A COMPREHENSIVE REVIEW ON STEGANOGRAPHIC TECHNIQUES AND IMPLEMENTATION

S. Jeevitha[1] and N. Amutha Prabha[2]
[1]School of Electronics Engineering, VIT University, Vellore, India
[2]School of Electrical Engineering, VIT University, Vellore, India
E-Mail: jeevitha.s2016@vitstudent.ac.in

ABSTRACT

Steganography is the hidden communication, concealing the existence of secret information. Steganography hides the secret messages with high security by obscurity. This technique is mainly used in image processing to maintain its confidentiality, provides authentication and improves the medical image security. This paper provides a state-of-the-art review of the steganographic techniques such as Spatial and Transform domain embedding schemes, the different algorithm utilized to implement the embedding and extracting process in steganographic system. Implementation of steganography yields high Imperceptibility, Robustness, embedding capacity, security with PSNR.

Keywords: authentication, imperceptibility, steganography, spatial domain, transform domain, PSNR.

1. INTRODUCTION

Image processing is an important tool for image understanding and analysis. This is used to enhance or extract an important features or information from the image. Image processing is applied in several areas such as Multimedia, computing, secured image communication, biomedical imaging, remote sensing, pattern recognition, image compression and retrieval etc.

Now-a-days image processing plays a major role in bio-medical field. In upcoming years [1] the tremendous growth of information and digital communication technology becomes more appropriate and necessary demand in various sectors like government, banking, education, and healthcare for data exchanging and sharing, Blaze to medical information, involves in the communication of patient data between different doctors and provides robust and efficient remote diagnosis.

Digital medical images are most fundamental for diagnosis and treatment of many diseases. Hence, it is very potentially important to guarantee secure storage, processing and analysis of medical images. Diagnostic and therapy are the most specific in this field, where X-rays (CT scans), Magnetism (MRI), Sound (ultrasound), radioactive pharm1aceuticals (nuclear medicine: SPECT, PET) or light (endoscopy, OCT) are used to identification. But presently, the recent and advanced techniques like cryptography and steganography are implemented for high security and image quality. Cryptography technique is converting the input of plain text block into the output of cipher text block and vice-versa. The cryptography technique just hiding the secret data but cannot conceal the existence of the secret message. This provides the attention to the intruders. This may leads to serious causes when communicating the patient information between the doctors and someone not yet under suspicion has obvious implications. The several drawbacks of the cryptography techniques are difficult to access even for a legitimate user, information security cannot be ensured, Selective access control, high cost, does not guard against the vulnerabilities and threats that emerge from the poor design of systems.

In modern era, the steganographic technique emerges to overcome the limitations in cryptography and also implements a high secure communication in medical field. Steganography [2] is an art and science of hiding and sending the content of secret information used in invisible communication. Steganography is the presently applicable hiding scheme which is mainly used to transform the high dynamic range images securely over the insecure medium in the bio-medical field. Steganography embeds the secret data into the different kind of digital carrier media such as Text, image, audio and video [3].

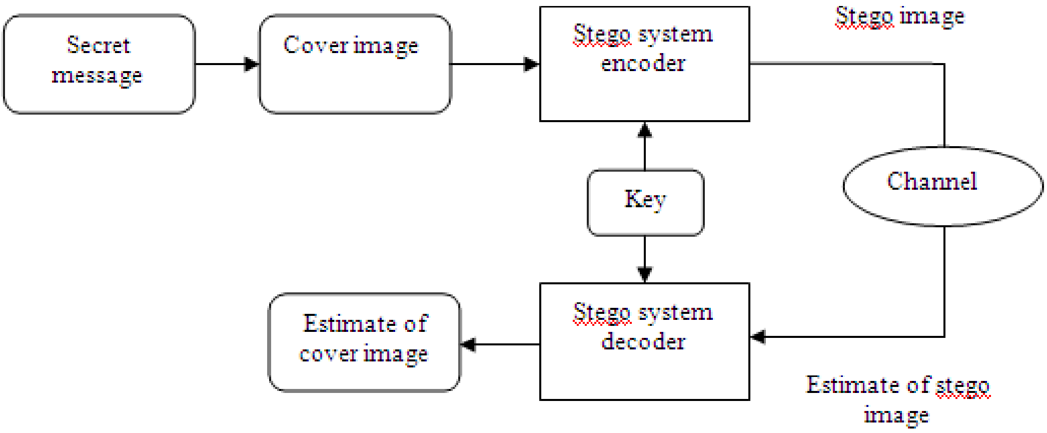

Figure-1. Systematic model of Image Steganography System [4].

The systematic model of steganography system has shown in below Figure-1. Cover image is the original image, used to hide the secret message [5, 6]. Stego image is the image where the secret image embedded. Steganography hides or embeds the secret information into cover image and produces the stego image (combination of cover image and embedded message). Stego encoder system is a device used to convert the cover image into stego image. Stego system decoder decodes the payload that was hidden in a stego image.

The steganographic techniques are divided into two domains: Spatial domain and Transform domain [7, 8]. By using these domains the secret information can be hiding into an image. In spatial domain, the data gets directly embeds into the image. The merits are more data can be stored, easy implementation. Transform domain techniques embed the secret data into the different range of frequency bands in cover image. It is having high computational cost, less embedding capacity and low payload compare with the spatial domain.

The Steganographic technique [9] satisfies the important requirements such as Imperceptibility, robustness, hiding capacity, undetectibility, and invisibility and signal to noise ratio. Steganography overwhelms by providing higher level of security, high embedding capacity, low distortion and better authentication. It is applicable in various fields [10, 11] are intelligence agencies, law enforcement, military organizations, multimedia applications, broadcasting industries, automatic monitoring of radio advertisements, and protection of intellectual property.

The major work reviewed in this paper are related to various steganographic techniques involved in spatial and transform domain for hiding the secret data into cover image efficiently. Also presents the different algorithm implemented in embedding and extraction process used to enhance the imperceptibility and embedding capacity.

2. STEGANOGRAPHY TECHNIQUES:

2.1 Spatial domain

Spatial domain techniques, are manipulating the pixels or bits of an image directly, for the purpose of enhancing the image quality. The image quality will be enhancing by this technique. Spatial domain is used to enclose the secret data into the cover image directly. This technique consumes less execution time with high embedding rate. Figure-2 represents the different methods used in spatial domain.

