Synopsis of proposed thesis entitled

Design and Implementation of Dual Image based Reversible Data Hiding Techniques

To be submitted to

VIDYASAGAR UNIVERSITY

For the Award of Degree of

DOCTOR OF PHILOSOPHY
(SCIENCE)

In

COMPUTER SCIENCE

By

BISWAPATI JANA

Under the guidance of

Prof. Debasis Giri
Department of Computer Science and Engineering
Haldia Institute of Technology
Haldia, Purba Medinipur
West Bengal-721657, INDIA

AND

Dr. Shyamal Kumar Mondal
Department of Applied Mathematics with
Oceanology and Computer Programming
Vidyasagar University
Paschim Medinipur
West Bengal-721102, INDIA

June, 2016

PUBLICATION

The list of Published Paper:

1. High payload reversible data hiding scheme using weighted matrix, (2016, March), **Optik International Journal for Light and Electron Optics**, 127(6), 3347-3358, Elsevier. **Impact Factor: 0.677**.
   Indexing: Compendex, Engineering Index, INSPEC, Science Citation Index (SCI), Scisearch, Technology and Applied Sciences, Scopus, Engineering Information Compendex, Google Scholar,

2. Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion,(2016, July), **International Journal of Network Security**, 18(4), 633-643. **Impact Factor: 1.3921**.
   Indexing: EI-Compendex, Summon by Serial Solutions, SCImago, Scopus and SciVerse, Data Base systems and Logic Programming (DBLP), EBSCO, Directory of Open Access Journals (DOAJ) and Google Scholar.

3. An Efficient Data Hiding Scheme Using Hamming Error Correcting Code, (2015, September), Published in the proceedings of the Sixth International Conference on Computer and Communication Technology, (ICCCT-2015), ACM digital library, ACM New York, NY, USA 2015, pp. 360-365.
   Indexing: ACM Digital Library, Google Scholar.

4. Dual Image Based Reversible Data Hiding Scheme Using Three Pixel Value Difference (TPVD), (2016, February), Published in the proceedings of the Third International Conference on Information System Design and Intelligent Application (INDIA 2016), Advances in Intelligent Systems and Computing, Springer, Vol. 434, pp. 403-412.
   Indexing: ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springer link.

5. Weighted Matrix Based Reversible Data Hiding Scheme Using Image Interpolation, (2015, December), Published in the proceedings of the International Conference on Computational Intelligence in Data Mining (ICCIDM-2015), Advances in Intelligent Systems and Computing, Springer India, Vol. 411, pp. 239-248.
   Indexing: ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springer link.

6. An Efficient Weight Matrix Based Reversible Data Hiding Scheme, (2015, December), Published in the proceedings of the International Conference on Computers and Management (ICCM-2015), Jaipur, Rajasthan, December 16-17, 2015.

7. Reversible Data Hiding Through Hamming Code Using Dual Image,(2015, October), Published in the proceedings of the International Congress on Information and Communication Technology (ICICT - 2015), Advances in Intelligent Systems and Computing, Vol. 439, pp. 495-504.
   Indexing: ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springer link.

8. Dual Image based Reversible Data Hiding Scheme Using Pixel Value Difference With Exploiting Modification Direction, (February, 2106), Published in the proceedings of the First International Conference on Intelligent Computing and Communication (ICIC^2), Advances in Intelligent Systems and Computing (AISC), Springer.
   Indexing: ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springer link.

The list of Communicated Papers:

9. Partial Reversible Data Hiding Scheme Using (7,4) Hamming Code, **Multimedia Tools and Application**, Springer, **Impact Factor 1.346**, (Revised version submitted).

10. Dual Image Based Reversible Data Hiding Scheme Using (7,4) Hamming Code, **Multimedia Tools and Application**, Springer, **Impact Factor 1.346**, (Revised version submitted).

ABSTRACT

Communication through data hiding is an important and demanding issues for many applications. The important parameters to measure the performance of data hiding schemes are imperceptibility, data hiding capacity and robustness which are inversely proportional to each others. So, there is a challenge to design some innovative data hiding techniques and solved while maintaining the tradeoff among these three parameters. After extraction the secret message from the stego media, the recovery of original image is also demanding issues in several human centric application areas. Many data hiding techniques are developed since last decades which have either limited embedding capacity and/or lower visual quality.

In the light of this discussion, some innovative secured data hiding schemes have been proposed to maintain a perfect balance of these important components of data hiding schemes that is payload, imperceptibility and robustness. Some new data hiding methods are designed and solved using Hamming code, Pixel Value Difference (PVD), Difference Expansion (DE), Exploiting Modification Direction (EMD) and Weighted Matrix based techniques.

In this thesis, two partial reversible data hiding schemes have been designed through error creation using Hamming code. Reversibility has been achieved using dual image but data hiding capacity is limited. To improve the embedding capacity, three new reversible data hiding techniques are designed and solved using PVD, DE and EMD methods. The maximum embedding capacity of these suggested methods is 2.15 bits per pixel (bpp) with moderate visual quality.

Again to improve the data hiding capacity while maintaining good visual quality, three more new data hiding techniques are introduced and solved using weighted matrix. In these schemes, data hiding capacity has been achieved finally at 3.46 bpp with visual quality measured by Peak Signal to Noise Ratio (PSNR) is 35.39 dB. Dual image and image interpolation techniques accelerate the data hiding capacity, visual quality and security of proposed data hiding schemes. To enhance the security of these schemes, shared secret key has been introduced. All these schemes are compared with the state-of-the-art methods and observed a considerable improvement in terms of visual quality as well as capacity. Development of some new innovative data hiding methods are not enough, but their security analysis is paramount important. So, these suggested methods are analyzed through some standard steganalysis and tested under some known steganographic attacks. We observed that all these proposed schemes are robust against several steganographic attacks.

1 Introduction

Data hiding is the art and science of data smuggling that communicates information by concealing secret message through innocuous cover media such as images, audio signals, videos, documents and so on. Various kinds of multimedia objects can be used as cover media to hide the existence of secret information from an eavesdropper, but digital images are the most commonly used media because they are ubiquitous and moreover, images speak more than words. Due to the higher degree of distortion tolerance with a larger hiding capability, digital images are being used as cover media in data hiding applications for the past few decades.

Now-a-days, data hiding provide secured and private communication that becomes the essential requirement of various types of applications. Data hiding plays an important role in multimedia security. It is useful in various purposes such as copyright protection, covert communication, content authentication, forensic tracking, tamper detection and many other human centered approaches. It consists of several branches such as Steganography, Watermarking, Secret Sharing, Visual Cryptography etc. Steganography and Watermarking are two main research areas in data hiding. These two approaches conceal secret information within cover media by changing some of its attributes, but they have still some properties distinguishable from each other. In Steganography, embed messages are hard to reveal by an adversary, but in Watermarking it may not always be true. The main intention is to concentrate on precluding the adversary from moving out the content of the confidential messages by applying a variety of distortion techniques. Some data hiding schemes proposed in this research work are classified in the category of Steganography through gray scale digital image as per their degree of redundancy. The objective of Steganography are quite different from Cryptography. The cryptographic schemes scramble secret messages so that if intercepted, messages cannot be understood but Steganography camouflages the messages to hide its existence and makes it seem almost invisible. An encrypted message may draw suspicion while an invisible message will not.

