimental results show that the image can overcome JPEG lossy compression and cropping of an image.

8. PERFORMANCE METRICS

Spreading multimedia technology and internet cause a big motivator of choosing quality measure factors for transmission and retrieval of the data. These factors should be standard. The formulas and description is in [57][58][59].

8.1 Peak Signal to Noise Ratio (PSNR)

Quality of the watermarked image can be measured by PSNR. In the ideal case, Peak Signal to Noise Ratio should be infinite. In real, this can't be achieved to the watermarked image, consequently big PSNR will be good.

$$PSNR = 10log_{10}(\frac{max * max}{MSE})$$

Where max = 255 for grey scale image.

8.2 Correlation Coefficient (CR)

the correlation coefficient is used in measuring original image and watermarked image. In ideal case, CR should equal 1. But this may not be possible, so if the value of CR is near one, it is ok.

$$C_r = \frac{\sum_m \sum_n (Xi - X')(Yi - Y')}{\sqrt{(\sum_m \sum_n (Xi - X')^2)(\sum_m \sum_n (Yi - Y')^2)}}$$

Where, X' is the original image average value and Y' is the watermarked image average value.

8.3 Mean Square Error (MSE)

MSE is another watermarked image measurement of Quality. In the ideal case, Mean Square Error should be zero. In real, this is can't be achieved to the watermarked image, minor MSE is good.

$$MSE = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{ORG(i,j) - WM(i,j)}{m * n}$$

Where, 'ORG' is the original image, 'WM' is the watermarked image and m & n are the original image size.

9. COMPARATIVE STUDY

Table 1 illustrates the differences between spatial domain watermarking methods and transformation domain watermarking methods with respect to embedding modality, imperceptibility, capacity, robustness, complexity and processing time [46].

Table 1 Comparison between spatial domain techniques and transform domain techniques

Domain / Factor	Spatial	Transform
Embedding	Directly onto image pixels	On transform coefficient
Imperceptibility	Highly controllable	Lower controllable
Capacity	High	Low
Robustness	Low	High
Complexity	Low	High
Processing time	Low	High

Table 2 illustrates a brief comparison between data hiding methods with respect to domain, robustness, capacity, complexity and also a summarized conclusion for each method.

Table 2 Comparison between data hiding methods

	Algorithm	Robustness		Complexity	Conclusion
Domain: Spatial	LSB [11] [13][14]	Low	Capacity: High	Low	LSB does not provide great level of security as it can be easily manipulated, LSB can simply be replaced by an enormous amount of watermark bits.
	Grey level modification [18]	Moderate		Low	GLM is perfect in industry scale systems and networks. GLM can be used in data and server security, and also in protection without needing to use third party trustees.
	Pixel value differencing (PVD) [19]	Low		High	PVD is better than LSB in watermarked image quality and imperceptibility.
	Quantization Index Modulation (QIM) [25][60]	High against AWGN (message is embedded by adding of white Gaussian noise)		Low	QIM methods are better than spread spectrum(SS) against additive noise corruption
	Multiple Base Notational System (MBNS) [61]	Low		-	MBNS is better than PVD In terms of PSNR and invisibility
	Prediction based steganography [28][62]	Low		Low	Prediction based steganography is proved to be perfect in increasing capacity payload as shown by Wu et al. as it leads to nearly 99.85% capacity of embedding.
Domain: Transform	Discrete Cosine Transformation (DCT) [33]	High But is affected by cropping	Capacity: Low	Low	DCT is The most robust technique to lossy compression, but it is not robust against picture cropping effect
	Discrete wavelet transformation (DWT) [63]	High		Moderate but may reach high	DWT is described as an efficient and very flexible method.