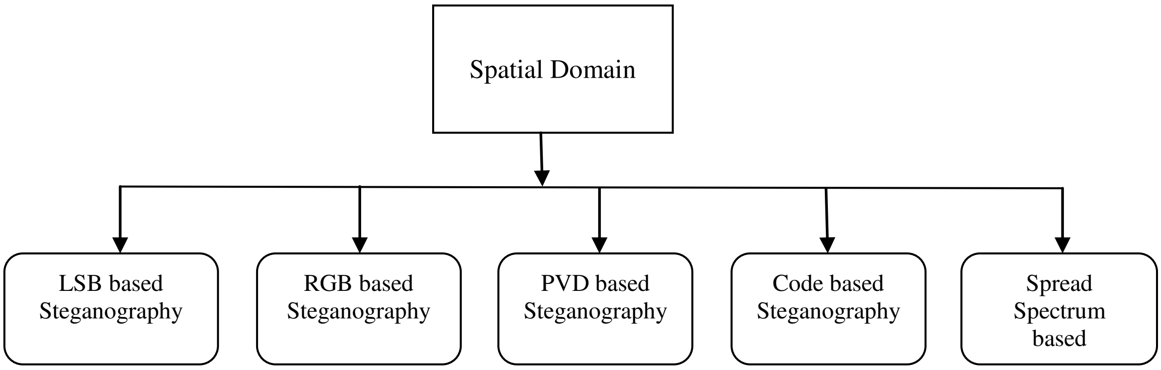

Figure-2. Different methods of spatial domain.

2.1.1 LSB based Steganography

The Least Significant Bit (LSB) of each pixel value of an image is adjusted to hide the secret information by using the LSB technique [12]. LSB technique is widely used because for better hiding capability, good adaptability and easy to implement [13].

The author explains the LSB technique using binary addition [14]. The target bits are indirectly embedded into the cover image, without adjusting the intensity value of the pixel. The data cannot be extracted directly from the unknown person by just using the standard LSB technique. The number of LSB layers presents in the binary addition should be known for extraction. Imperceptibility meets when maximum number of changes in intensity value is independent with the number of layers performing in the binary addition. Robustness achieved by performing binary addition in the extraction side. It also meets the capacity, by using more target bits at a time. All three challenges in the steganography is achieved by this the binary addition.

This paper implements, the combination of LSB substitution method to maintain the higher payload capacity and pixel value differencing (PVD) used in a block to provide high undelectibity [15]. The LSB technique involves embedding the k-bits of secret data into the upper-left position of 2X2 pixel block of an image. The pixel value is generated newly. By considering the new values, the stego image is formed. Three pixel differences of upper-right, bottom-left, bottom-right in a block is calculated. The high PSNR (peak signal to noise ratio) and high capacity can be achieved by using the variant-1 (Type 1) and variant-2 (Type 2) techniques.

This paper proposes the genetic algorithm in LSB substitution [16]. The steganography and cryptography technique provides better protection. Genetic algorithm involves for pixel assortment. This algorithm is used to choose the best possible pixels for embedding the data into the cover image.

The proposed work is done by using Hybrid Fuzzy neural networks [17] to achieve the better embedding capacity in the cover image. It proposes the random selection of pixels for embedding the secret data and also post-processing the stego image. Pseudo random key concept involves the random selection of pixels. It provides an efficient pixel adjustment and attains good stego image quality with high imperceptibility. This paper describes the spatial LSB steganography technique in the payload location [18]. This involves in restoring the original cover image and also computing the probability of successful recovery of secret data. While obtaining the original cover image, the payload carrying Pixels should accurately locate the lower and upper bound of the image.

This paper deals with the one-third probability embedding capacity [19]. One bit of information stored in each and every pixel of an image. The algorithm reduces the changing probability in each pixel to one-third and attaining the better embedding capacity. The stego image will be same as cover image. The changes may not be visible from the recovering section. The histogram compensating version is achieved. This method implements the LSB steganography in color images as well as gray scale images [20]. The size of the color image and gray scale image are 24-bit and 8-bit. It is very reliable and accurate method in LSB embedding approach.

2.1.2 RGB based Steganography

This proposed work relates to RGB Pixel Pattern based Steganography on Images [21]. So far in the existing methods, when altering the LSB or MSB bits for hiding the data, results in Dull image or noisy one. This dull image creates suspicious in the cover image to the eaves droppers at the receiver end. To avoid this, Pixel Pattern RGB based steganography technique is introduced. Here only possible value of Red, Green, and Blue (RGB) pixel can be aligned or some minimum changes can be done for embedding the image. When the data is large, the changes in the color image cannot be noticeable easily with the human visual system (HVS). The quality of the picture is good in the color images. This method can increase the protection by encrypting stego image and also the key used to decrypt the payload stored at pixel level.

This paper implements [22] the combination of Matrix Pattern (MP) and LSB based steganographic techniques for hiding the cover image. Both techniques differ with each other. In MP pattern, the cover image will be split into *B* x *B* blocks. The MP Pattern accomplishes different matrix pattern in each character of every block. The hidden data can be either Text or Binary Message. This method yields faster, efficient and produces a better visual quality stego image.

2.1.3 Pixel Value Differencing (PVD) based Steganography

PVD is an efficient technique to embed the secret data into the two consecutive pixels of the non-overlapping blocks of cover image. Random mechanism used in secrecy protection. Moreover the imperceptible result can be achieved easily than simple LSB method [23].This paper proposes [24] to enhance the security in original PVD by generating a pseudo-random dithering to various ranges of pixel-value differences. It avoids the abnormal changes presents in the histogram analysis, which saves to the large payload capacity and imperceptibility of the real PVD. This paper implements an improved steganographic technique to secure the PVD histogram with modulus function [25]. This method is used to avoid the abnormal raises and fluctuation occurring in PVD histogram. Turnover policy and novel adjusting process involved to eliminate the weaknesses of the PVD steganographic algorithm. The merits are high embedding capacity and achieve imperceptibility. A new data hiding scheme is proposed to use the varieties of PVD in multimedia images [26]. This method processed four value blocks simultaneously to extend the PVD approach. The edge area is used efficiently to enhance the embedding capacity by implementing this scheme. Because of this, more secret information can be embedded into edge areas. This provides better way of embedding.

