Chapter 1

Introduction

With the rapid development of communication technology and the widespread distribution of digital data over the Internet, it has become easy to obtain valuable information. Consequently, multimedia signals need more protection against unauthorized access and modification. Digital watermarking becomes an effective method for protecting multimedia documents. Watermarking refers to the process of embedding an identification code or some other information called watermark into a multimedia document without affecting the visual quality. Such a watermark can be used for various purposes including authentication, copyright protection, ownership identification, copy-move forgery, digital forensic and tamper detection of multimedia documents. Watermarking is used to protect the original materials from being misused, and it helps us to know the lawful ownership.

Watermarking is applied to conserve copyrighted documents from being perverted and allow us to get the information about permissible ownership. Nowadays for any watermarking technique security is a pinnacle attraction for developers. One of the paramount demand of the watermarking technique is robustness. The preeminent challenges in watermarking are to stand robust against modification, compression, scaling, filtering, cropping, etc. So an efficient watermarking scheme should make a good tradeoff among security, robustness, and imperceptibility. Though high embedding capacity is not the purpose of watermarking schemes, many of the current researchers also take this as one of the crucial characteristics while possessing the quality of the watermarked image. The essential features of watermarking schemes are imperceptibility, payload, security, tamper detection, complexity, authentication and execution time.

To increase the embedding capacity, enhance security and maintain good visual quality in reversible watermarking technique through the weighted matrix is still an important issue in current research. In addition, tamper detection and image authentication are the demanding issues in the era of digitization. So, it is a critical challenge for the researchers in the area of multimedia security to maintain a trade-off among the robustness, visual quality, and payload.

1.1 Literature Review

Richard Wasley Hamming [28] devised a sophisticated pattern of parity checking code that could correct a single error and detect double errors. Crandall [18] first pointed out that embedding efficiency could be improved by coding methods and suggested the matrix coding.

Westfeld [95] introduced data hiding techniques through matrix encoding based on Hamming code. Tseng et al. [87] proposed data hiding scheme by taking into consideration the quality of the image after data hiding. Willems and Dijk [96] suggested that the embedding code based on the ternary Hamming code and ternary Golay code is optimum in the sense that they achieve the smallest possible distortion. Then Fridrich and Soukal [24] presented a data hiding scheme using matrix embedding that is efficient for embedding messages. This scheme is based on the 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. [108] which improves the embedding capacity by employing an extended block of binary cover code. This method performs equally with ternary code without binary-ternary conversion of the message. Again, Fridrich et al. [24] 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 a code with the smallest covering radius. Chang et al. [12] 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 achieved embedding payload 0.99 (bpp) where average PSNR equals to 50 (dB). Kim et al. [43] developed Data Hiding using Hamming Code (DHHC) to hide secret messages within a 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. A Dispersed Data Hiding scheme through Hamming Code (DDHHC) has been designed by Lien et al. [51] using space-filling curve decomposition. In this scheme, average PSNR of 44.31 (dB) is obtained, when $4, 096$ bits are embedded. Using Hamming code, Kim et al. [43] gained good quality image and their modified PSNR (MPSNR) and payload are 48.20 (dB) and 0.86 (bpp) respectively. Lien et al. [51] achieved PSNR of 29.66 (dB) for embedding 65,536 bits. Cao et al. [8] developed high payload Hamming code based data hiding scheme with embedding rate up to 3 (bpp) and PSNR 51 (dB). High payload steganographic scheme has been developed by Bai and Chang [5] for compressed images. Their payload is 2 (bpp), but PSNR is below 30 (dB). Recently, a partial reversible and a dual image based reversible data hiding schemes using (7, 4) hamming code have been developed by the Jana et al. [36] [37] to improve both the data hiding capacity and visual quality.

In watermarking schemes, achievement of reversibility along with the enhancement of security while maintaining good visual quality through the 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 a shared secret key in watermarking through Hamming code is also rarely available. In the present research, dual image based reversible watermarking schemes using (15, 11) Hamming code has been proposed.

Westfeld [95] 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 improve the embedding efficiency and payload simultaneously, an extended F5 algorithm was developed by Fan et al. [21]. They come up with a brand new idea to realize this aim by adding an n-layer extension into previous technique and modifying the form of original hash function. Jung and Yoo [42] suggested a new data hiding method using image interpolation through Neighbor Mean Interpolation (NMI). Lee and Huang [46] proposed to improve image interpolation technique by Interpolating with Neighboring Pixels (INP). After that, Tang et al. [81] 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. [86] proposed an adjustable interpolation-based data hiding scheme based on LSB substitution and histogram shifting. It is a two-stage data hiding scheme based on interpolation, LSB substitution, and histogram shifting.

