Chapter 2

LITERATURE REVIEW

2.1 Introduction

This being the information age, it is required to maintain information about every aspect of lives. During the last two decades, computer networks created a mutiny in the use of information. Sending and receiving information from a distance uses computer networks by legal recipient. The information needs to be masked from unauthorized access (confidentiality) protected from unauthorized change (integrity) and made available to a legal recipient only when it is required. Although the three previously mentioned requirements have not changed, they now have recent possibilities. When the information stored in a computer, it should not to be disclosed. There should also be away to sustain its confidentiality when it is transmitted from one computer to another [20].

Information transmitted over computer networks nowadays is not only text, but also audio, image, and other multimedia types. The field of multimedia security has matured in the last decade to provide a class of tool-sets and design insights for the protection and enhancement of digital media under a number of diverse attack scenarios. Research in multimedia security was first motivated, in part, by increasing use of digital means to communicate, store and represent entertainment information such as music and video. The digital form allowed the perfect duplication of information and almost seamless manipulation and tampering of the data. This created new types of security attacks not (as seriously) addressed in the past by the entertainment industry. The paradigm shift from analog to digital multimedia for entertainment has had an enormous impact for artists, publishers, copyright holders and consumers alike providing flexible and more accessible business models [12]. In such a setting, one natural question that arises is the security and confidentiality of a digital packet of multimedia information.
2.2 Different Encryption methods

Different cryptography methods are used to encrypt different data. This chapter, discuss the encryption of image information. With the Internet development, large volumes of binary data are processed every day. Text as well as audio was processed on a normal method. The digital multimedia data security distribution network is commonly provided by encryption. The mathematical process transforms a plaintext message into unintelligible ciphertext. Nevertheless, the classical and modern ciphers have all been developed for the simplest form of multimedia data, and are not appropriate or higher forms such as images and video with very bulky file sizes. Partial encryption is a modern approach to reduce the computational requirements for huge volumes of multimedia data in distribution networks with different client device capabilities. This chapter discusses the current issues and presents some future directions for existing methods. Presently, encryption appears to be the only technical tool that can be used to provide confidentiality in applications such as video conferencing, DSTV and on-line video games, which is also true of telemedicine application. The cost of multimedia data compression can be aggravated by the additional need for protecting digital copyright content.

2.3 Security Definitions

Minimum requirement of security is that entire text cannot be recovered in case to understand the type of algorithm with respect to ciphertext. The desirable properties are listed below.

- The secured information should be hard to recover the messages from the ciphertext when the messages are drawn from arbitrary probability distributions defined on the set of all sequences.
- The secured data must be hard to compute partial information about messages from the ciphertext.
- The above properties should hold with high probability.

In short, it would be desirable for the encryption scheme to be the mathematical analogy of opaque envelopes containing a piece of paper on which the message is
written. The envelopes should be such that all legal senders can fill it, but only the legal recipient can open it.

2.4 Literature Survey

An important role for an Image encryption is to make sure that to maintain confidentiality during transmission and storage of images over network. The privacy of the encrypted data with a balance in time and the challenge faced in image encryption is the cost efficiency of the encryption.

N. Bourbakis, and C. Alexopoulos [22], proposed the wide range of sequential accessing patterns that are produced by SCAN grammar, allows the consideration of a SCAN word as an encryption key bound to a given 2D image array. The formal definition of the SCAN languages and describe the underlying method for spatial access [23].

N. Bourbakis [24] provide an efficient image compression-encryption methodology by using fractals. The methodology is based on the principles and ideas reflected by the family of fractal based languages and is mainly motivated for the compression and encryption of 2-D digital images. The Scan methodology can be used either as lossy or lossless compression scheme.

S. S. Maniccam, N. G. Bourbakis,[25] Proposed a method for image and video encryption and a first stage lossy video compression based on frames difference before the encryption. First stage compression-based frames differences and encryption of video whose compression error can be bounded pixel wise by a user specified value, very large number of encryption keys, and ability to encrypt large blocks of any digital data. The compression and encryption schemes are based on SCAN patterns or space filling curves generated by a two dimensional spatial accessing methodology called SCAN. This distinct advantage of lossless compression and encryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. The drawback of the methodology is that compression-encryption takes longer time [26].