The author implements the tri-way PVD (TPVD) to achieve the high payload capacity [27]. The TPVD suggests for compressing the secret image by JPEG2000 and embeds into the cover image. Residual value coding is proposed to decrease the distortion noise presents in the recovered image. This method provides image quality while recovering and maintains secrecy in dual statistics steganalysis. This work proposes [28] the combination of PVD and approach LSB to eliminate the lower capacity and larger distortion provided by PVD approach. It affords efficient way of data embedding in spatial domain.

This paper [29] proposes the steganography method in PVD using artificial neural networks (ANN). It achieves average accuracy 88.3% by implementing an estimator using a neural network. Estimator handled to measure the average amount of data gets embedding into an image.

2.1.4 Code based Steganography

2.1.4.1 Bose, Chaudhuri, and Hocquenghem codes

The main objective of the Steganographic algorithm is to protect the statistical properties of the cover image [30]. While manipulating the cover image two possible cases exist. In first case (Classical), only minor changes are possible in cover source whereas in second case, the unnoticeable section of the cover source can be modified. Binary Bose, Chaudhuri, and Hocquenghem (BCH) codes are better for both the above cases. In first case, by proper selection of accurate positions, modification iteration is reduced to the maximum extent and any position of the cover image can be considered. In second case, few positions cannot be altered. The sender only knows the locked positions presents in the cover image to maximize the security [31]. This paper explains the improved data hiding technique [32] related to BCH (n, k, t) where (n, k, t) mention to code length (n), dimension (k), error correction capability (t). This scheme hides the data into the input block (n). Hiding is performed by adjusting the co-efficient of the input data. This method consumes less time, also provide less storage capacity. So BCH syndrome coding is feasible compared with the existing techniques.

This paper deals with BCH Code Selection which is used to select the accurate error correction code and Iterative decoding connecting the inner BCH to outer Quasi-Cyclic Low-Density Parity-Check (QCLDPC) to eliminate the overall performance degradation [33].The BCH code alone cannot meet the error correcting requirement in multi-level cell flash memory. So they proposed the updated version flash memory by applying concatenated coding scheme [34]. This technique avoids the performance degradation and also neglects the more complexity presents in decoder hardware design [35].

2.1.4.2 Syndrome-Trellis Codes

This paper proposes the Syndrome-Trellis Codes (STC) used to reduce the additive Distortion presents in Steganography [36]. It implements the work on non binary function for embedding operation. All the possible value of stego elements are assigned as a scalar function. The payload limited sender and distortion limited sender are considered for binary and non binary functions. The non binary function is disintegrating into binary function by replacing individual bits performed using Convolution code with a Trellis Quantizer. This method is fast, versatile and reducing an additive distortion functions.

This paper proposes the work to minimize the distortion for secure binary image steganography in texture [37]. The STC is employed to minimize the designed embedding distortion on the texture. This proposal attains the statistical security without diminishing the image standard or the embedding rate. The visual quality and statistics of the image is improved by using this code. The local structure of binary image illustrates by the complement, rotation and mirroring-invariant Local Texture Patterns (crmiLTPs) distribution.

This author [38] demonstrates the block complexity and matrix embedding for an adaptive steganography. Matrix embedding is known as syndrome coding. This scheme uses linear codes to minimize the modification amount of data embedding. It provides a moderate hiding capacity with lower distortion and high security.

2.1.5 Spread spectrum based Steganography

This paper [39] deals with the Spread Spectrum Image Steganography (SSIS). The main advantage is hiding and recovering the wide range of data without affecting the actual image size. It strengthens the payload and invisibility. The symmetric key should be known by the sender and receiver while retrieving the cover image. The various filters used in the image restoration section are Mean (or) Median filter. This paper [40] proposes Chaos based Spread Spectrum Image Steganography (CSSIS). The merits of chaotic system are easy to implement in analog and digital circuits, low power, inexpensive and also provides flexibility. Chaotic-shift keying principle is used in the modulation. The median filter is used for image restoration for better performance Hamming code is used for error-correction.

2.2 Transform domain

Transform Domain is another important technique used in image enhancement. The processing takes place in the frequency or time domain [41].

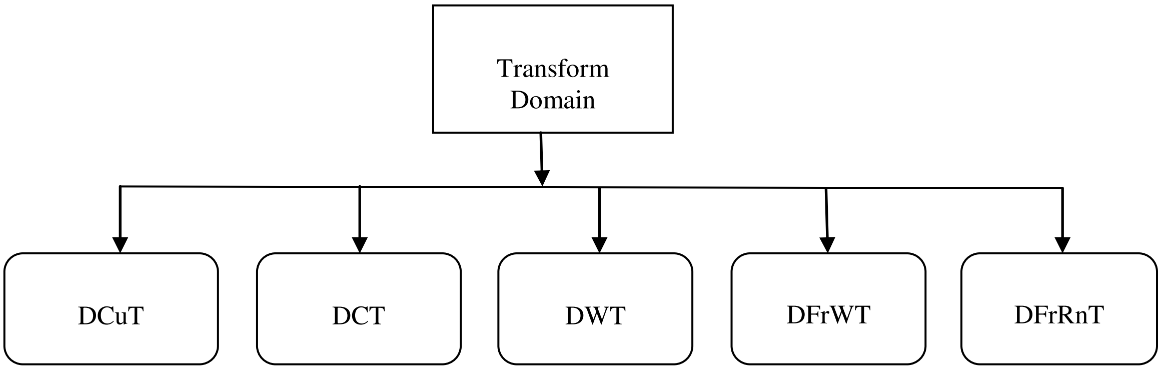

Figure-3. Various techniques of Transform Domain.

By using this domain, the given original image is transferred into frequency domain [42]. Figure 3 represents the various techniques of transform domain: Discrete Curvelet Transform (DCuT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fractional Wavelet Transform (DFrWT), Discrete Fractional Random Transform (DFrRnT). These techniques presents a very efficient way for hiding the information due to its high embedding rate, less time consuming in extraction and achieves better security protection.

2.2.1 Discrete curvelet transform

This paper deals with the DCuT [43] for secure communication. While sending the secret data through the medium, the data should be safe for diagnosing the medical abnormalities. Here the patient's information gets hidden into their Electro Cardio Gram (ECG) signals. The signal contains low, intermediate and high frequency components. The cover image is converted into the frequency sub-bands of ECG signals. This transform is good for safe transferring of patient's secret information. But when transmitting a large amount of data, the overall performance will be reduced.