Depending on the manner of data embedding, current data hiding algorithms can be grouped into three domains: spatial, frequency and compress domains. Each domain has its own advantage and disadvantage with regard to hiding capacity, execution time and storage space. Whereas, algorithms in spatial domain embed secret messages by directly manipulating the image pixel values. However, algorithms in the frequency domain first transform the input image into frequency coefficients. Then the secret message is embedded by coefficient modifications. Algorithms in the compress domain adopt the image representation by a series of compress code as their embedding media. Data embedding is accomplished by modifying the compress code. Transform domain methods are more robust compared to spatial domain methods.

Sometimes, after extracting secret data from the cover media, recovery of cover image is essential in some applications such as remote sensing, military application, medical image sharing, multimedia archive management etc. According to whether the cover image pixels can be recovered or not after data extraction, current data hiding schemes are classified into two categories: reversible and irreversible. The scheme of reversible data hiding usually exploits the techniques of histogram shifting, prediction error, and difference expansion etc. On the other hand, irreversible data hiding schemes such as data hiding using Pixel Value Difference (PVD), Exploits Modification Direction (EMD), Weighted Matrix (WM) often have greater data hiding capacities, but the modification caused by data embedding are not invertible. In addition to this, dual image based data hiding techniques are often being used recently. During data embedding, dual image based techniques can generate two similar copies stego-image from the cover image to increase data embedding capacity and enhance security. It is hard for an adversary to extract the hidden content without simultaneous two stego-images. This concept is talked about as a particular case of secret sharing.

However, communication through data hiding usually puts stress on simply finding the presence of a secret message. Thus, the imperceptibility becomes the most significant place for the data hiding schemes. For sophisticated data hiding strategies, it has been proven in practice that one efficient style of increasing security is to reduce the number of changes that is inserted into the cover media. A high embedding efficiency becomes the principal aim to accomplish for the current data hiding schemes by substituting the payload. The goal of data hiding is to ensure embedded data extraction and original cover image reconstruction. The performance of a reversible data hiding schemes are evaluated by three aspects: embedding capacity (payload), visual quality (measured by PSNR) and computational complexity. For a desired capacity, one expects to minimize the distortion and meanwhile keep computational complexity as low as possible. To get high capacity, repeated embedding process may applied, leading to rapid decrease of visual quality and increase of computational complexity. The key factors of secured hidden data communications are high security, high embedding capacity and good imperceptibility. Each of these requirements occupies each corner of a triangle in a data hiding system and there is always a trade-off between these contradictory requirements.

Imperceptibility: The first and foremost requirement of any data hiding algorithm is the imperceptibility. The embedded secret data within cover image should not cause any degradation in visual quality. The secret message should remain invisible, it should not be detectable to the human eyes and there should not be any visual distortion within stego-image so that it remains unsusceptible and unsafe. Higher the stego-image quality, more invisible the hidden message which can be measured through PSNR. A higher PSNR value means a lower degree of distortion.

Payload: The amount of inserted information within stego-image is considered as payload. The payload should be higher as much as possible with an acceptable resultant stego quality. It is measured by some absolute value or relative measurement (bits per pixel) or data embedding rate. The importance of data hiding schemes are based on the tradeoff between payload or data hiding capacity and stego-image quality. So, a scheme does have its contribution to the field of research if it increases the payload while maintaining an acceptable quality of stego-image or improves image quality while keeping the hiding capacity at the same level or better.

Robustness: Robustness is the level of difficulty required by an eavesdropper to decide whether an image contains hidden message(s) or not. An effective data hiding scheme would be the one where an image can sustain under steganographic attack that may prove inconclusive. Statistical analysis is the practice of detecting hidden information through applying statistical tests on stego image.

Stanley [48] suggests that another important property of data hiding is speed or time complexity where information should be embedded as quickly as possible. However, it is not feasible that any data hiding algorithm should sacrifice above mentioned criteria to embed information in a timely manner.

In recent years, the demand of efficient secured high capacity data communication through data hiding is increasing. To accomplish good quality stego with high payload and robustness, is a challenging problem to the researchers. After extracting the confidential message from stego media, the demand of image reversibility without any distortion goes high. In this light, it is necessary to investigate reversible data hiding approaches which enhance security and improve embedding capacity. However, data hiding is a double-edged sword since terrorist and illegal organizations may use it to undermine social stability, endanger public safety and engage in criminal activities. Thus security analysis (steganalysis) plays an important role as counter process of data hiding. Fridrich et al. [13] suggest that the power to discover secret information in stego images is associated with the data length. This means that a short message hiding within a big size carrier will result in a little amount of distortion and hence this is practically hard to distinguish any hidden content within stego media. It is obvious that every data hiding scheme may cause undesirable artifacts in the resulted stego image which is used as a tool to detect and estimate the length of secret message through security analysis. The steganalysis falls into two broad categories: specific or targeted and universal. Specific steganalysis can reveal the secret message, but it is hard to know which data hiding methods were used to generate stego images. While the latter, also called blind steganalysis, is more attractive in practical application, because it can detect the secret message independent of the data hiding algorithms. Blind security analysis is a critical task than targeted analysis because the analyst does not know how secret message can be embedded. In this case, the analyst develop an algorithm for checking marks of tampering found within the suspected media which contains secret messages. Fridrich et al. [14] developed an authentic and exact method called Regular Singular (RS) analysis for detecting the Least Significant Bit (LSB) embedding within the image. In this thesis, some new innovative reversible data hiding techniques have been designed and implemented. Design security scheme is not enough, but their security guarantee is of paramount impermanence. If the detection of secret information within a media is made by an eavesdropper then the data hiding scheme will fail.

2 Literature Review

Brief review of some existing data hiding schemes have been described below:

2.1 Brief review of data hiding through Hamming code

Hamming [18] devised a sophisticated pattern of parity checking code that could correct single error along with the detection of double errors. Crandall [10] first pointed out that embedding efficiency could be improved by coding methods and suggested the matrix coding. Westfeld [58] introduced data hiding techniques through matrix encoding using Hamming code. Tseng et al. [56] proposed data hiding scheme by taking into consideration the quality of image after data hiding. It ensured that any bit that is modified in the host image is adjacent to another bit which has a value equal to the former's new value. Willems and Dijk [59] suggested that the embedding code based on the ternary Hamming code and ternary Golay code is optimum in a sense that they achieve the smallest possible distortion. Then Fridrich and Soukal [16] presented a data hiding scheme using matrix embedding that is efficient for embedding messages. This scheme is based on random linear code of small dimension which provides good embedding efficiency, where the relative payload is above 0.9 bits per pixel (bpp). A data hiding scheme suggested by Zhang et al. [64], which improves the embedding efficiency of binary covering function that employed the capacity more efficiently by extending the block of binary cover code. This method performs equally with ternary code without binary-ternary conversion of the message. Again Fridrich et al. [17] observed that the quality which determines the embedding efficiency is not the covering radius but the average distance to code. For the linear code, the highest embedding efficiency is not necessarily achieved using code with the smallest covering radius. Chang et al. [7] proposed a data hiding method using (7, 4) Hamming code. This scheme embeds a section of seven bits within a set of seven original image pixels at a time. They achieve embedding payload 0.99 (bpp) where average PSNR equals to 50 (dB). Kim et al. [24] developed Data Hiding using Hamming Code (DHHC) to hide secret messages within halftone image. Here, they used codeword to generate a syndrome value. Then using Exclusive-OR operation they embed four bits secret data within the codeword of four bits. Ma et al. [41] suggested an improvement of Kim et al.'s scheme by altering pixel pair which reduces data embedding capacity by half. Recently, a Dispersed Data Hiding scheme through Hamming Code (DDHHC) has been designed by Lien et al. [35] using space filling curve decomposition. In this scheme, average PSNR is 44.31 (dB), when $4,096$ bits are embedded. Using Hamming code, Kim et al. gained good quality image and their modified PSNR (MPSNR) and payload are 48.20 (dB) and 0.86 (bpp) respectively. Lien et al. achieved 29.66 (dB) for embedding 65,536 bits. Recently, Cao et al. [4] developed high payload Hamming code based data hiding schemes with embedding rate up to 3 (bpp) with PSNR 51 (dB). High payload steganographic scheme also has been developed recently by Bai and Chang [2] for compressed images. Their payload is 2 (bpp) but PSNR is below 30 (dB).