H. Cheng et. al [27,28] proposed partial encryption for quadtree compression. This method notably reduces encryption and decryption time without affecting the
compression performance of the underlying compression algorithm. Here the compression output is partitioned into two parts: first part is important part and second part is unimportant part. A major amount of information is available in the important parts, whereas unimportant parts may not provide much information without important parts. Encryption will only perform for important parts.

Podesser et al [29] proposed selective bit plane encryption using AES. In this method several experiments were conducted on 8 bit grayscale images, and the results for this method as follows:

- Encrypting only the MSB is not secure, a replacement attack is possible
- Encrypting the first two MSBs gives hard visual degradation, and
- Encrypting three bit planes gives very hard visual degradation.

This scheme is not tunable as fixed numbers of bits are encrypted. For 8 bits per pixel uncompressed image, hard visual degradation (of 9 dB) can be observed for a minimum of 3MSB bits encrypted. This scheme is intended for uncompressed data. Encryption can increase data size so it is not compression friendly. This scheme is format compliant because encryption is performed before compression. Security achieved in this method is medium.

In [30,31] proposed for uncompressed image, which applies to a binary image, combination of image data and a message (key) that has the same size as the image; a XOR function is enough when the message is used only once. A simplification to gray level images is uncomplicated: each bitplane encrypt independently and restore gray level image. With this approach no dissimilarity between bitplanes is initiated even though the subjective relevance of each bitplane is not equal. The uppermost bitplanes show evidence of some resemblance with the original image, but the LSBs look arbitrary. Because encrypted bits also look arbitrary, noise is added to the original image after encryption of least significant bitplanes. This scheme is tunable and very high visual degradation can be achieved by encrypting 4 to 5 bitplanes. This technique is used for uncompress image so no impact is observed on efficiency of compression.
Zeng and Lei [32] proposed selective encryption in the frequency domain (8x8 DCT and wavelet domains) is proposed. In Wavelet transform case, the proposed scheme consists of Selective bit scrambling and Block shuffling. The selective bit scrambling is a biplane selective encryption. Here each coefficient bitplane is partitioned into a sign bit separately, which is extremely random and neighboring coefficient sign bits are uncorrelated, so it is greatly unpredictable. Then significance bits (the first nonzero magnitude bit and all subsequent zero bits if any), these give a range for the coefficient value. These bits have low entropy and thus are extremely compressible. Ultimately, the alteration bits are uncorrelated with neighboring coefficients and allocated arbitrarily. The proposed method scramble the sign bits to arbitrarily and alteration bits. The algorithm is not specified for encryption.

In Block shuffling, the basic initiative is to shuffle the arrangement of coefficients within a block in a way to preserve some spatial correlation; this can achieve enough security without negotiating the compression efficiency. Each subband is split into equal-sized blocks (the block size can be different for each subband). Within the same subband, block coefficients are shuffled as said by a shuffling table generated using a secret key (this table can be different from a subband to another or from one frame to another). Since the shuffling is block based, it is expected the atmost 2D local subband statistics are preserved and compression not greatly impacted. The 8x8 DCT coefficients can be measured as entity narrow frequency components situated at some subband. The block shuffling and sign bits change can be applied on these “subbands.” I-, B- and P-frames are processed in different manners. For I-frames, the image is first split into segments of macroblocks (e.g., a segment can be a slice), blocks/macroblocks of a segment can be spatially disjoint and chosen at random spatial positions within the frame. Each segment surrounded by DCT coefficients at the same frequency location are shuffled together (in order to preserve coefficients distribution property). Then, sign bits of AC coefficients are changed erratically and DC coefficients are turn over with particular threshold. There may be many intracoded blocks in P- and B-frames. At least DCT coefficients of the same intracoded block in P- or B-frames are shuffled. Sign bits of motion vectors are also scrambled.
A syntax compliant encryption algorithm is proposed for H.264/AVC in [33]. Encryption is placed within the encoder. A selected compliant codewords are permuted arbitrarily with other compliant codewords to accomplish syntax compliance. AES counter determine the shift permutation. The major shortcoming of this scheme is the lack of cryptographic security. Indeed, the security of the encrypted bitstream does not depend more on the AES cipher. It depends on the size of the compliant codewords. Hence, the diffusion of the AES cipher is reduced to the plaintext space size. Additionally, a bias is introduced in the ciphertext. This bias depends on the key size and the plaintext space size. The proposed scheme does not provide accurate values for overall encryption ratio. However, it is mentioned that about 25% of I-slices and 10–15% of P-slices are encrypted. Since intra-coded slices can represent 30–60%, the encryption ratio is predictable to be relatively high.