2.2.2 Discrete cosine transform

This work describes the eigenvalue steganography in quantized DCT matrices [44]. Confidential data gets hidden into subdivision of quantized DCT coefficient blocks instead of LSB of DCT coefficient. This paper describes a Global-Adaptive region (GAR) with New DCT approach [45]. Normally the spatial and frequency domain techniques have low embedding capacity, whereas transform domain have high embedding capacity. The GAR is technique used to implement high embedding capacity in color image Steganography and also upgrading the image perceptibility. The new DCT uses the high frequency coefficient for hiding the cover image because of the good energy compaction property in 2D-DCT.

This paper deals with a technique to estimate the Steganographic capacity used in DCT Domain based Maximum Capacity under Undetectable (MCUU) Model [46]. This technique is proposed, beneficial to enhance the embedding capacity in cover image. Steganographic analyzer architecture and an algorithm are implemented to improve the capacity. The analyzer architecture are designed by considering the factors like image size, steganography operator, loading band, embedding intensity and image complexity that affects the embedding capacity. Quantization index modulation (QIS) is used, which yields two times better than MCUU model used in Spread Spectrum (SS).

2.2.3 Discrete wavelet transform

The author implements the reversible data embedding using wavelet techniques [47]. For improving the performance and also for achieving high embedding capacity, two important techniques are involved. That is, wavelet lifting scheme with LSB prediction and techniques of different expansion. It embeds the huge quantity of data without losing the image and its quality. This technique is used in medical and military applications.

This paper reveals to protect the patient' secret information by applying Wavelet technique in ECG based Steganography [48]. In this technique, the normal Psychological factors like blood pressure, sugar, temperature are embedded into the ECG signal and transmit confidentially by using DWT. The Percentage Residual Difference (PDR) and the wavelet weighted PDR schemes are utilized to calculate the effectiveness of the proposed technique. The patient's confidential data's are transmitted with very low distortion compared with the existing techniques.

2.2.4 Discrete fractional wavelet transform

The author [49] uses the DFrWT and chaotic map techniques for multiple image encryption method. Image transmission and encryption scheme involves in secure communication of multiple images. This paper deals with DFrWT, applied in medical image fusion [50]. This technique provides the actual information about the image and diagnosis accurately.

This paper [51] proposes the Fractional Wavelet transform (FRWT) for the image encryption process in steganography system. Encrypt the images by using two fractional keys. Optical image encryption realized with the multifractional and multiwavelet transforms. This Author [52] presents the multi resolution analysis and orthogonal wavelet using FRWT technique. It is applicable for sampling in wavelet domain and estimating time delay in chirp signals.

2.2.5 Discrete fractional random transform

FrRnT [53] mainly used for image encryption and decryption process. It is an efficient tool used in signal processing and image manipulation. The merits are high precision, high computational speed and low complexity.This paper proposes the image encryption using multiple-parameter DFrRnT [54]. This is the combination of FrRnT and Multi-parameter fractional FT. The plain text and cipher text uses spatial domain, whereas the keys used for encryption in fractional domain. It provides security, robustness and noise immunity.

This author proposes the double image encryption based on DFrRnT and chaotic map [55]. This algorithm does not use phase key and matrix key for encryption. The efficient way of encryption, storage and transmission takes place. This paper [56] deals with discrete chirikov standard transform in double optical image encryption scheme (DCST) and chaos-based DFrRnT (CBDFrRnT). Optical image encryption methods have high speed, parallel processing and extreme storage memories. This method provides good protection from Bruce-Force attacks, Plain-Text attacks and chosen plain text attacks because of its high sensitivity and better tolerance in noise level.

The author demonstrates the double image encryption based on DFrRnT and logistic map [57]. They provide asymmetric encryption technique and high resistance from conventional attacks. This paper [58] proposes the Pulse Coupled Neural Network (PCNN) mainly provides the fusion parameter details in images and the discrete multi-parameter fractional random transform (DMPFRnT) spectrum domain used for random distribution. The PCNN and DMPFRnT techniques are implements to achieve the high spatial resolution and low spectral distortion in remote sensing image fusion. This method provides good performance and provides protection for spectral information.

This paper explains double image encryption key with the combination of compressive sensing and DFrRnT [59]. Compressive sensing established from two-dimensional sine logistic modulation map. This scheme achieves compression and encryption together. Scrambling and pixel changing accomplishes by the Arnold transform and DFrRnT. This proposes the adaptive pulse coupled neural network (APCNN) and DFrRnT techniques, involves for image fusion in medical field [60]. This satisfies the high spatial resolution and low spectral distortion. This work utilizes the Hybrid Dual Tree Complex Wavelet Transforms (DT-CWT) and support vector machine (SVM) for image fusion [61]. This approach achieves low PSNR and maintains image quality without loss.

3. IMPLEMENTATION OF EMBEDDING AND EXTRACTION PROCESS

3.1 Embedding process

Let ‘C’ denotes the cover medium i.e. image *A* and *C′* stego image obtained by data embedding. Let ‘*K*’ represents an optional key and ‘*M*’ is the message. E_m suggests the embedding process and E_x is for the process of extraction [62]. Data embedding process can be represented as follows:

$$E_m : C \oplus K \oplus M \rightarrow C^{'} \quad \text{(A.1)}$$

$$E_X(E_m(c,k,m)) \approx m, \\ \forall c \in C, k \in K, m \in M. \quad \text{(A.2)}$$

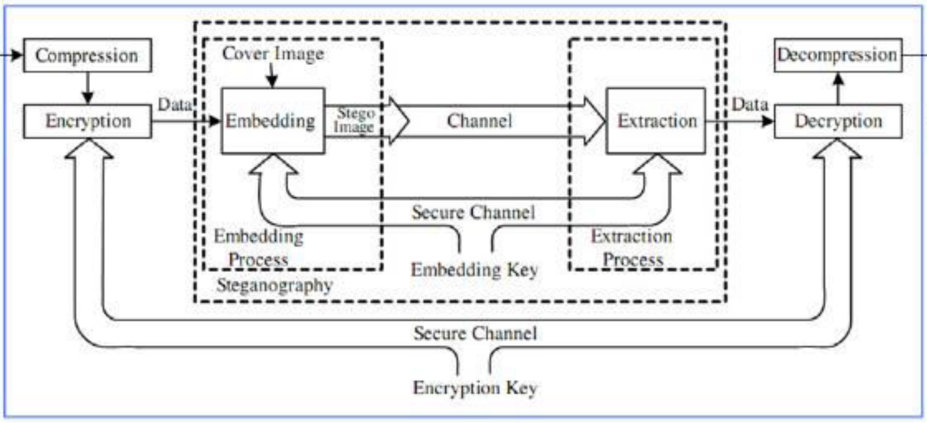

Figure-4. Block diagram of Steganography [63].