In data hiding schemes, achievement of reversibility and enhancement of security while maintaining good visual quality through Hamming code is still an important issue. So far in the literature, it is found that no such scheme exists, where reversibility has been achieved through Hamming code. The use of shared secret key in data hiding through Hamming code is also rarely available. In the present research, dual image based reversible data hiding schemes using (7, 4) Hamming code has been proposed.

2.2 Brief review of data hiding through Pixel Value Difference (PVD), Difference Expansion (DE) and Exploiting Modification Direction (EMD)

A simple data hiding scheme is the Least Significant Bit - Replacement (LSB-R) has been introduced by Turner [52]. The LSB-R scheme is unbalanced because even valued pixel will never be decremented and odd valued pixel will never be incremented. This asymmetry is easily detected by some detectors [14]. To overcome this problem, Sharp [45] proposed LSB matching (LSB-M) scheme which does not replace LSB but randomly either increments or decrements *one* in LSB of cover image when no match is found with secret data bit. Embedded message within the scheme is also detected by the detector suggested by Ker [23]. To enhance the LSB-M scheme, Mielikainen [42] proposed the LSB matching revisited (LSB-M-R) where payload was same as LSB-M but changes are fewer, which guarantees good quality stegos. Zang and Wang [63] claimed that the modification direction of Mielikainen's scheme is not exploited fully; that is why they developed a data hiding scheme by Exploiting Modification Direction (EMD) which achieves maximum data hiding capacity through one bit per pixel (bpp).

A novel data hiding scheme has been introduced by Wu and Tsai [60] using Pixel Value Difference (PVD). The PVD scheme calculates the difference between two adjacent pixels of cover image and the number of data bits are to be embedded depending on the absolute difference value and a predefined reference table. Data bits are embedded by modifying these two pixel values. Zhang et al. [65] have shown that the scheme proposed by Wu and Tsai [60] is vulnerable to steganalysis based on histogram of pixel value difference. It can provide an estimate of the embedded data length due to its abnormal behavior. They suggested a pseudo random dithering approach which removes the undesirable steps existing in the PVD histogram of the stego image which preserve invisibility of large embedding capacity. Wang et al. [57] followed the idea of PVD and presented a data embedding method using PVD and modulus. It uses the same technique that was used in Wu and Tsai [60] to decide the number of bits to be concealed into a given pixel pair and then the remainder of these two pixels are calculated. Data is then embedded by modifying the remainder values. Compared to Wu and Tsai's method, Modulus Function -Pixel Value Difference (MF-PVD) reaches a higher payload with good image quality. A loss-less data hiding scheme was designed by Lin and Hsueh [37] which embeds secret message into a cover image using the two differences - between the first and second pixel as well as between the second and third pixel in a three pixel block. The average payload and pure payload capacities are 1.39 and 1.32 (bpp) respectively for PSNR greater than 30 (dB). Chang et al. [6] proposed three PVD (TPVD) to provide large embedding capacity and reduce the distortion by optimal approach of choosing the address point and adaption. They achieved smaller than 38 (dB) PSNR with 1.5 (bpp). PVD scheme developed by Wang et al. [57] had abnormal increase and fluctuation of PVD histogram which may reveal the existence of a hidden message that has been solved by Joo et al. [21]. They used some adjusting process which helps to remove fluctuation around the border of sub-range and achieve high capacity with good imperceptibility. After embedding around 52,275 bytes data they achieve 48.9 (dB) PSNR. Their scheme is also secure against various attacks like RS analysis, steganalysis for LSB matching and PVD histogram based attack. In 2010, Luo et al. [40] proposed a new data hiding scheme based on edge adaption which can take the embedding region corresponding to the length of secret data and the difference between consecutive pixel in the cover image. But their PVD scheme was not good for adaptive embedding. It may lead to possible attack by counting the difference of adjacent pixels in both vertical and horizontal direction that can be exploited by Li et al.[34].

A new data hiding approach was designed by Yang et al. [61] in which two pairs of pixel in a block are processed at the same time. The exploited edge area is more efficient to increase embedding capacity but the quality has been slightly dropped. In 2012, Zaker and Hamzeh [62] observed that the histogram of difference value of stego image under the TPVD is vulnerable to a particular statistical analysis. So they introduced a new steganalytic measure named *Growing Anomalies* that has a linear relationship with secret messages. This proposed steganalyzer can classify with test image as stego or cover with 97% accuracy when they contain more than 10% secret data. A histogram modification scheme for loss-less data hiding has been suggested by Tsai et al. [55] that can calculate the difference between each processing pixel and its neighbor and then use these differences to construct the histogram while the secret message is also being embedded into the pixel located at the peak value based on a histogram shifting scheme in gray scale image. The data capacity for one peak value of each histogram can achieve 44,168 bits on average PSNR value around 50 (dB) but for two peak value data hiding capacity can achieve 61,885 bits on average PSNR values around 47 (dB).

Hong [19] presented a new strategy using the idea of PVD and a patched reference table (PVD-PRT) to provide a better image quality and extendable embedding capacity. In addition, Hong and Chen [20] developed a steganography method based on pixel pair matching (PPM). This method utilized the values of pixel pairs as reference coordinates. To hide the message bits, this method first search for a coordinate in the neighborhood set of this pixel pair based on the message bits. Then, it replaces the pixel pair with the selected coordinate to embed the message bits.

Chen [9] proposed the PVD based method to embed unequal amount of secret information using pixel complexity. In this approach, secret information was embedded in an embedding cell of size (2 × 2), which was composed of randomized embedding units to reduce the falling of boundary program and eliminate sequential embedding. Each embedding cell has two embedding units Pivot Embedding Unit (PEU) and Non Pivot Embedding Unit (NPEU). The difference value of the pair pixel in PEU is calculated to determine the complexity of the pair and to determine the amounts of secret bits to be embedded. More bits will be embedded in the complex area and less in the smooth area. This scheme achieve 47.3 (dB) PSNR when embedded with 54,384 bytes secret data.