Grangetto et al. [34] proposed a randomization of the arithmetic coder. This is accomplished by randomly swapping the most probable symbol (MSP) and least probable symbol (LSP) intervals. Since only the interval magnitude is important for encoding, the compression performance remains unchanged. The complete encryption and selective encryption are achievable by choosing the layers or resolution levels to encrypt. Selective region encryption is made possible since JPEG2000 is a code block based algorithm. To apply the encryption on the code blocks contributing to confines of the region considered for encrypt a region of interest. The, brute force attack is feasible because of low security

Yang Ou et. al. in [35], proposed two novel region-based selective encryption schemes for medical imaging. The first method is to invert the first two MSBs of ROI coefficients in wavelet transform domain arbitrarily. It can be implemented smoothly and only acquire little compression efficiency overhead, also it can be enlarged to other motion formats. The second method, selective encryption of the compressed Region of Interest (ROI) data, offers a high level security and has no file size changes. Both of them are format backward compatible and have their own improvement so that they are appropriate for different medical security imaging systems to convince different prerequisite.
Abugharsa et.al. [36] Proposed an image encryption method based on shifting rows and columns of image. Using a shifting table that is generated by hash function, the original image is divided into block of 3 x 3 pixels. To encrypt the blocks of an image are further shifted through rows and columns. The security is high because of the highest value of entropy.

The color space rotation consists of three stages proposed in [37]. Converting the color image from RGB space to RGB compleent space through rotating the color space of original color image. Then the individual color component is transformed using their proposed reality preserving fractional Mellin transform on different fractional orders of the image. Ultimately the scrambling of pixels is done three dimensionally to achieve high security.

The orthogonal composite grating and double random phase encoding for single channel color image encryption scheme was proposed in [38]. The partial encryption schemes dissimilar than the fully layered encryption schemes, significant regions are encoded in a given image. Confidentiality and computational necessities without tradeoffs are the main advantage of the partial encryption technique.

AES stream ciphering using variable length coding (VLC) of the Huffman’s vector proposed by Rodrigues et al. [39]. First, the input image is divided into blocks of 8x8 pixels. Second, each block is transformed from the spatial domain to the frequency domain using discrete cosine transform (DCT). Third, the quantization is applied on the resultant image using Zigzag scan method then applying AES encryption method. The advantages of this scheme [27] is that there is the likely to recognizing one or two regions for each block of 8x8 pixels, it can be obtained by using used the AES in CFB (Cipher Feedback Block) mode, and have applied it over each block. The ROI must be defined in unit of block of 8x8 pixels as a default of JPEG format, it is one of the essential point in this method. This method is high sensitivity to a small change in secret key Because of large key space.

The advanced encryption standard AES-Rijndael proposed in [40] based on five criteria, there are block sizes, plain data compression, software implementation optimization, selectable round and whole routine selection strategy. These criteria
form the basis of their so called selective encryption technique, which is an improvement of the AES algorithm. Execution time is reduced to 50% and the entropy value is about 7.9892 using this method, so the security level is average.

To encrypt selected blocks that contain edges based on DCT transformation and scalable lightweight encryption technique proposed by yekkala et al. [41]. Selected blocks are encrypted by make use of the threshold values at a meticulous range and if the blocks are not comes into a particular range are unencrypted, this is the basic idea of this selection approach. The average computation time because of the huge area specified by 43%, used for encryption.