A novel data embedding method using a key matrix K and a weighted matrix W has been proposed by Tseng et al. [87] for the binary image, that can be 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. [20] for the gray scale image that can be concealed only four secret data bits within a (3×3) block. Through 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 watermarking through weighted matrix while maintaining good visual quality is still an important research issue. RDH becomes very important and a challenging task in hidden data communication especially in medical and military applications for ownership identification, authentication and copyright protection.

To increase the data embedding capacity, without affecting high quality, image interpolation has been used which enlarges the size of the image depending on neighbours pixels. A reversible data hiding scheme based on neighbour mean interpolation (NMI) has been developed by Jung and Yoo [42] which improved the embedding capacity and image quality. Lee and Huang [46] developed interpretation by neighbouring pixel (INP). Further, Tang et al. [81] suggested capacity reversible steganography (CRS) which can improve image interpolation. Recently, Jana et al. [35] developed a weighted matrix based reversible data hiding scheme through image interpretation which can hide 2.97 bpp, but till date, no such development has been found to accomplish three major research issue such as tamper detection, authentication, and recovery in a single model. In the literature, a few researcher has considered reversibility in watermarking scheme with high embedding capacity using a weighted matrix. In this thesis, some new weighted matrix based watermarking schemes have been formulated and solved using dual image and image interpolation.

Cellular automata were introduced by Ulam and Von Neumann [88]. The idea that pushed Von Neumann to propose the cellular automata model was constructing a self-replicating machine, which components would obey physical laws defined by differential equations. A cellular automaton is a computer algorithm that is discrete in space and time and operates on a lattice of sites (in our case, pixels). It consists of a regular grid of cells with each one of a finite number of states, such as “On” and “Off” (in contrast to a coupled map lattice). The grid can be in any finite number of dimensions. For each cell, a set of cells called its neighborhood. The communication between constituent cells is limited to local interaction. Using cellular automata as a discrete model is another way to generate such intricate information. This information would be embedded in a particular domain of an image for image encryption and digital image forgery detection. Xiaoyang et al. [99] used elementary cellular automata state rings to encrypt and decrypt QR code binary image. Jin [38] developed an image encryption approach utilizing the behavior of Elementary Cellular Automata (ECA) with periodic boundary conditions. Tafti et al. [80] proposed a method to use the one-dimensional cellular automata including statistical information of a digital image as an operational and practical way for image forgery detection. They proposed another CA-based watermarking scheme for active image forgery detection. Copy-move forgery detection using cellular automata has been proposed by Tralic et al. [85]. Then to enhance security Tralic et al. [83] employ Local Binary Pattern (LBP) in the watermarking scheme.

Zhang and Shih [94] proposed a novel semi-fragile watermarking scheme based on the LBP.

According to the exclusive-or (XOR) value of LBP in each block, a binary watermark is embedded into the host image by adjusting pixel values in the neighbourhood. The LBP operator is a simple texture descriptor, proposed by Ojala et al. [62]. It reflects the local contrast between the central pixel value and its neighbourhood pixel values, and this spatial relationship is finally described in a binary pattern. With continuous improvements in the LBP algorithm, many improved LBP operators have been proposed, such as uniform LBP [93] and rotation invariant LBP [73]. Guo et al. [27] presented another modeling of the local binary pattern operator for texture classification using two complementary components: the signs and the magnitudes. Zhang et al. [107] improved the LBP operator by considering the magnitude of gray-level differences, concentrating on the visually most important texture pattern parts of images, and disregarding the unimportant details. Here, we have used LBP in the watermarking scheme for tamper detection.