Recently, reversible data hiding has attracted much attention to the researchers. Reversible Data Hiding (RDH) is a technique to embed a piece of information into a cover media to generate the stego-media, from which the original cover media can be exactly recovered after extracting the embedded messages. RDH, introduced by Barton [3] which compresses some alternate overlapping bits and add bit stream first then embed them into data block. Fridrich et al. [15] suggested a high capacity data hiding method that embed some message into a cluster of bits. Tian [50] designed a data hiding scheme using difference expansion technique to hide the secret message within a pair of pixel. Alattar [1] modified Tian's method and used the distance difference between four pixels. Lee et al. [33] utilized the histogram of the difference of pixel values to hide the secret data within cover media for improving the visual quality. Being reversible, the original and the embedded data can be completely restored. A RDH using histogram shifting has been proposed by Ni et al. [43]. After that Lin et al. [36] and Tsai et al. [53] suggested to improve RDH scheme through multilevel histogram shifting. Thodi et al. [51] presented RDH scheme that combine histogram shifting and difference expansion.

Chang et al. [5] offered dual image based data hiding technique using EMD method. They first established a mod function of a (256×256) magic matrix. Then convert the secret data bits into numeral system of base-5. Two bits secret data are embedded within a pixel pair of each image at a time. Lee et al. [29] introduced a loss-less data hiding technique that utilizes centralized difference expansion to hide more secret data into smoother areas of cover image. Later, Lee et al. [30] embedded secret message using the center point direction of pixels to get the stego-pixels. To protect the deterioration of the image quality, Lou et al. [38] proposed Reduced Difference Expansion (RDE) method. Lou's scheme is not only reversible but also meets low computational cost with high capacity data embedding scheme. Lee and Huang [28] developed a dual-image based RDH method. In their scheme, the average embedding rate is 1.07 (bpp). Qin et al. [44] presented a dual image based data hiding scheme using EMD. A LSB matching data hiding technique has been designed by Lu et al. [39]. The stego images are obtained through the mod function. To achieve the reversibility in data hiding, the LSBs are checked via an averaging procedure then modification has been performed using a rule table. Chang et al. [5] embedded secret message bits by the mod function to accomplish a higher data hiding capability of 1.00 (bpp), but the visual quality of image was substandard to the method proposed by Lee et al. [33]. Zhang and Wang [64] suggested EMD method, which takes n pixels as embedding bits, and embed digits in $(2n + 1)$ base number system. Kieu and Chang [26] presented a new extraction function by modifying the extraction function proposed by Zhang and Wang's scheme. To solve the irreversibility of the EMD method in Zhang and Wang's scheme, they suggested a novel data hiding strategy based on EMD with reversibility by using two steganographic images, which can achieve satisfactory performances of the data embedding capacity and the quality. Shen and Huang [46] developed a data hiding scheme using PVD and improved EMD but the scheme was not reversible. Qin et al. [44] presented only EMD as a reversible data hiding scheme. In 2016, Lee et al.[31] developed an efficient reversible data hiding with reduplicated exploiting modification direction using image interpolation. Kuo et al. [27] presented a high capacity data hiding scheme using multi-bit encoding function. The embedding capacity of Kuo et al.'s scheme is 4.5 (bpp) but the image quality is nearer to 30 (dB).

Thus, designing an innovative scheme is still an important issue which could maintain good quality image and increase data embedding capacity through dual-image. In this thesis, some data hiding schemes have been proposed based on PVD, DE and EMD using dual-image which achieve good visual qualities and high embedding capacity.

2.3 Brief review of data hiding through Weighted Matrix

A. Westfeld [58] introduced F5 algorithm in which matrix based data embedding occurs using binary Hamming code. They embed k-bits secret message by modifying one bit of $2^k - 1$ least significant bits in the host data. The embedding efficiency increases with the increase of k, while the payload decreases contrarily. In order to increase the embedding efficiency and payload simultaneously, an extended F5 algorithm was developed by Fan et al.[11]. They come up with a brand new idea to realize this aim through adding n-layer extension into previous technique and modifying the form of original hash function. Jung and Yoo [22] suggested a new data hiding method using image interpolation through Neighbor Mean Interpolation (NMI). Lee and Huang [32] proposed improve image interpolation technique by Interpolating with Neighboring Pixels (INP). After that, Tang et al. [49] designed high capacity RDH through multi-layer embedding (CRS) with payload 1.79 (bpp) and PSNR is nearer to 33.85 (dB). In 2016, Tsai et al. [54] proposed an adjustable interpolation-based data hiding scheme based on LSB substitution and histogram shifting. This is two-stage data hiding scheme based on interpolation, LSB substitution, and histogram shifting.

A good data embedding method using a key matrix K and a weighted matrix W has been proposed by Tseng et al. [56] for binary image, that can concealed only two bits in a (3×3) pixel block. A better data hiding scheme through weighted matrix has been presented by Fan et al. [12] for gray scale image that can concealed only four secret data bits within a (3×3) block. Both these matrix based data hiding schemes one can perform only one modular sum of entry-wise-multiplication with weighted matrix W and a (3×3) pixel block. Achieving high capacity with reversibility in data hiding through weighted matrix while maintaining good visual quality is still an important research issue. RDH becomes a very important and challenging task in hidden data communication especially in medical and military applications for ownership identification, authentication and copy right protection.

In the literature, no researcher has considered reversibility with high embedding capacity using weighted matrix. In this thesis, some new weighted matrix based data hiding schemes have been formulated and solved using dual image and image interpolation.

3 Problem Domain

Data hiding is the technique of secured concealed communication which carry private data via some multimedia object so that the representation of private message will not draw any attention from the eavesdroppers while they are being moved through an open public channel. There is a high risk of disclosing while they are being transferred through unsecured public channel. Therefore achieving safe secure communication is one of the important objectives of current research. The story of prisoner's problem was presented by Simmons in 1983 [47] in which the merits and capabilities were explained when the public channel is unsecured.

If the probability of modification within the cover image is less, the security of the data hiding method may increase. A possible way to enhance data hiding security is to increase the embedding efficiency [*number of embedding bits per one embedding change*]. Matrix encoding is one of the popular technique of data hiding which can be used to increase the embedding efficiency. The concept was first proposed by Crandall [10] and implemented by Westfeld [58]. The basic idea is to divide coefficients into groups and use Hamming error correcting codes to limit the changes in each group. A(d, n, k) code can be used to embed k bits into n coefficients by making changes at most d coefficients. The data hiding through Hamming code recently proposed by Chang et al. [7], Kim et al. [24], Ma et al. [41], Kim and Yang [25] and Lien et al. [35]. Chang et al. [7] presented data hiding scheme on (7,4) Hamming code which is not reversible scheme and its visual quality is nearer to 50 (dB). Kim et al. [24] used halftone image to hide secret data using Hamming code where payload and the visual quality is limited. Ma et al. [41] and Lien et al. [35] also used halftone image for data hiding where visual quality is poor. Kim and Yang's [25] data hiding scheme is not reversible. All these developed schemes do not consider any shared secret key to enhance the security. They do not consider reversibility in their developed schemes which is one of the important issues in current research on data hiding.

In Wu and Tsai's [60] PVD based data hiding scheme, the quality as well as the capacity is limited and the scheme is not reversible. The data hiding capacity of Wang et al.'s [57] scheme is same as Wu and Tsai's scheme although the quality is a bit improved due to modulus function but the scheme does not achieve reversibility. Joo and Lee [21] proposed data hiding scheme to enhance the security by preventing abnormal increase of histogram values by a novel adjusting process but the scheme can not recover original image successfully. Chen [9] proposed data embedding technique by pixel pair matching (PPM) to embed more information and to improve image quality but the scheme is also not reversible. All these schemes do not consider any shared secret key to enhance the security in data hiding. Data hiding using DE and EMD method is also paid more attention in the current research. Lu et al. [39] developed dual image based data hiding scheme with payload only one bpp but no shared secret key has been considered to enhance the security. Qin et al. [44] design a hybrid reversible data hiding scheme by combining PVD, DE and EMD with payload 1.16 (bpp) but did not considered any shared secret key in their approach. Data hiding in a special domain is not as much secure as other domains because data hiding is carried out in LSB. So, use of shared secret key is very important issue in data hiding for authentication, copyright control and privacy protection. It is possible to enhance security without compromising quality and embedding capacity.