Brahimi et al. [42] proposed a novel selective encryption of image plane based on JPEG2000 for encrypting the code-blocks corresponding to some sensitive terrain. To improve the security using the permutation of blocks code are chosen in the area selection. The combined permutation and selective encryption methods are used to reduce the amount of data processed. Security is good when the encrypted image is free from the original image because PSNR has very small value.

*Nidhi S Kulkarni et. al.*[43], the proposed encryption technique reduces intelligent information in an image by scrambling the image first and then changing the pixel values. The scrambling arrangement is done with the help of a random vector and the pixel values are changed by a simple substitution method which adds confusion and diffusion property to encryption technique. This method can be used for any kind and any size of gray level images. Tunability of this scheme is not specified. These methods accomplish high visual degradation. It is compression friendly as well as rapid speed. If all the bits are encrypted, so 100% encryption ratio is achieved. Moderate level of security is obtained. Security is increased against the brute force attack.

Younis [44] proposed a new encryption method; an important part of image level two sub band is used by employing fuzzy c-means (FCM), an advanced technology for clustering analysis combined with the permutation cipher. The encryption algorithm include: wavelet packet transform, quantization by FCM, permutation cipher and arithmetic coding to level two sub-band images. This method produces an average
level of security because of the reconstructed image of the PSNR value is large. Threat is reduced because of large key space.

Flyah et al. [45] proposed an efficient partial image encryption technique that employs three levels of the discrete wavelet transform (DWT) with the AES cipher and stream cipher. The image is smoothened using a smoothing filter in order to mask details of cipher image so that perceptibility of the encrypted regions in the image is reduced. It is studied that the reconstructed image is almost the same as the original image.

In [46], proposed a technique that applies the Arnold Cat map permutation on low frequency sub-band of the DCT transformed image for encryption. Basic idea for selecting the low frequency sub-band of the DCT transformed image is attributed to the fact that the human visual system is more drawn to information at the lower frequencies than the higher frequency information. Important information such as object, shape, etc. is presented in low frequency sub-bands, while the detailed information is contained in higher frequency sub-bands. The decrypted image shows some presence of noise it can be considered as robust against noise to some extent.

A novel solution for selective encryption to achieve data security and privacy proposed by Priyanka et. al [47]. This method uses two fold contributions to achieve data protection in less time to save computational energy. Segmenting the multimedia data by reducing the encrypted data volumes using the grid division and diagonal selection. To reduce the complexity of the operation and protect the data in a reasonable computational cost with the help of symmetric key algorithm. From observation this method is appropriate for real-time applications.

A JPEG2000 lightweight encryption scheme is proposed by Engel et. al in [48]. Only lower resolutions are compressed with classical dyadic ripple transform. For higher resolutions, the algorithm relies on a secret transform domain constructed with anisotropic wavelet packets (AWPs). The objective of this method is to permit transparent encryption for applications requiring low-resolution sample. Therefore, low resolution is reachable by all users and decodable with any JPEG2000 compliant codec, limited adjustability is permitted. Only lightweight concealing is allowed.
Indeed, this algorithm does not allow concealing lower resolutions. It offers poor error tolerance since any error in the encrypted parameters for generating random AWP would severely impact the decoding of the bitstream.

Loic Dubois et. al. in [49], proposed a new approach for the selective encryption of video. In SSE-CAVLC, they have added a guessing system of the decoded frame with an implementation of measures which decides whether to encrypt a given MB. Thus only the essential MBs are encrypted while keeping a global final PSNR under the predefined threshold. Indeed, this approach allows encrypting only a small percentage of the bitstream. Though, this method requires some added computations in the H.264/AVC encoder in order to analyze the confidentiality of the current MB. To compute, SSE-CAVLC is a solution to the key problems which are data protection and adequate confidentiality.