Figure-4 represents the block diagram of Steganography. Encryption technique, converts the plain image into cipher image, whereas decryption converts cipher image into cover image. The secret key is implemented for both the encryption and decryption technique. The encrypted secret image is embedding into the cover image. Thus the stego image is generated from the embedding process. This image transmits over the secure channel. In the extraction side, the recovering of an original image from the cover image takes place. The key provides security for the embedding and extraction process for the secure communication.

This paper implements the protection of the person's biometric signatures, and an author proposes the orthogonal code and joint transform correlation techniques [64] for a secured way. Three level of processing occurs in the encryption section i.e. orthogonal coding, random bit replacement and non linear encryption. Orthogonal code is used to encode the different biometric signatures and also achieves the robustness. The individual bit is selected from the R, G, and B color to hide the information into the color cover image. The Multiple Phase Shifted Reference Joint Transform (MRJTC) is a non-linear encryption technique is used to enhance the security level.

This work describes the improved performance and analysis of the high capacity of color image using Wavelet fusion Technique [65]. High Capacity and security steganography using DWT (HCSSD) encoder and decoder techniques are used for forming the stego image and payload image. The result has been verified by the following measurements. The author [66] implements the combination of Absolute moment block truncation coding compression (AMBTC compression) and interpolation technique (ASAI) to enhance the capacity and provide better image quality. The merits are reducing complexity in embedding and extraction process, reliability, high security, high embedding capacity and minimize the distortion to retrieve the clear cover image.

It deals [67] with the Adaptive neural networks (ANN) and modified particle swarm modification (MPSO). ANN-MPSO implements to adjust the pixel values by using second order differential equations (SODE). MPSO required to identify the new positions and also to modify the weighting factor (W) of the ANN. Image segmentation algorithm is used to hide the information randomly whereas existing methods do sequentially. The advantages are better picture quality, enhancing the hiding capability with five layers of protection, faster, less number of iteration.

This paper introduces three phase intelligent scheme [68]. The first, second and third phases are adaptive genetic algorithm using upwind adaptive relaxation $(LS_{ANN\ AGAUpAR1}),\ LS_{ANN\ AGAUpAR2},\ LS_{ANN\ AGAUpAR3}$ respectively. It achieves the maximum embedding rate of 12bpp (bits per pixel). This hiding algorithm results in the better protection from the various kinds of attacks such as visual, structural and at statistical attacks. It also provides seven layer of protection for the hidden image. Adaptive image filtering and new image segmentation algorithm are used for image compression and encryption.

This work proposes fuzzy logic based LSB algorithm [69] and similarity based LSB algorithm, used to send the patient's medical data's. The cover image contains the patient's EEG, ECG signal, health information, medical resonance imaging (MRI), and doctor comments. These all information's are combined together and transmitted as a single image. The performance and transmission capacity, the Mean square of error (MS), PSNR, Universal quality index (UQI), Structural similarity measure (SSIM) and Correlation co-efficient are evaluated.

In this, a novel image Steganography algorithm is implemented [70] based on the edge detection and XOR coding for hiding the information. The domain can be either spatial domain or integer wavelet transform. This method concentrates from sharpest regions to less sharp regions in the non overlapping blocks for concealing the cover image. The performance of algorithm is measured from the following three analyses i.e. embedding efficiency, embedding payload and security. The merits are better imperceptibility and good level of security.

The author employs the Adaptive circular queue steganography with RSA (Rivest-Shamir-Adleman) cryptography algorithm [71]. The secret Cipher text will be embedded into the LSBs of cover image by using circular queue substitution technique. RSA algorithm is also known as asymmetric algorithm, which provides confidentiality, integrity, non-reputability and authenticity. The results were obtained from the MSE, PSNR and maximum embedding capacity.

The techniques suggested in this paper [72] are redundant discrete wavelet transform [RDWT] and quick response [QR] factorization. This algorithm achieves better computational quality, good hiding capacity and security compared with the previous Singular Value Decomposition (SVD) technique. Proposed algorithm uses the wavelet based and contourlet based steganalysis schemes resulting in low error rate, robustness, accuracy.

This work [73] deals with Steganography Pattern Discovery (SPD) method used for stegnalysis. The main objective is to get the stego image from the original image. Each stego images have an exclusive pattern or signature, generated by the steganography method used for embedding. Filtering and wrapper method helps for image feature selection. The certain fuzzy rules formed by the evolutionary fuzzy algorithm to recognize the pattern adopted. It achieves better detection with high accuracy.

The author proposes QR code Fresnelet transform in frequency domain [74]. The important two aspects are high stego image quality and high embedding capacity. This transform hides the QR coded secret data in Fresnelet co-efficient of LSB. The obtained stego image quality retains the average PSNR value of 45.40db and the embedding capacity is 352,332 bits.

This paper implements the hybrid edge detector for high payload Steganography method [75] in gray scale images. Hybrid edge detector is used for the selection of possible edges in the color image to embed the maximum number of bits. Hybrid edge detector is the combination of the existing edge detection detectors like Canny, Fuzzy, Sobel and Laplacian edge detector. This work, [76] describes a Steganography algorithm developed by merging the edge detection and high payload capacity techniques for color image. It provides high payload capacity by adding one bit in each RGB color comparing with the existing technique.

This research includes the interval-valued intuitionistic fuzzy edge detection (IVIF) technique to utilize the edge areas efficiently and modified LSB substitution scheme is used to enhance the quality of image and also improve the payload capacity [77]. IVIF edge detector differentiates the edge as well as smooth areas. The extraction takes place in edge areas without any distortion. The secret message embedded into the pixel by using Modified LSB substitution method. This approach provides balancing between the embedding capacity and stego image quality and also attain high PSNR rate.

This author [78] used the multilayer embedding approach for high capacity reversible steganography (CRS). This method helps to retrieve the clear original image, after the secret image extraction. CRS provides low computational complexity, low distortion, attains high performance, and gain high PSNR value. The payload capacity and PSNR value is 1.79 bpp and 33.85db respectively.