Some reversible data hiding schemes have been proposed by Chang et al. [5], [8], using dual image but their embedding capacity falls short to the demand for today's digital world. The data hiding capacity is nearer to one bpp. So there is a scope to improve the embedding capacity in dual image based data hiding schemes. Lee et al. [30], [28] also developed dual image based data hiding scheme with poor data hiding capacity. In the literature, none have attempted to achieve reversibility through PVD based data hiding scheme. To achieve a good quality image with low modification, in low cost is a challenge in designing a new reversible data hiding scheme using dual image.

In PVD, DE and EMD based data hiding schemes, overflow and underflow may occur frequently during data embedding. This may effect to measure the performance of data hiding. This is also a challenging job to design a new RDH scheme to control overflow and underflow situation without disturbing quality, security and capacity.

Tseng et al.[56] suggested a secure scheme that uses binary image as cover media and can conceal only two bits secret data within a (3×3) pixel block. After that Fan et al.[11] proposed an improved efficient data hiding scheme which can hide only four bits secret data within a (3×3) pixel block. To increase the data hiding capacity Jung and Yoo [22] first advised data hiding scheme using image interpolation then Lee and Huang [32] proposed more eminent data hiding scheme through image interpolation using multi-layer embedding. Tang et al.[49] observed that the average payload 1.79 (bpp) with PSNR 33.85 (dB) when using image interpolation with multi-layered data hiding scheme. In the literature, a single weighted matrix has been used for data embedding in Tseng et al.[56] and Fan et al.'s [11] scheme. There is an opportunity to enhance security through modification of weighted matrix for every new block using shared secret key.

In Tseng et al.[56] and Fan et al.'s [11] scheme only one entry-wise-multiplication has been performed to embed only few bits secret data in a single block. So, there is a possibility to improve data hiding capacity by performing repeated entry-wise-multiplication operation using image interpolation and dual image through weighted matrix. In this literature, no researcher has exploited reversibility in data hiding through weighted matrix. Dual image provides security in a data hiding scheme because without simultaneous dual image, it is hard for eavesdroppers to retrieve secret data from stego images. This is a special case of secret sharing.

4 Motivations and Objectives of the Thesis

The main objective of this thesis is to design some new secured high capacity reversible data hiding schemes. Now, the key issues on the data hiding schemes are embedding capacity, the perceived quality, reversibility and security.

(i) So far, the data hiding through Hamming code, PVD and Weighted matrix which are not reversible, has a limited embedding capacity. Therefore, the motivation is to increase data hiding capacity and achieve reversibility using said techniques.

(ii) In the literature, it is seen that to send the secret message to the receiver, it is necessary to send the length of secret data through Hamming code based data hiding schemes. This has motivated us to develop some new schemes in which the length of secret message is not required.

(iii) So far, few data hiding techniques have been developed using dual image and image interpolation techniques which have a limited data embedding capacity with moderate magnitude of visual quality. From studying such types of techniques, we are motivated to investigate data hiding schemes using dual image and image interpolation in such a way that its capacity and quality have been improved.

(iv) There are many research works in which secret message has been communicated innocently through steganography without having any shared secret key. But, in real world it is seen that these techniques are less secure. This forces us to develop some innovative data hiding schemes to enhance the security of message using shared secret keys.

(v) In existing literature related with weighted matrix based data hiding schemes, it is observed that there is a limitation of data hiding capacity which is less. Again it is also seen that existing methods are not reversible. But, in present day there are many application areas in which reversibility is very essential. So noticing this, we are motivated to formulate some schemes through which these two drawbacks can be overcome.

The objectives of this thesis have been described elaborately as follows:

(i) **Designing some high payload data hiding schemes:**
In the literature, there are some techniques using Hamming code, PVD and Weighted matrix which have certain data hiding capacity, but from our experience in applications of data hiding schemes in some real life problems, it is seen that it is not sufficient for data hiding capacity. So, for this purpose, the objective of this thesis is to design some techniques to increase the payload using Hamming code, PVD and Weighted matrix which are discussed in Chapters 3, 4, and 5 respectively.

(ii) **Use of shared secret key in data hiding schemes:**
From the literature survey on data hiding schemes, it is seen that till now there exists some security loop hole for sending message from sender to receiver. So, our objective is to develop some schemes using a shared secret key in such a way that data hiding schemes will be more strengthened than previous ones. For this purpose in Chapters 3, 4 and 5, some schemes have been developed using Hamming code, PVD-DE, PVD-EMD, TPVD-DE and Weighted matrix incorporating shared secret keys in sequel.

(iii) **Introducing reversibility in data hiding:**
Though there exists many research work on data hiding schemes, till now no one has developed a scheme using Hamming code, PVD or Weighted matrix to achieve the reversibility. So, here, our objective is to develop some algorithms to achieve the reversibility through Hamming code, PVD and Weighted matrix to developed data hiding schemes which is explained in Chapters 3, 4 and 5 respectively.

(iv) **Conservation of perceptibility**
We know that in steganography, perceptibility is the main requirement in any data hiding algorithm. So, the first and foremost objective is to maintain perceptibility in all our proposed schemes.

5 Organization of the Thesis

In this thesis, some new reversible data hiding techniques are designed and solved. The thesis is divided into seven chapters.

Chapter 1

(Introduction)

This chapter contains an introduction giving an overview of the development on data hiding schemes. Brief review of data hiding, Problem domain, Motivations, Objectives and Organization of the thesis are included in this section.

Chapter 2

(Data Hiding Methodologies)

In this chapter, data hiding methodologies have been described that are used to solve different types of data hiding problems. In the development of the data hiding schemes in this thesis, following data hiding methods have been used.

(i) Hamming Code

(ii) Pixel Value Difference (PVD)

(iii) Difference Expansion (DE)

(iv) Exploiting Modification Direction (EMD)

(v) Weighted Matrix based Data Hiding

(vi) Image Interpolation

(vii) Dual Image based Data Hiding Methods

We have then discussed Steganalysis and Steganographic Attacks.

Chapter 3

(Reversible Data Hiding using Hamming Code)

3.1: Partial Reversible Data Hiding using (7,4) Hamming Code (PRDHHC)

Secure data communication through Hamming code based data hiding without knowing the length of secret message is a challenging problem. A data hiding scheme using Hamming code with shared secret position is developed and solved. In this method, the original cover image is partitioned into (7×7) pixel block then collect LSB of each pixel. Now, adjust redundant bits using odd parity. The bit at the shared secret position is complemented and secret data bit is embedded through error creation. For the next row, the shared secret position is updated by the data embedding position of the previous row. The process is repeated to embed all secret message bits within cover image. If a row contains all 1s or 0s, then secret data bit is embedded at the first position. At the receiver end, bit at the shared secret position is complemented first and then secret data bit is retrieved by applying Hamming error correcting code. The extraction process will be continued until error is found at the secret position. In this scheme, Hamming adjusted cover image is recovered by complement bits at both the secret position and data embedding position but original cover image could not be recovered. It is observed that PSNR of PRDHHC scheme is nearer to 58 (dB) which is more than other existing schemes but the payload is only 0.142 (bpp). This is not reversible scheme.