Table 2 Comparison between data hiding methods (continue)

	Algorithm	Robustness		Complexity	Conclusion
Domain: Transform	Singular Value Decomposition (SVD) [64][65]	High	Capacity: Low	High	SVD is robust but it faces the problem of diagonal that will appear in the extracted watermark.
	Spread Spectrum steganography [62][42]	High	Capacity: Low	High	SS present good watermarked image quality and high level of security against various attacks.
	Model Based steganography [62], [66] [9]	High	Capacity: High	Low	Model based steganography embeds the secret data in cover image with no change in its properties This technique overcome the weaknesses in the data hiding embedding process such as: problems that faces spatial domain, Stego image distortions and modifications

10. CONCLUSIONS

In this paper, a literature survey of digital image steganography information hiding techniques is presented. first, a classification of watermarking algorithms based on embedding domain is shown. These domains are spatial domain, transform domain, Spread Spectrum steganography, Model Based steganography. All these algorithms try to satisfy three most important factors of steganographic design i.e. un-detectability, robustness, and capacity. then, some hybrid techniques are discussed. Finally, a comparative study between the different methods is introduced. It is clearly observed that the embedding procedure is easy in spatial domain techniques compared to complex transform domain techniques. Also, Spatial domain techniques are simple and have high stego visual quality, but transform domain techniques are more robust and less exposure to image processing attacks. From the paper, it can be concluded that every technique has advantages and disadvantages if compared with other techniques of steganography. Which mean that it is not fair to call any method 'the best or the worst of all'. So determining the suitable method is chosen based on the wanted purpose.

11. ACKNOWLEDGMENTS

An acknowledgement to Academy of Scientific Research and Technology for its contributing constructively in completion of this paper.

12. REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography : Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[2] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice," in *Digital Watermarking*, Springer Berlin Heidelberg, 2004, pp. 35–49.

[3] E. E. A. Elgabar and H. A. A. Alamin, "Comparison of LSB Steganography in GIF and BMP Images," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, no. 4, pp. 79–83, 2013.

[4] L. Zhang, J. Wu, and N. Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos †," in *Proceeding of Fifth International Conference on Information Assurance and Security*, 2009, pp. 61–64.

[5] P. Ajit and K. Chouhan, "A Study and literature Review on Image Steganography," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 6, no. 1, pp. 685–688, 2015.

[6] P. B. Kutade and P. S. A. Bhalotra, "A Survey on Various Approaches of Image Steganography," *International Journal of Computer Applications*, vol. 109, no. 3, pp. 1–5, 2015.

[7] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," in *Advances in Cryptology: Proceedings of CRYPTO '83*, springer, 1983, pp. 51–67.

[8] N. Akhtar, P. Johri, and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," in *Proceeding of 5th International Conference on Computational Intelligence and Communication Networks*, 2013, pp. 385 – 390.

[9] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, vol. 13–14, pp. 95–113, 2014.

[10] D. Salomon, *Coding For Data And Computer Communications*. California State University: Springer, 2005.

[11] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, 1998.

[12] M. Mishra and F. L. D. M. C. Adhikary, "An Easy yet Effective Method for Detecting Spatial Domain LSB Steganography," *International Journal of Computer Science and Business Informatics*, vol. 8, no. 1, pp. 1–12, 2013.

[13] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk,

"Watermarking Digital Image and Video Data A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[14] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding techniques for stegnography and digital watermarking*. Artech House, Inc. Norwood, MA, USA, 2000.

[15] P. C. Mandal, "Modern Steganographic technique : A survey," *International Journal of Computer Science & Engineering Technology (IJCSET)*, vol. 3, no. 9, pp. 444–448, 2012.

[16] C. Kurak and J. McHugh, "A Cautionary Note On Image Downgrading," in *Proceeding of Computer Security Applications Conference, Eighth Annual*, 1992, pp. 153–159.

[17] F. Petitcolas, "The information hiding homepage." [Online]. Available: http://www.petitcolas.net/steganography/image_downgrading/.

[18] V. M. Potdar and E. Chang, "Grey Level Modification Steganography for Secret Communication," in *Proceeding of 2nd IEEE International Conference on Industrial Informatics*, 2004, pp. 223 – 228.

[19] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, 2003.

[20] Xinpeng Zhang and S. Wang, "Vulnerability of pixel-value differencing stegnography to histogram analysis and modification for enhanced security," *Pattern Recognition Letters*, vol. 25, no. 3, pp. 331–339, 2004.

[21] J. C. Joo, H. Y. Lee, and H. K. Lee, "Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, pp. 1–13, 2010.

[22] C. H. Yang, C. Y. Weng, H. K. Tso, and S. J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," *The Journal of Systems and Software*, vol. 84, no. 4, pp. 669–678, 2011.