This paper proposes the high performance JPEG steganography based complementary embedding strategy [79]. This technique mainly involves safeguarding the JPEG cover image from the various kinds of statistical attacks such as Chi-Square and extended chi-square, S-family attack. This method mainly used for covert communication. It provides better performance and capacity than the J-Steg, F5 and Outguess algorithms.

This paper deals with the large payload matrix embedding method (ME) to upgrade the embedding efficiency [80]. Parity Check Matrix (PCM) in binary linear code method involves embedding the data. PCM is a matrix exclusively designed for better embedding performance. The advantages are low complexity, increases payload and embedding efficiency. This author introduces the Pseudo noise (PN) sequence masking, employed for secure Spread Spectrum (SS) Steganography [81]. This masking is used to enhance the security, restrict improper data extraction, avoids additional distortion occurring in the carrier signal, improve carrier performance. The carrier optimization algorithm is also incorporated for increasing the output Signal-to-Interference-plus-Noise Ratio (SINR) and reducing BER. The paper proposed the genetic algorithm in spatial domain image steganography. This approach is mainly used to increase the embedding capacity and prevent the visual image quality [82].This scheme is simple, feasible for the various Steganographic applications.

3.2 Comparison of reversible data hiding techniques

Reversible (lossless or distortion free or invertible) data hiding techniques involves recovering an original cover image without distortion [83]. The main purpose of extraction is embedding the information without any loss [84]. It provides high payload capacity and achieves better PSNR value. It's mainly used in military, legal, and texture images, aerial images and medical imaging. Table-1 represents the comparison of payload capacity versus PSNR value.

Table-1. Comparison of payload capacity and PSNR.

Reversible data hiding techniques	**Payload capacity**	**PSNR value** (dB)
Hao Luo, Fa-Xin [85]	0.66bpp-0.7bpp (13432 bits)	50 to 32 dB
Kyung-Su Kima [86]	0.5-3 bpp (6k to 210k)	50 to 30.27 dB
Piyu Tsai [87]	42,322bits	49.59dB
Chin-Chen Chang [88]	1.21bpp	>52 dB
Chia-Chen [89]	1.3 bpp	30 dB
Fei Peng [90]	2.17 bpp	20.71 dB
Chin-Feng Lee [91]	2.28 bpp.	20.96dB

CONCLUSIONS

The paper deals with various types of spatial and transform domain steganographic techniques has been discussed. The most important criteria of steganographic techniques are the embedding capacity, imperceptibility and robustness. Imperceptibility meets high, when the discrepancy between the stego image and cover image maintains very small. The embedding capacity achieves by hiding large amount of embedded secret data into the cover image. Robustness obtains the rescue of the secret information over the transmission. The different algorithms are dealt to implement the embedding and extraction process in order to achieve the payload capacity, high image quality, security and high PSNR value. Steganography is the upgrading technique in research field and further improvement can be promoted by the various algorithms to achieve more capacity, security and robustness in bio-medical image processing.

REFERENCES

[1] Al-Dmour Hayat, Ahmed Al-Ani. 2016. Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Computer methods and programs in biomedicine. 127: 24-43.

[2] Cheng Yu-Ming, Chung-Ming Wang. 2009. A Novel Approach to Steganography in High-Dynamic-Range Images. IEEE Multi Media. 16.3: 70-80.

[3] Shie Shih-Chieh, Shinfeng D. 2009. Lin. Data hiding based on compressed VQ indices of images. Computer Standards & Interfaces. 31.6: 1143-1149.

[4] Jain Rupali, Jayshree Boaddh. 2016. Advances in digital image steganography. Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on IEEE. 2016: 163-171.

[5] Lee Chin-Feng, Chin-Chen Chang et al. 2008. An improvement of EMD embedding method for large payloads by pixel segmentation strategy. Image and Vision Computing. 26.12: 1670-1676.

[6] Johnson Neil F, Sushil Jajodia. 1998. Exploring steganography: Seeing the unseen. Computer 31.2: 26-34.

[7] Morkel Tayana, Jan HP Eloff, Martin S. Olivier.2005. An overview of image steganography ISSA. 2005: 01-12.

[8] Jain Ruchi. 2014. An Extensive Survey on Image Steganography. International Journal of Emerging Technology and Advanced Engineering. 4.3: 674-679.

[9] Lin Iuon-Chang, Yang-Bin Linet et al. 2009. Hiding data in spatial domain images with distortion tolerance. Computer Standards & Interfaces. 31.2: 458-464.

[10] Anderson Ross J, Fabien AP Petitcolas. 1998. On the limits of steganography. IEEE Journal on selected areas in communications. 16.4: 474-481.

[11] Katzenbeisser Stefan, Fabien Petitcolas.2000. Information hiding techniques for steganography and digital watermarking. Artech house. 2000: 01-237.

[12] Corser George. 2013. Entropy as an Estimate of Image Steganography. Oakland University Rochester USA. 2013: 01-04.

[13] Luo Xiangyang, Fenlin Liu, Peizhong Lu. 2007. A LSB steganography approach against pixels sample pairs steganalysis. International Journal of Innovative Computing, Information and Control. 3.3: 575-588.

[14] Datta Biswajita, Upasana Mukherjee et al. 2016. LSB Layer Independent Robust Steganography using Binary Addition. Procedia Computer Science. 85: 425-432.

[15] Swain Gandharba. 2016. A Steganographic Method Combining LSB Substitution and PVD in a Block. Procedia Computer Science. 85: 39-44.

[16] Sethi Pratiksha, V. Kapoor. 2016. A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. Procedia Computer Science. 87: 61-66.

[17] Saleema A, T. Amarunnishad. 2016. A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks. Procedia Technology. 24: 1566-1574.

[18] Liu Jiu-fen et al. 2015. LSB steganographic payload location for JPEG-decompressed images. Digital Signal Processing. 38: 66-76.

[19] Sarreshtedari Saeed, Mohammad Ali Akhaee. 2014. One-third probability embedding: a new±1 histogram compensating image least significant bit steganography scheme. IET image processing. 8.2: 78-89.

[20] Fridrich Jessica, Miroslav Goljan et al. 2001. Reliable detection of LSB steganography in color and grayscale images. Proceedings of the 2001 workshop on Multimedia and security: new challenges. ACM. 2001: 27-30.

[21] Rejani R, D. Murugan, Deepu V. Krishnan. 2025. Pixel Pattern Based Steganography on Images. ICTACT Journal on Image and Video Processing. 5.3: 991-997.