3.2: Dual Image based Reversible Data Hiding using Hamming Code (DRDHHC)

To overcome the irreversibility of previous approach, dual image has been proposed. In this scheme, two copies of LSBs are collected and redundant bits at positions 1, 2 and 4 of first copy are adjusted by odd parity using bit positions 3, 5, 6 and 7; and the redundant bit at positions 3, 5, 6, and 7 of second copy are adjusted by odd parity using bits at positions 1, 2 and 4. After successfully embedding the secret data bits using previous technique, two stego pixel blocks are distributed between dual stego images depending on shared secret key. The secret data bits are successfully recovered at the receiver end from dual images by the help of shared secret position and Hamming error correcting code. After extracting the secret message from dual stego images, bits from 3, 5, 6 and 7 positions from first stego image and bits from 1, 2 and 4 positions of second one are combined and rearranged to recover original cover image. The average PSNR of this proposed RDH scheme is greater than 53 (dB) and the maximum payload is 0.142 (bpp).

3.3: Enhanced Partial Reversible Data Hiding using Hamming Code (EPRDHHC)

Data embedding concept of PRDHHC is used in three LSB layers (LSB, LSB+1 and LSB+2) of cover image to enhance the payload. In this approach, PSNR is nearer to 52 (dB) and payload is 0.426 (bpp). The main drawback of this approach is that, it can not recover original cover image successfully after extraction the secret data.

3.4: Enhanced Dual Image based Reversible Data Hiding using Hamming Code (EDRDHHC)

To achieve reversibility, the techniques of DRDHHC and EPRDHHC have been combined to embed secret data. Dual image concept has been taken from DRDHHC and three LSB layers (LSB, LSB+1, LSB+2) concept has been taken from EPRDHHC. This is an RDH scheme in which the average PSNR is greater than 38 (dB) and the payload is 0.426 (bpp).

All the experimental results are presented graphically and numerically. The results are compared with existing schemes. The results of different steganalysis (RS analysis, Statistical analysis) and steganographic attacks (Histogram attack and Brute force attack) are presented. There is a scope to improve the data hiding capacity while maintaining good visual quality through other data hiding approaches discussed in next chapter.

Key features of the schemes in Chapter 3:

(i) Achieving reversibility with good visual quality is the main key feature of these proposed Hamming code based data hiding schemes.

(ii) Any arbitrary length of secret message can be communicated through these data hiding schemes.

(iii) Shared secret position has been used to enhance security. It has been updated for new block using $\kappa_{i+1} = (\kappa_i \times \omega) \mod 7+1$, where i= 1, 2, 3, . . . , N_B. N_B represents the number of block, κ_0 is the shared secret position and ω is the data embedding position.

(iv) In the dual image based schemes, both shared secret position κ_0 and shared secret key ξ have been used. The stego image blocks are distributed between dual stego images depending on the bit pattern of secret key ξ.

Chapter 4

(Reversible Data Hiding using PVD, DE and EMD)

4.1: Dual Image based RDH using PVD with DE (PVDDE)

To enhance the embedding capacity while preserving good visual quality, a dual-image based RDH scheme using PVD with DE (PVDDE) has been proposed. Here, a secret message is partitioned into n bits, where $(n-1)$ bits are embedded using PVD and one bit is embedded through DE and generate two sets of pixel pair. These two sets of pixel pair are distributed within dual images depending on the bit pattern of a shared secret key. At the receiver end, extraction of the hidden message is performed through either PVD or DE that also depends on the same secret key. Here, overflow and underflow situation has been controlled which may occurs at the data embedding stage. The payload is 1.25 (bpp) and PSNR is greater than 37 (dB) in this approach.

4.2: Dual Image based RDH using PVD with EMD (PVDEMD)

To increase the payload, another dual-image based RDH scheme using PVD with EMD has been proposed. First, enlarge the original image using image interpolation technique then embed secret data bits within pixel pair using PVD. Here, four data bits are embedded through PVD method and two data bits are embedded using EMD method. After embedding two sets of stego pixel pairs have been generated. After that stego pixel pairs are distributed between dual image based on the bit pattern of a shared secret key. At the receiver end, the stego pixel pairs are distinguished using secret key. Then corresponding PVD or EMD methods are used to extract hidden message and recover original image. In this approach, the PSNR is 40.43 (dB) and payload is 1.75 (bpp).

4.3: Dual Image based RDH using Three PVD (TPVD) with DE (TPVDDE)

Further, RDH method using Three Pixel Value Difference (TPVD) with DE (TPVDDE) has been proposed. The embedding capacity of this method is 2.15 bpp which is higher than other existing schemes but the PSNR is less than 30 (dB).

All the experimental results are numerically and graphically illustrated. The results of these new three different approaches are compared with existing schemes. The effect of different steganalysis (RS analysis, Relative entropy and Statistical analysis) and steganographic attacks (Histogram attack Brute force attack) are demonstrated.

Key features of the schemes in Chapter 4:

(i) Data embedding using PVD method was not reversible. Reversibility has been achieved through proposed data hiding schemes using PVD, DE and EMD methods.

(ii) Data embedding capacity has been increased in PVD based data hiding methods using dual image and image interpolation.

(iii) Shared secret key has been used to distribute stego pixel pairs among dual images to enhance security.

(iv) Overflow and underflow situations have been controlled which may appears during data embedding.

Chapter 5

(Reversible Data Hiding using Weighted Matrix)

5.1: Dual Image based RDH using Weighted Matrix (DRDHWM)

Weighted matrix based RDH using dual image has been introduced. First, partition the cover image into (3×3) pixel block. Then perform modular sum of entry-wise-multiplication between image block and a predefined weighted matrix. After that calculate the difference between value of modular sum and selected data unit. To embed these secret data, increase or decrease the pixel value that depend on the sign of the calculated difference value. The pixel has been selected depending on the position of the element of weighted matrix. Now, store the difference value within stego pixel by adding with original pixel value. The process is repeated nine times to embed thirty six bits secret data within the selected block. For each next i-th block $(i = 1, 2, \ldots)$, update weighted matrix W_{i+1} as $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where $gcd\ (\kappa,\ 9) = 1$ and κ is shared secret key. Finally, the original and stego pixels are distributed between dual images depending on the bit pattern of a shared secret key. At the receiver end, secret message has been extracted successfully using predefined weighted matrix and the shared secret key. The original image has been recovered without any distortion from dual stego images because the original pixels are kept unaltered within stego images during data embedding which ensure reversibility. In this scheme, payload is 1.98 (bpp) and PSNR is greater than 39 (dB).

5.2: Interpolated Image based RDH using Weighted Matrix (IRDHWM)

To increase the payload, a high capacity secure RDH scheme has been proposed. First, enlarge the size of original image into double through image interpolation. Then partition the original image into (3×3) pixel block and interpolated image into (5×5) pixel block. Perform modular sum of entry-wise-multiplication of image block with predefined weighted matrix. Calculate the difference value between modular sum of entry-wise-multiplication and selected data unit. In each operation, the data embedding position is identified and stored at three least significant bits of the interleaved pixel of interpolated image. Embed secret data by increasing or decreasing the original pixel value by one. Twelve multiplication operations have been performed to embed forty-eight bits secret data within a (5×5) pixel block of interpolated image. For next each i-th block, $(i = 1,\ 2, \ldots)$, update weighted matrix W_{i+1} as $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where $gcd\ (\kappa, 9) = 1$ and κ is shared secret key. The data hiding capacity of this approach is 2.96 (bpp) and PSNR is 37.37 (dB).