[23] Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. Su, and C. P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Information Sciences*, vol. 191, pp. 214–225, 2012.

[24] G. Swain and S. K. Lenka, "Steganography using two sided , three sided , and four sided side match methods," *CSI Transactions on ICT*, vol. 1, no. 2, pp. 127–133, 2013.

[25] B. Chen and G. W. Wornell, "Quantization Index Modulation : A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[26] T. D. Kieu and C. C. Chang, "A steganographic scheme by fully exploiting modification directions," *Expert Systems with Applications*, vol. 38, no. 8, pp. 10648–10657, 2011.

[27] C. C. Chang, T. S. Nguyen, and C. C. Lin, "A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies," *The Journal of Systems & Software*, vol. 86, no. 2, pp. 389–402, 2013.

[28] H. C. Wu, H. C. Wang, C. S. Tsai, and C. M. Wang, "Reversible image steganographic scheme via predictive coding," *Displays*, vol. 31, no. 1, pp. 35–43, 2010.

[29] T. Bhattacharya, N. Dey, and S. R. B. Chaudhuri, "A Session based Multiple Image Hiding Technique using DWT and DCT," *International Journal of Computer Applications*, vol. 38, no. 5, pp. 18–21, 2012.

[30] J. Jeswani and D. T. Sarode, "A New DCT based Color Video Watermarking using Luminance Component," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, no. 2, pp. 83–90, 2014.

[31] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," *IEEE TRANSACTIONS ON IMAGE PROCESSING*, vol. 8, no. 1, pp. 58–68, 1999.

[32] S. R. Hallur, S. Kuri, G. S. Sudi, and D. G.H.Kulkarni, "A Robust Digital Watermarking For Gray Scale Image," *International Journal For Technological Research In Engineering*, vol. 2, no. 10, pp. 2440–2443, 2015.

[33] O. S. Faragallah, "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain," *AEU - International Journal of Electronics and Communications*, vol. 67, no. 3, pp. 189–196, 2013.

[34] D. Gupta and S. Choubey, "Discrete Wavelet Transform for Image Processing," *International Journal of Emerging Technology and Advanced Engineering*, vol. 4, no. 3, pp. 598–602, 2015.

[35] E. E. D. Hemdan, N. El Fishawy, G. Attiya, and F. A. El-Samie, "Hybrid Digital Image Watermarking Technique for Data Hiding," in *Prceeding of 30th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2013)*, 2013, pp. 220–227.

[36] M. Jiansheng, L. Sukang, and T. Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT," in *Proceeding of nternational Symposium on Web Information Systems and Applications*, 2009, pp. 104–107.

[37] A. Al Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science*, vol. 3, no. 9, pp. 740–746, 2007.

[38] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on DWT-SVD," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 1002–1013, 2009.

[39] P. Rai, S. Gurung, and M. K. Ghose, "Analysis of Image Steganography Techniques : A Survey," *International Journal of Computer Applications*, vol. 114, no. 1, pp. 11–17, 2015.

[40] E. E. D. Hemdan, N. El Fishawy, G. Attiya, and F. A. El-Samie, "An Efficient Image Watermarking approach based on Wavelet Fusion and Singular Value Decomposition in Wavelet Domain," in *Proceeding of 3rd International Conference on ADVANCED CONTROL CIRCUITS AND*

SYSTEMS (ACCS'013), 2013, no. 1–10.

[41] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE TRANSACTIONS ON IMAGE PROCESSING*, vol. 8, no. 8, pp. 1075 – 1083, 1999.

[42] S. A. Halim and M. F. A. Sani, "Embedding Using Spread Spectrum Image Steganography with GF(2m)," in *Proceedings of the 6th IMT-GT Conference on Mathematics, Statistics and its Applications*, 2010, pp. 659–666.

[43] A. Valizadeh and Z. Jane Wang, "Correlation-and-Bit-Aware Spread Spectrum Embedding for Data Hiding," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 6, no. 2, pp. 267 – 282, 2011.

[44] P. Sallee, "Model-Based Steganography," in *Digital Watermarking*, Springer Berlin Heidelberg, 2004, pp. 154–167.