[22] Nilizadeh Amirfarhad, Ahmad Reza Naghsh Nilchi. 2016. A novel steganography method based on matrix pattern and LSB algorithms in RGB images. 1st Conference on Swarm Intelligence and Evolutionary Computation (CSIEC) IEEE. 2016: 154-159.

[23] Wu Da-Chun, Wen-Hsiang Tsai. 2003. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters. 24.9: 1613-1626.

[24] Zhang Xinpeng, Shuozhong Wang. 2004. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters. 25.3: 331-339.

[25] Joo Jeong-Chun, Hae-Yeoun Lee et al. 2010. Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP Journal on Advances in Signal Processing. 26.

[26] Cheng-Hsing Yang, Chi-Yao Weng, Hao-Kuan Tso et al. 2011. A data hiding scheme using the varieties of pixel-value differencing in multimedia images. Journal of Systems and Software. 84.4: 669-678.

[27] Yen-Po Lee, Jen-Chun Lee, Wei-Kuei Chen et al. 2012. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences. 191: 214-225.

[28] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang et al. 2010. Varied PVD+ LSB evading detection programs to spatial domain in data embedding systems. Journal of Systems and Software. 83.10: 1635-1643.

[29] Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavia et al. 2010. Steganalysis and payload estimation of embedding in pixel differences using neural networks. Pattern Recognition. 43.1: 405-415.

[30] Schönfeld Dagmar, Antje Winkler. 2006. Embedding with syndrome coding based on BCH codes. Proceedings of the 8th workshop on Multimedia and security. ACM. 2006: 214-223.

[31] Jessica Fridrich, Miroslav Goljan, Petr Lisonek et al. 2005. Writing on wet paper. IEEE Transactions on Signal Processing. 53.10: 3923-3935.

[32] Rongyue Zhang, Vasiliy Sachnev, Magnus Bakke Botnan et al. 2012. An efficient embedder for BCH coding for steganography. IEEE Transactions on Information Theory. 58.12: 7272-7279.

[33] Pin-Han Chen, Jian-Jia Weng, Chung-Hsuan Wang et al. 2013. BCH code selection and iterative decoding for BCH and LDPC concatenated coding system. IEEE Communications Letters. 17.5: 980-983.

[34] Dai, Yongmei, Ning Chen, Zhiyuan Yan. 2008. Memory efficient decoder architectures for quasi-cyclic LDPC codes. IEEE Transactions on Circuits and Systems. 55.9: 2898-2911.

[35] Zongwang Li, Lei Chen, Lingqi Zeng et al. 2006. Efficient encoding of quasi-cyclic low-density parity-check codes. IEEE Transactions on Communications. 54.1: 71-81.

[36] Filler, Tomas, Jan Judas et al. 2011. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security. 6.3: 920-935.

[37] Feng, Bingwen, Wei Lu, et al. 2015. Secure binary image steganography based on minimizing the distortion on the texture. IEEE transactions on Information Forensics and Security. 10.2: 243-255.

[38] Guangjie Liu, Weiwei Liu, Yuewei Dai et al. 2014. Adaptive steganography based on block complexity and matrix embedding. Multimedia systems. 20.2: 227-238.

[39] Marvel Lisa M, Charles G. Boncelet et al. 1999. Spread spectrum image steganography. IEEE Transactions on image processing. 8.8: 1075-1083.

[40] K. Satish, T. Jayakar, Charles Tobin et al. 2004. Chaos based spread spectrum image steganography. IEEE transactions on consumer Electronics. 50.2: 587-590.

[41] Mundhada Snehal O, V. K. Shandilya. 2012. Spatial and transformation domain techniques for image enhancement. International Journal of Engineering Science and Innovative Technology (IJESIT). 1.2: 213-216.

[42] Morkel Tayana, Jan HP Eloff et al. 2005. An overview of image steganography ISSA. 2005: 1255-1260.

[43] Jero S. Edward, P. Ramu. 2016. Curvelets-based ECG steganography for data security. Electronics Letters. 52.4: 283-285.

[44] Behbahani Yasser M, Parham Ghayour et al. 2011. Eigenvalue Steganography based on eigen characteristics of quantized DCT matrices. Information Technology and Multimedia (ICIM). 01-04.

[45] Rabie Tamer, Ibrahim Kamel. 2016. High-capacity steganography: A global-adaptive-region discrete cosine transforms approach. Multimedia Tools and Applications. 2016: 1-21.

[46] MAO Jiafa, HUANG Yanhong, NIU Xinxin et al. 2016. A method to estimate the steganographic capacity in DCT domain based on MCUU model. Wuhan University Journal of Natural Sciences. 21.4: 283-290.

[47] Kamstra Lute, Henk JAM Heijma ns. 2005. Reversible data embedding into images using wavelet techniques and sorting. IEEE transactions on image processing. 14.12: 2082-2090.

[48] Ibaida Ayman, Abrahim Khalil. 2013. Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE

Transactions on Biomedical Engineering. 60.12: 3322-3330.

[49] Bhatnagar Gaurav, QM Jonathan Wu et al. 2013. Discrete fractional wavelet transform and its application to multiple encryptions. Information Sciences. 223: 297-316.

[50] Xu Xiaojun, Youren Wang et al. 2016. Medical image fusion using discrete fractional wavelet transform. Biomedical Signal Processing and Control. 27: 103-111.

[51] Chen Linfei, Daomu Zhao. 2005. Optical image encryption based on fractional wavelet transforms. Optics Communications. 254.4: 361-367.

[52] Shi Jun, Xiaoping Liu et al. 2015. Multi resolution analysis and orthogonal wavelets associated with fractional wavelet transform. Signal, Image and Video Processing. 9.1: 211-220.

[53] Liu Zhengjun, Haifa Zhao et al. 2005. A discrete fractional random transform. Optics communications. 255.4: 357-365.

[54] Zhou Nanrun, Taiji Dong et al. 2010. Novel image encryption algorithm based on multiple-parameter discrete fractional random transform. Optics Communications. 283.15: 3037-3042.

[55] Li Huijuan, Yurong Wang. 2011. Double-image encryption based on discrete fractional random transform and chaotic maps. Optics and Lasers in Engineering. 49.7: 753-757.

[56] Zhang Yushu, Di Xiao. 2013. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. Optics and Lasers in Engineering. 51.4: 472-480.