5.3: Interpolated Dual Image based Reversible Data Hiding using Weighted Matrix (IDRDHWM)

Finally, a very high capacity RDH scheme has been proposed through weighted matrix using interpolated dual image. The data embedding procedure has been done in two stages. In the first stage, embed thirty six bits secret data within a block of dual image through repeated embedding process of nine times using weighted matrix. In the next stage, repeat embedding process twenty four times to embed ninety six bits secret data within each block of interpolated dual image. After hiding one hundred and thirty-two bits secret data within one block of dual image update the weighted matrix. For i-th block ($i = 1, 2, \ldots$), the weighted matrix W_{i+1} can be updated as $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where $gcd\ (\kappa, 9) = 1$ and κ is a shared secret key. In the extraction process, the positional values are extracted from interpolated dual stego images and the secret data is recovered by performing modular sum of entry-wise-multiplication between weighted matrix and original pixel block. Again rearrange the pixel using shared secret key from dual image and perform the same extraction operation thirty-three times and extract one hundred thirty-two bits secret data from a pixel block. The scheme provides average embedding payload 3.46 (bpp) with PSNR greater than 35 (dB).

All the experimental results of the proposed methods are numerically and graphically illustrated. The results of these different approaches are compared with existing methods. Steganalysis and steganographic attacks on stego images are performed which are also illustrated numerically.

Key features of the schemes in Chapter 5:

(i) Achieve high payload with good visual quality in weighted matrix based data hiding schemes.

(ii) Achieve reversibility in weighted matrix based data hiding schemes.

(iii) Update weighted matrix $W_{i+1} = (W_i \times \kappa - 1) \mod 9$, where $gcd\ (\kappa, 9) = 1$ and $i = 1, 2, 3, ..., N_B$, N_B represents the number of blocks in the cover image for each new block to enhance security.

Chapter 6

(Analysis and Discussions)

In this chapter, proposed data hiding schemes are analyzed. The comparisons of suggested schemes with respect to data embedding capacity and visual quality are presented here. The results of steganalysis and various steganographic attacks are presented.

Chapter 7

(Conclusion and Future Research Work)

At the end, some limitations and the scope of future research works have been discussed.

References

[1] Alattar, A. M. (2004), *Reversible watermark using the difference expansion of a generalized integer transform*, IEEE Transactions on Image Processing, 13(8), 1147-1156.

[2] Bai, J. and Chang, C.C. (2016), *A High Payload Steganographic Scheme for Compressed Images with Hamming Code*, International Journal of Network Security, 18(6), 1122-1129.

[3] Barton, J. M. (1997), *Method and apparatus for embedding authentication information within digital data*, U.S. Patent No. 5,646,997.

[4] Cao, Z., Yin, Z., Hu, H., Gao, X., and Wang, L. (2016), *High capacity data hiding scheme based on (7, 4) Hamming code*, Springer Plus, 5(1), 1-13.

[5] Chang, C. C., Kieu, T. D., and Chou, Y. C. (2007), *Reversible data hiding scheme using two steganographic images*, TENCON 2007-2007, IEEE Region 10 Conference, 1-4.

[6] Chang, K. C., Chang, C. P., Huang, P. S. and Tu, T. M. (2008), *A novel image steganographic method using tri-way pixel-value differencing*, Journal of multimedia, 3(2), 37-44.

[7] Chang, C. C., Kieu, T. D. and Chou, Y. C. (2008), *A high payload steganographic scheme based on (7, 4) hamming code for digital images*, International Symposium on Electronic Commerce and Security, IEEE, 16-21.

[8] Chang, C. C., Lu, T. C., Horng, G., Huang, Y. H. and Hsu, Y. M. (2013), *A high payload data embedding scheme using dual stego-images with reversibility*, 9th International Conference on Information Communications and Signal Processing (ICICS), IEEE, 1-5.

[9] Chen, J. (2014), *A PVD-based data hiding method with histogram preserving using pixel pair matching*, Signal Processing: Image Communication, Elsevier, 29(3), 375-384.

[10] Crandall, R. (1998), *Some notes on steganography*, Posted on steganography mailing list, http://os.inf.tudresden.de/ westfeld/crandall.pdf

[11] Fan, L., Gao, T., Yang, Q. and Cao, Y. (2011), *An extended matrix encoding algorithm for steganography of high embedding efficiency*, Computers & Electrical Engineering, Elsevier, 37(6), 973-981.

[12] Fan, L., Gao, T. and Cao, Y. (2013), *Improving the embedding efficiency of weight matrix-based steganography for grayscale images*, Computers & Electrical Engineering, Elsevier, 39(3), 873-881.

[13] Fridrich, J., Goljan, M. and Hogea, D. (2002), *Attacking the outguess*, Proceedings of the ACM Workshop on Multimedia and Security, Juan-les-Pins, France.

[14] Fridrich, J., Goljan, M. and Du, R. (2001), *Reliable detection of LSB steganography in color and grayscale images*, Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM, 27-30.

[15] Fridrich, J., Goljan, M. and Du, R. (2002), *Lossless data embedding: new paradigm in digital watermarking*, EURASIP Journal on Applied Signal Processing, 2002(1), 185-196.

[16] Fridrich, J. and Soukal, D. (2006), *Matrix embedding for large payloads*, Electronic Imaging 2006, International Society for Optics and Photonics, 60721W-60721W.

[17] Fridrich, J., Lisonek, P. and Soukal, D. (2006), *On steganographic embedding efficiency*, Information Hiding, Springer Berlin Heidelberg, 282-296.

[18] Hamming, R. W. (1950), *Error detecting and error correcting codes*, Bell System Technical Journal, Wiley Online Library, 29(2), 147-160.

[19] Hong, W. (2013), *Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique*, Information Sciences, Elsevier, 221, 473-489.

[20] Hong, W. and Chen, T. S. (2012), *A novel data embedding method using adaptive pixel pair matching*, IEEE Transactions on Information Forensics and Security, IEEE, 7(1), 176-184.

[21] Joo, J. C., Lee, H. Y. and Lee, H. K. (2010), *Improved steganographic method preserving pixel-value differencing histogram with modulus function*, EURASIP Journal on Advances in Signal Processing, 2010, 26.

[22] Jung, K. H. and Yoo, K. Y. (2009), *Data hiding method using image interpolation*, Computer Standards & Interfaces, Elsevier, 31(2), 465-470.

[23] Ker, A. D. (2005), *Steganalysis of LSB matching in grayscale images*, Signal Processing Letters, IEEE, 12(6), 441-444.

[24] Kim, C., Shin, D. and Shin, D. (2011), *Data hiding in a halftone image using hamming code (15, 11)*, Intelligent Information and Database Systems, Springer Berlin Heidelberg, 372-381.

[25] Kim, C. and Yang, C. N. (2014), *Data hiding based on overlapped pixels using hamming code*, Multimedia Tools and Applications, Springer, 1-13.