The image authentication and tamper detection is an important issue to ensure the protection of digital information and to preserve the integrity of the multimedia document. Two categories of image authentication have been found such as active and passive [72] [44]. Passive authentication scheme [3] is a technique which employs no additional information embedded within the object required for image forensic whereas active authentication can store authentication code within the watermark image. In authentication based watermark scheme through data embedding can verify the authentication code which is extracted from the watermarked image as well as detect tamper location that is present within the tampered object. The promising image authentication techniques based on watermarking schemes have been categorized as fragile and semi-fragile. The fragile watermarking techniques are to detect and localize modification areas whereas semi-fragile can resist the modification. Several image authentication based watermarking schemes have been developed [44, 49, 54, 66, 82, 92] but, they have the capability to detect only the tampered area in the modified image but cannot recover. Wang and Tsai [92] developed an image authentication and recovery scheme using fractal coding and image inpainting. In another work, Qin et al. [70] suggested a fragile watermarking scheme that has restoration capability. Recently, Chuang et al. [15] suggested vector quantization based tamper detection and authentication scheme for grey scale image. Several authentication methods based on the reversible watermarking scheme have been developed for different image formats such as for PNG image proposed by Lee and Tsai [49], JPEG image suggested by Yang et al. [101] and index colour image developed by Lo et al. [54]. A fragile watermarking scheme proposed by Lin et al. [52] that can be achieved not only for tamper detection and recovery but also to verify the ownership of the copyrighted document. An enhanced fragile watermarking technique has been proposed by Fan et al. [110] to protect the digital images and to achieve self-recovery after modification of the watermarked image. Their technique is based on set partitioning in hierarchical trees (SPIHT) encoding and Reed-Solomon code, which helps for block-based tamper detection. Golea and Melkemi [109] proposed an ROI based fragile watermarking scheme for medical image tamper detection. In their scheme, they used cyclic redundancy check code for detecting the tampered region. Here we have proposed some innovative scheme to detect tampering and check authentication in a single model. Moreover, proposed schemes have been tested against the different attacking condition.

1.2 Problem Domain

Details of Reversible Watermarking Scheme (RWS) based on Weighted Matrix (WM), Cellular Automata (CA), Hamming code (HC) and Local Binary Pattern (LBP) has been analysed in forthcoming chapter. It is very difficult to achieve satisfactory performance in watermarking scheme with respect to the standard benchmark performance parameters such as imperceptibility, robustness, reversibility, capacity and security. So there are a numerous watermarking scheme which can achieve a better performance considering only one or some of these parameter with compromising the other parameters. So, there must need to develop an efficient watermarking scheme which can make a good trade-off among the said parameters for authentication, tamper detection, copyright protection and ownership identification. Moreover computational cost is also an important parameter to determine the performance of any watermarking scheme. In light of this discussion, we have tried to develop some novel watermarking methods which are able to make good trade-off among the above said parameters while achieving the goal of authentication, tamper detection and localization.

1.3 Objective and Scope of the Thesis

The objective of this investigation is to design some reversible watermarking scheme in spatial domain:

Although there exist many watermarking techniques, but still there is a scope to develop a new scheme based on Weighted Matrix, Local Binary Pattern and Cellular Automata. The objective of this thesis is to formulate some algorithms to verify the authenticity and to localize tamper region. Mostly watermarking schemes are designed in such a way that they can resist a special types of attacks, but no scheme has been developed which can resist various geometric attacks. So our motivation is to generate such algorithms which can withstand various geometric attacks. Uses of watermarking schemes for some real life applications need high embedding capacity. So, designing some techniques to increase the payload using WM, LBP and CA is an important requirement today. From the literature survey on the watermarking scheme, it is found that till date there exists some security loophole during multimedia communication. So, our objective is to develop some schemes using a shared secret key in such a way that watermarking schemes will be more strengthened than existing ones. For this purpose in Chapters 3, 4 and 5, some schemes have been developed using WM, LBP and CA incorporating shared secret keys in sequel using some standard key generator algorithm like MD5, SHA-128, SHA-512, and LFSR.

The dissertation has been organized depending on the recovery of both the original image and watermark under ten (10) different attacking environment. In each case, after embedding watermark, we apply attacks on the watermarked image, and then during watermark extraction, it is examined to find the number of cases in which watermark and original cover image can be successfully recovered. The attacks with various perturbation are as follows: (i) **Salt & Pepper Noise** (0.01, 0.1 and 0.5 noise density), (ii) **Cropping** (10%, 20% and 50%), (iii) **Copy-Move Forgery** (5%, 10% and 20%), (iv) **Opaque** (10%), (v) **Blurring** (Sigma = 0.4), (vi) **Median Filtering** (3 x 3 block filtering), (vii) **Flipping (Vertical)**, (viii) **JPEG Compression**(QF=70), (ix) **Inversion** (Negative invert to all), (x) **Rotation** (1 degree, 90 degree).

1.4 Contributions of the Present Work

In this thesis, some novel reversible watermarking techniques have been designed using Weighted Matrix (WM), Local Binary Pattern (LBP), Cellular Automata (CA) and Lagrange Interpolation Polynomial (LIP) for ownership identification, image authentication, tamper detection and localization with high embedding capacity and good visual quality. Moreover, the proposed schemes have been analyzed against existing attacks such as salt and pepper, cropping, opaque, copy-move forgery, median filtering, blurring, rotation, JPEG compression, etc. It is found that our algorithms can sustain these types of attacks. The contributions of the present work may be summarized as follows.