[57] Liansheng Sui, HaiweiLu, ZhanminWang et al. 2014. Double-image encryption using discrete fractional random transform and logistic maps. Optics and Lasers in Engineering. 56: 1-12.

[58] Lang Jun, Zhengchao Hao. 2014. Novel image fusion method based on adaptive pulse coupled neural network and discrete multi-parameter fractional random transform. Optics and Lasers in Engineering. 52: 91-98.

[59] Nanrun Zhou, JianpingYang, ChangfaTan et al. 2015. Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform. Optics Communications j. 354: 112-121.

[60] Lang Jun, Zhengchao Hao. 2015. Image fusion method based on adaptive pulse coupled neural network in the discrete fractional random transform domain. Optik-International Journal for Light and Electron Optics. 126.23: 3644-3651.

[61] Biting Yu, BoJia, LuDing et al. 2016. Hybrid dual-tree complex wavelet transform and support vector machine for digital multi-focus image fusion. Neurocomputing. 182: 1-9.

[62] Abbas Cheddad, JoanCondell, KevinCurran et al. 2010. Digital image steganography: Survey and analysis of current methods. Signal processing. 90.3: 727-752.

[63] Subhedar, Mansi S, Vijay H. Mankar. 2014. Current status and key issues in image steganography: A survey. Computer science review. 13: 95-113.

[64] Islam, M. Nazrul, Muhammad Faysal Islam et al. 2015. Robust information security system using steganography, orthogonal code and joint transform correlation. Optik-International Journal for Light and Electron Optics. 126.23: 4026-4031.

[65] Sidhik, Siraj, S. K. Sudheer et al. 2015. Performance and analysis of high capacity Steganography of color images involving Wavelet Transform. Optik-International Journal for Light and Electron Optics. 126.23: 3755-3760.

[66] Mingwei Tang, Shenke Zeng, Xiaoliang Chen et al. 2016. An adaptive image steganography using AMBTC compression and Interpolation Technique. Optik-International Journal for Light and Electron Optics. 127.1: 471-477.

[67] El-Emam, Nameer N. 2015. New data-hiding algorithm based on adaptive neural networks with modified particle swarm optimization. Computers & Security. 55: 21-45.

[68] El-Emam, Nameer N, Mofleh Al-Diabat. 2015. A novel algorithm for colour image steganography using a new intelligent technique based on three phases. Applied Soft Computing. 37: 830-846.

[69] R. Karakıs, I. Güler, İ. Çapraz et al. 2015. A novel fuzzy logic-based image steganography method to

ensure medical data security. Computers in biology and medicine. 67: 172-183.

[70] Al-Dmour, Hayat, Ahmed Al-Ani. 2016. A steganography embedding method based on edge identification and XOR coding. Expert systems with Applications. 306.46: 293

[71] Jain, Mamta, Saroj Kumar Lenka et al. 2016. Adaptive circular queue image steganography with RSA cryptosystem. Perspectives in Science. 2016: 01-04.

[72] Subhedar Mansi S, Vijay H. Mankar. 2016. Image steganography using redundant discrete wavelet transform and QR factorization. Computers & Electrical Engineering. 2016: 01-17.

[73] Sajedi Hedieh. 2016. Steganalysis based on steganography pattern discovery. Journal of Information Security and Applications. 2016: 01-12.

[74] Maheswari S. Uma, Jude Hemanth. 2015. Frequency domain QR code based image steganography using Fresnelet transform. AEU-International Journal of Electronics and Communications. 69.2: 539-544.

[75] Chen Wen-Jan, Chin-Chen Chang. 2010. High payload steganography mechanism using hybrid edge detector. Expert Systems with applications. 37.4: 3292-3301.

[76] Ioannidou Anastasia, Spyros T. Halkidis. 2012. A novel technique for image steganography based on high payload method and edge detection. Expert systems with applications. 39.14: 11517-11524.

[77] Dadgostar H, F. Afsari. 2016. Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. Journal of Information Security and Applications. 30: 94-104.

[78] Tang Mingwei, Jie Hu, Wen Song. 2014. A high capacity image steganography using multi-layer embedding. Optik-International Journal for Light and Electron Optics. 125.15: 3972-3976.

[79] Liu Chiang-Lung, Shiang-Rong Liao. 2008. High-performance JPEG steganography using complementary embedding strategy. Pattern Recognition. 41.9: 2945-2955.

[80] Xiaolong Li, Siren Cai, Weiming Zhang et al. 2015. A further study of large payloads matrix embedding. Information Sciences Inj. 324: 257-269.

[81] Ming Li, Yanqing Guo, Bo Wang et al. 2015. Secure spread-spectrum data embedding with PN-sequence masking. Signal Processing: Image Communication. 39: 17-25.

[82] Kanan Hamidreza Rashidy, Bahram Nazeri. 2014. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications. 41.14: 6123-6130.

[83] Ni Zhicheng. 2006. Reversible data hiding. IEEE Transactions on circuits and systems for video technology. 16.3: 354-362.

[84] Celik Mehmet Utku. 2002. Reversible data hiding. Image Processing. 2002. Proceedings. 2002 International Conference on. Vol. 2. IEEE 2002: 157-160.

[85] Hao Luo, Fa-Xin Yu, Hua Chen et al. 2011. Reversible data hiding based on block median preservation. Information Sciences. 181.2: 308-328.

[86] Kyung-Su Kim, Min-JeongLee, Hae-Yeoun Lee et al. Reversible data hiding exploiting spatial correlation between sub-sampled images. Pattern Recognition. 42.11: 3083-3096.

[87] Tsai Piyu, Yu-Chen Hu, Hsiu-Lien Yeh. 2009. Reversible image hiding scheme using predictive coding and histogram shifting. Signal Processing. 89.6: 1129-1143.

[88] Chang Chin-Chen, The Duc Kieu. 2010. A reversible data hiding scheme using complementary embedding strategy. Information Sciences. 180.16: 3045-3058.

[89] Lin Chia-Chen, Wei-Liang Tai et al. 2008. Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recognition. 41.12: 3582-3591.

[90] Peng Fei, Xiaolong Li et al. 2012. Adaptive reversible data hiding scheme based on integer transform. Signal Processing. 92.1: 54-62.

[91] Lee Chin-Feng, Yu-Lin Huang. 2012. An efficient image interpolation increasing payload in reversible data hiding. Expert Systems with Applications. 39.8: 6712-6719.