[26] Kieu, T. D. and Chang, C. C. (2011), *A steganographic scheme by fully exploiting modification directions*, Expert systems with Applications, Elsevier, 38(8), 10648-10657.

[27] Kuo, W. C., Kuo, S. H., Wang, C. C., and Wuu, L. C. (2016), *High capacity data hiding scheme based on multi-bit encoding function*, Optik-International Journal for Light and Electron Optics, 127(4), 1762-1769.

[28] Lee, C. F. and Huang, Y. L. (2013), *Reversible data hiding scheme based on dual stegano-images using orientation combinations*, Telecommunication Systems, Springer, 52(4), 2237-2247.

[29] Lee, C. C., Wu, H. C., Tsai, C. S. and Chu, Y. P. (2008), *Adaptive lossless steganographic scheme with centralized difference expansion*, Pattern Recognition, Elsevier, 41(6), 2097-2106.

[30] Lee, C. F., Wang, K. H., Chang, C. C. and Huang, Y. L. (2009), *A reversible data hiding scheme based on dual steganographic images*, Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ACM, 228-237.

[31] Lee, C. F., Weng, C. Y., and Chen, K. C. (2016), *An efficient reversible data hiding with reduplicated exploiting modification direction using image interpolation and edge detection*, Multimedia Tools and Applications, Springer, 1-24.

[32] Lee, C. F. and Huang, Y. L. (2012), *An efficient image interpolation increasing payload in reversible data hiding*, Expert Systems with Applications, Elsevier, 39(8), 6712-6719.

[33] Lee, S. K., Suh, Y. H. and Ho, Y. S. (2004), *Lossless data hiding based on histogram modification of difference images*, Advances in Multimedia Information Processing-PCM 2004, Springer Berlin Heidelberg, 340-347.

[34] Li, X., Li, B., Luo, X., Yang, B. and Zhu, R. (2013), *Steganalysis of a PVD-based content adaptive image steganography*, Signal Processing, Elsevier, 93(9), 2529-2538.

[35] Lien, B. K., Chen, S. K., Wang, W. S. and King, K. P. (2015), *Dispersed Data Hiding Using Hamming Code with Recovery Capability*, Genetic and Evolutionary Computing, Springer International Publishing, 179-187.

[36] Lin, C. C., Tai, W. L. and Chang, C. C. (2008), *Multilevel reversible data hiding based on histogram modification of difference images*, Pattern Recognition, Elsevier, 41(12), 3582-3591.

[37] Lin, C. C. and Hsueh, N. L. (2008), *A lossless data hiding scheme based on three-pixel block differences*, Pattern Recognition, Elsevier, 41(4), 1415-1425.

[38] Lou, D. C., Hu, M. C. and Liu, J. L. (2009), *Multiple layer data hiding scheme for medical images*, Computer Standards & Interfaces, Elsvier, 31(2), 329-335.

[39] Lu, T. C., Tseng, C. Y. and Wu, J. H. (2015), *Dual imaging-based reversible hiding technique using LSB matching*, Signal Processing, Elsevier, 108, 77-89.

[40] Luo, W., Huang, F. and Huang, J. (2010), *Edge adaptive image steganography based on LSB matching revisited*, IEEE Transactions on Information Forensics and Security, 5(2), 201-214.

[41] Ma Z., Li Y. and Zhang X. (2013), *Based on Hamming and subordinate pixel compensation halftone image information hiding*, Journal of Shanghai University (Natural Science), 19(2), 111-115.

[42] Mielikainen, J. (2006), *LSB matching revisited*, Signal Processing Letters, IEEE, 13(5), 285-287.

[43] Ni, Z., Shi, Y. Q., Ansari, N. and Su, W. (2006), *Reversible data hiding*, IEEE Transactions on Circuits and Systems for Video Technology, IEEE, 16(3), 354-362.

[44] Qin, C., Chang, C. C. and Hsu, T. J. (2015), *Reversible data hiding scheme based on exploiting modification direction with two steganographic images*, Multimedia Tools and Applications, Springer, 74(15), 5861-5872.

[45] Sharp, T. (2001), *An implementation of key-based digital signal steganography*, Information hiding, Springer Berlin Heidelberg, 13-26.

[46] Shen, S. Y. and Huang, L. H. (2015), *A data hiding scheme using pixel value differencing and improving exploiting modification directions*, Computers & Security, Elsevier, 48, 131-141.

[47] Simmons, G. J. (1984), *The prisoners problem and the subliminal channel*, Advances in Cryptology, Springer US, 51-67.

[48] Stanley, C. A. (2005), *Pairs of Values and the Chi-squared Attack*, Department of Mathematics, Iowa State University.

[49] Tang, M., Hu, J. and Song, W. (2014), *A high capacity image steganography using multi-layer embedding*, Optik-International Journal for Light and Electron Optics, Elsevier, 125(15), 3972-3976.

[50] Tian, J. (2003), *Reversible data embedding using a difference expansion*, IEEE Transactions on Circuits and Systems for Video Technology, 13(8),890-896.

[51] Thodi, D. M., and Rodríguez, J. J. (2007), *Expansion embedding techniques for reversible watermarking*, IEEE Transactions on Image Processing, IEEE, 16(3), 721-730.

[52] Turner, L. F. (1989), *Digital data security system*, Patent IPN wo, 89, 08915.

[53] Tsai, P., Hu, Y. C. and Yeh, H. L. (2009), *Reversible image hiding scheme using predictive coding and histogram shifting*, Signal Processing, Elsevier, 89(6), 1129-1143.

[54] Tsai, Y. Y., Huang, Y. H., Lin, R. J., and Chan, C. S. (2016), *An Adjustable Interpolation-based Data Hiding Algorithm Based on LSB Substitution and Histogram Shifting*, International Journal of Digital Crime and Forensics (IJDCF), 8(2), 48-61.

[55] Tsai, Y. Y., Tsai, D. S. and Liu, C. L. (2013), *Reversible data hiding scheme based on neighboring pixel differences*, Digital Signal Processing, Elsevier, 23(3), 919-927.

[56] Tseng, Y. C., Chen, Y. Y. and Pan, H. K. (2002), *A secure data hiding scheme for binary images*, IEEE Transactions on Communications, IEEE, 50(8), 1227-1231.

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

[58] Westfeld, A. (2001), *F5 a steganographic algorithm*, Information hiding, Springer Berlin Heidelberg, 289-302.

[59] Willems, F. M. and Van Dijk, M. (2005), *Capacity and codes for embedding information in gray-scale signals*, IEEE Transactions on Information Theory, 51(3), 1209-1214.

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

[61] Yang, C. H., Weng, C. Y., Tso, H. K. and Wang, S. J. (2011), *A data hiding scheme using the varieties of pixel-value differencing in multimedia images*, Journal of Systems and Software, Elsevier, 84(4), 669-678.

[62] Zaker, N., and Hamzeh, A. (2012), *A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram*, Multimedia Tools and Applications, Springer, 58(1), 147-166.

[63] Zhang, X. and Wang, S. (2006), *Efficient steganographic embedding by exploiting modification direction*, Communications Letters, IEEE, 10(11),781-783.

[64] Zhang, W., Wang, S. and Zhang, X. (2007), *Improving embedding efficiency of covering codes for applications in steganography*, Communications Letters, IEEE, 11(8), 680-682.

[65] Zhang, X. and Wang, S. (2004), *Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security*, Pattern Recognition Letters, Elsevier, 25(3), 331-339.