Salient features of the thesis:

- Authentication Code (AC) is generated using SHA-512 from watermark image and embedded within sub-sample images.
- Tamper detection and authentication of both cover and the secret image is achieved by employing CA attractor with a shared secret key.
- Cellular automata attractor is used to enhancing the security of proposed watermarking scheme in case of secret sharing.
- Sharing the watermark into four different sub-sample images gives the sharing flavour of watermarking scheme.
- Sub-sample images with interpolation are used to increase embedding capacity, security and achieve reversibility. It is hard to extract the secret message without simultaneous sub-sampled images which are the particular case of secret sharing.
- Shared secret key has been XORed with watermark bits and generated an encrypted message which is used in CA for distribution in the sub-sampled image to increase security. It is hard to retrieve the secret message without knowing shared secret key and proper CA rule.
- Encrypted watermark bits are generated through XOR with a shared secret key and embedded within sub-sampled image.
- Achieving reversibility with good visual quality is the primary key feature of these proposed weighted matrix based watermarking schemes.
- Any arbitrary length of a watermark can be communicated through these watermarking schemes.
- The Index file is used to enhance the security of the proposed watermarking scheme.

- Authentication can be achieved by using Local Binary pattern and Dual image.

- Shared secret key has been used to distribute watermark pixel pairs among dual images to enhance security. At the time of sharing, LFSR gives the randomness of the key.

- Hamming code has been used to detect and correct tampered location.

- Tampered location can be identified with the help of the LBP operator.

- Digital watermarking based on LBP method is not reversible. Reversibility has been achieved in proposed watermarking schemes using LBP and Hamming methods.

- Watermark embedding capacity has been increased in LBP based watermarking scheme using dual image and image interpolation.

- Achieve tamper localization in watermarking schemes through LBP operator and Cellular Automata.

- Achieve security by using 2D-CA. LBP operator and LFSR stream cipher algorithm.

- No original watermark data is directly embedded into the cover image. Watermark bits are encrypted with the help of a shared secret key. Four bits watermark data are just embedded by changing one bit of the cover image.

- Achieve the advantages of secret sharing with the help of Lagrange Interpolation Polynomial.

- The 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, $\ldots, N_B$. N_B represents the number of blocks, κ_i is the shared secret position and ω is the watermark embedding position.

- Achieve high payload with good visual quality in Cellular Automata based watermarking schemes.

1.5 Outline of the Thesis

In this thesis, several schemes for reversible watermarking have been introduced for image authentication and tamper detection. The whole work reported in the dissertation has been organized as follows.

Chapter 2: A brief overview of digital watermarking techniques and their applications are presented in this chapter. Moreover, a survey on various research activities related to the existing watermarking methodologies has been described.

Chapter 3: Weighted matrix and Cellular Automata plays a significant role in the design of various watermarking primitives. In Chapter 3, two methods (RWS-WM and RWS-CA) have been developed to design a novel watermarking techniques. In RWS-WM, a modified weighted matrix has been used to improve the embedding capacity and security of the watermarking primitives. In RWS-CA, a novel reversible watermarking scheme using sub-sampled image has been introduced. The CA has been used to improve the security and robustness of the proposed scheme. This chapter also reports the stainability of the suggested methods against various attacks.

Chapter 4: The applications of Local Binary Pattern and Hamming Code for the design of watermarking algorithms establish an important area of research. In Chapter 4, two methods (DRWS-LBP and RWS-LBP-HC) have been developed to design a novel watermarking scheme. Employing LBP in the watermarking scheme for image authentication and tamper detection through dual image has been presented in DRWS-LBP. The tampered region can be corrected with the help of Hamming code and LBP which has been illustrated in RWS-LBP-HC. This chapter also reports the resistivity of the suggested schemes against various attacks.

Chapter 5: This chapter presents an integrated scheme for both tamper detection and localization. Here the LBP operator, WM and CA rule have been employed. In this Chapter, two methods (RWS-LBP-CAand RWS-LBP-WM-LIP) have been proposed to design a novel watermarking scheme. In RWS-LBP-CA, a novel watermarking scheme has been described with the help of LBP operator and CA for image authentication and tamper detection. Lagrange interpolation polynomial has been employed in RWS-LBP-WM-LIP. Here LBP and WM play an important role in authentication and tamper detection. This chapter also reports the robustness of the proposed schemes against various attacks.

Chapter 6: In chapter 6, the comparison of developed schemes and achievements have been summarized. Besides, some limitations and the future direction in the relevant field have been described in this chapter.