ABSTRACT

In the growing world of technology, the revolution of digital information has made access and modifications of multimedia content very easy. Due to technological revolution, the digital media such as images, audios, videos etc. are gaining extensive importance and so their security and confidentiality issues are of great concern. Digital watermarking provides a way to secure the digital images in an effective manner. But, there are few issues in digital watermarking such as loss of information, which is not tolerable in some sensitive fields. Reversible data hiding is a technique to embed the secret information in cover images in such a way that at the receiver's end, original cover image is recovered bit by bit along with the exact recovery of embedded information. It is mainly used for content authentication. The aim of authentication is not only to secure the digital content from illegal modification or tampering but also to provide a way to maintain the content's integrity and privacy. In this thesis, we have investigated various novel and efficient reversible data hiding techniques for encrypted images which can be used to achieve the image security and . The main focus is to enhance and develop different data hiding and encryption techniques to secure embedded data as well as cover image during their communication through public network.

Among all the proposed techniques in literature, algorithms based on difference expansion belong to a traditional and effective class of reversible data hiding techniques. In this thesis, the first work is based on difference expansion. Under this category we explored three algorithms in encrypted images namely difference expansion using bilinear interpolation, difference expansion using Lagrange interpolation and difference expansion in medical

images to achieve higher embedding capacity along with their privacy and security. In this chapter, the motive is to elevate the embedding capacity and reduce the distortion effect caused by embedding with the help of difference error expansion based reversible data hiding method. This chapter investigates the use of bilinear and indexed Lagrange's interpolation by utilizing the pixels located at even rows and even columns for the prediction of neighbouring pixels. Further, this chapter introduces a simple technique to preserve the privacy of medical data with the use of difference expansion technique. In this method, the space for data hiding is created before encrypting the medical image, such that highly correlated pixels can be utilized well, leading to notable embedding capacity. The effectiveness of proposed works is analysed by comparing it with existing works, and it is found that our work has achieved higher security and performance.

The correlation of two adjacent pixels estimated by the difference expansion usually does not prove a better estimation of the spatial correlation. To improve it, a prediction error expansion method is introduced which uses more neighbouring pixels to exploit the correlation among the pixels. Using this idea in encrypted images, we proposed an odd-even discrimination based method which utilizes prediction error concept. The proposed method reserves room after encryption and converts prediction errors (PE) to odd and even numbers to discriminate between embedded and non-embedded pixels. This avoids the computational overhead caused by the use of a location map. The proposed scheme also employs double-layer encryption using random permutation and a stream cipher to secure the cover images. The method is separable, which means that the secret data and cover image can be independently extracted and recovered, depending on the availability of

the data hiding and decryption keys. The scheme uses block-wise reference pixels for the calculation of PE, that enhances the payload capacity. Experimental results indicate that the proposed scheme is more effective than existing state-of-the-art works.

Further, histogram bin shifting and lossless compression that are two important methods in reversible data hiding are explored in encrypted domain. In the first technique, a simple iterative method which combines encryption and embedding schemes to increase the embedding capacity and security is proposed with the use of two side histogram shifting with reference to the peak point.
In the second technique, a selective bin model based reversible data hiding in encrypted images is proposed. The scheme focuses on enhancing the embedding capacity while ensuring the security of images with the help of encryption and the proposed data hiding process. For data embedding, lossless compression is utilized and the image is classified into three bins. Then, marker bits are assigned to these bins to distinguish between embeddable and non-embeddable regions. The proposed method shows a satisfactory embedding rate for smooth images as well as complex ones due to its selective bin approach. Also, the method is separable in nature i.e., data extraction and image recovery can be performed independently. Furthermore, the experimental results demonstrate the effectiveness of strategy when compared with others.

From the literature, it is evident that there are many different schemes for reversible data hiding in spatial domain but very few contribute towards the transform domain. We explored two techniques in transform domain

using singular value decomposition and integer wavelet transform. In the first technique, the encryption is performed twice to provide the double layer security of transmitted media/ digital image using Mersenne Twister and Philox counter-based pseudo random number generator. The proposed work utilizes properties of singular value decomposition for the embedding of secret data.

In the second technique a novel reversible data hiding method in the encrypted domain utilizing the integer wavelet transform is presented. The proposed work first encrypts the images using random permutation method and then perform embedding by utilizing integer wavelet transform. For data embedding, encrypted images are decomposed into four sub-bands by applying integer wavelet transform. Both the schemes attain desirable results in terms of embedding capacity and security against malicious attacks and thus, can be applicable in many cloud based, computing and privacy protection fields effectively.

One of the emerging techniques of reversible data hiding in encrypted images is the use of cryptographic approaches along with data hiding methods. Moving in this direction, we proposed two methods using multi secret sharing scheme and key policy attribute based encryption for reversible data hiding in encrypted images. In the first method, a recent reversible data hiding in encrypted images based algorithm termed as shared one key (SOK) is improved by introducing modified difference expansion for encrypted images. In this, the data hider independently hides the data in an encrypted image without any need of an encryption key. By using the key sharing properties, secure communication between the owner and receiver has been established. Also, in the proposed method, the key is shared between the owner and receiver

utilizing the Diffie-Hellman key exchange algorithm, unlike the conventional key sharing system where a private channel is required to share the keys. In the second method, a reversible data hiding technique along with an encryption scheme which ensures privacy as well as the sensitivity of information associated with medical images is introduced. The proposed method enhances the security of medical images by integrating reversible data hiding with key policy attribute-based encryption. To provide a double layer of security in medical communication, the key policy attribute-based encryption scheme is used. The proposed technique is appropriately applicable where the governance of medical images requires an assurance in terms of data certainty, confidentiality, integrity, and reliability. The experimental results show the effectiveness of both the proposed methods in terms of security and embedding capacity when compared to other existing works.

The works presented in this thesis have been tested on various standard test images and experimental results have also been compared with recent existing techniques in the field of reversible data hiding in encrypted images. The presented techniques are novel, provide higher embedding capacity along with good visual quality and are also efficient in terms of computational cost as well as security. These techniques are beneficial in real world applications where confidentiality of digital images is important such as e-healthcare system, scientific research, military applications, legal documents and many more. But still there is a scope to increase embedding capacity while maintaining visual quality and the work can be extended for 3D mesh models also.