[45] M. Mahajan and D. N. Kaur, "Adaptive Steganography : A survey of Recent Statistical Aware Steganography Techniques," *International Journal of Computer Network and Information Security*, vol. 4, no. 10, pp. 76–92, 2012.

[46] S. M. Mousavi, A. Naghsh, and S. A. R. A. Bakar, "Watermarking Techniques used in Medical Images : a Survey," *Journal of Digital Imaging*, vol. 27, no. 6, pp. 714–729, 2014.

[47] R. Mehta and N. Rajpal, "A Hybrid Semi-Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model," in *Proceeding of Sixth International Conference on Contemporary Computing (IC3)*, 2013, pp. 163–168.

[48] C. C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Optics Communications*, vol. 284, no. 4, pp. 938–944, 2011.

[49] P. Singh and S. Agarwal, "A Hybrid DCT- SVD Based Robust Watermarking Scheme for Copyright Protection," in *Proceeding of AFRICON*, 2013, pp. 1–5.

[50] M. I. Khan, M. M. Rahman, and M. I. H. Sarker, "Digital Watermarking for Image Authentication Based on Combined DCT , DWT and SVD Transformation," *International Journal of Computer Science Issues*, vol. 10, no. 3, pp. 223–230, 2013.

[51] P. Tao and A. M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain," in *Proceedings of the International Society for Optical Engineering (SPIE)*, 2004, pp. 133–144.

[52] P. S. Murty, S. D. Kumar, and P. R. Kumar., "A Semi Blind Self Reference Image Watermarking in Discrete Cosine Transform using Singular Value Decomposition," *International Journal of Computer Applications*, vol. 62, no. 13, pp. 29–36, 2013.

[53] M. M. Rahman, "A dwt, dct and svd based watermarking technique to protect the image piracy," *International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT)*, vol. 4, no. 2, 2013.

[54] L. K. Saini and V. Shrivastava, "A New Hybrid DWT-DCT Algorithm for Digital Image Watermarking," *International Journal of Advance Engineering and Research Development (IJAERD)*, vol. 1, no. 5, pp. 1–8, 2014.

[55] S. Sirmour and A. Tiwari, "A Hybrid DWT-SVD Based Digital Image Watermarking Algorithm for Copyright Protection," *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 6, pp. 7–10, 2014.

[56] M. Tikariha and A. K. Dey, "An Efficient JND based Digital Image Watermarking using Hybrid DWT-DCT-SVD Approach," *INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR)*, vol. 10, no. 1, pp. 11–20, 2015.

[57] I. Avcıbas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," *Journal of Electronic Imaging*, vol. 11, no. 2, pp. 206–223, 2002.

[58] I. Avcıbas, N. Memon, and B. Sankur, "Steganalysis Using Image Quality Metrics," *IEEE TRANSACTIONS ON IMAGE PROCESSING*, vol. 12, no. 2, pp. 221–229, 2003.

[59] M. A. Mohamed and A. M. El Mohandes, "Hybrid DCT-DWT Watermarking and IDEA Encryption of Internet Contents," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 1, pp. 394–401, 2012.

[60] S. P. Maity and M. K. Kundu, "Perceptually adaptive spread transform image watermarking scheme using Hadamard transform," *Information Sciences*, vol. 181, no. 3, pp. 450–465, 2011.

[61] X. Zhang and S. Wang, "Steganography Using Multiple-Base Notational System and Human Vision Sensitivity," *IEEE Signal Processing Letters*, vol. 12, no. 1, pp. 67–70, 2005.

[62] S. Singh and V. K. Attri, "State-of-the-art Review on Steganographic Techniques," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 7, pp. 161–170, 2015.

[63] R. K. Nayak, P. A. Saxena, and D. M. Manoria, "A Survey & Applications of Various Watermarking & Encryption Techniques," *International Journal of Scientific & Engineering Research*, vol. 6, no. 5, pp. 1532–1537, 2015.

[64] C. C. Lai and C. C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 11, pp. 3060–3063, 2010.

[65] C. C. Chang, P. Tsai, and C. C. Linc, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, 2005.

[66] A. A. Hanafy, G. I. Salama, and Y. Z. Mohasseb, "A secure covert communication model based on video steganography," in *Proceeding of IEEE Military Communications Conference (MILCOM)*, 2008, pp. 1 – 6.