Khashan et al. [50] provides an general analysis of selective image encryption based on edge and face detection methods using the Blowfish symmetric cipher. The majority cram of this domain use pixels based permutation with chaos-based techniques and other random permutation methods. However, while such encryption schemes are efficient, the security levels are unlikely to compete with those provided by standard ciphers, which are less affected by attacks. Thus, selective encryption of visual images based on symmetric ciphers is a more acceptable trade-off between security and performance. This method demonstrates the computational time taken by the different processes executed during image encryption using a symmetric cipher. The results obtained reflect a considerable reduction of computational time for selective encryption methods on still visual images compared to full encryption.

Upendra Bisht and Shubhashish Goswami [51] present an analysis and implementation of selective image encryption algorithm using matlab. In this algorithm the confusion and diffusion technique is used which means that each pixel of the input image is swapped by a new value. The value will be generated by random number generator. Those random numbers will be XORed with the original image pixels gives selective encryption of an image.
A fast partial image encryption scheme using RC4 stream cipher and Discrete Wavelet Transform (DWT) proposed in sasidharan et. al. [52]. The encryption is carried out at the lowest frequency band using the stream cipher is proposed. To retain all the image information is their basic idea of the stream cipher. However, using the stream ciphers consumes more time, since it typically encrypts one byte at a time. The bitwise exclusive-OR is used to combine between key stream and original image while the former is produced by arbitrary numbers. When edges are encountered, a shuffling algorithm is employed. To diminish the encryption time by encrypting only the lowest frequency band of the image and maintains a high level of security by shuffling the rest of the image using the shuffling algorithm with a large key space value of about 2256. It can be observed in [36] that the entropy result of the encrypted image, which is about 4.7807, provides a freer platform for an intruder to decipher the secret key used to encrypt the image. But it is strong against statistical attack because PSNR has high value, about 20.7056dB.

Kuppusamy et al. [53] proposed a partial image encryption optimization scheme using high energy coefficients of the transformed image, which were selected by employing the particle swarm optimization (PSO) technique. Because of large key space produces to the average level of security. This method gives medium speed for encryption for encrypting vicinity of the image is about 33%.

Applying a selective encryption approach before compression can significantly affect the statistical and structural properties of an image. Moreover, it generates extra overhead during compression and hence results in severe limitations in image compressibility proposed by [54-55].

Selective image encryption schemes can be obtained during the compression stages. A JPEG image is the most standard compression scheme used to represent an image to greatly save the storage space and the transmission band of the images. Therefore, it has been widely explored in research for protection. Moreover, encryption can be combined with the entropy-coding phase into a single step, hence reducing the computational time and maintaining format compliance and compression rates. These approaches similarly split an image into non-overlapping pixel blocks [56-58].
The detection output is a binary image with only two values (1 or 0) for each pixel, with 1 reflecting a significant pixel and 0 the opposite. Consequently, the blocks that contain edges greater than a specified threshold are identified for subsequent encryption using different encryption ciphers, for both the spatial and transmission domains. Although the level of security in each scheme is based on the encryption cipher used to encrypt the indicated significant parts on an image, it generally provides an acceptable perceptual security level [59-63]. However, very few of the presented schemes have proved the performance efficiency of the combination of edge detection and encryption operations, or compared it with a full encryption approach.

2.5 Performance Parameters

The parameters listed below are gathered from literature for evaluating and comparing partial image encryption schemes [64-69].

- **Tunability (T)**
  It is very much desirable and defines dynamically the encrypted part and the encryption parameters with respect to different applications and requirements. These parameters limit the usability of the scheme to a restricted set of applications.

- **Visual Degradation (VD)**
  It measures the perceptual distortion of the image data with respect to the plain image. It is desirable to achieve enough visual degradation in many applications, so that an attacker would still understand the content but prefer to pay to access the unencrypted content. Sensitive data (e.g., military images) also requires high visual degradation to completely disguise the visual content.

- **Compression Friendliness (CF)**
  A Partial encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some partial encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase.
Table 2.1: Summary of related work with respect to each criterion

<table>
<thead>
<tr>
<th>Ref</th>
<th>Tunability</th>
<th>Visual degradation</th>
<th>Compression Friendliness</th>
<th>Format Compliance</th>
<th>Encryption Ratio</th>
<th>Speed</th>
<th>Cryptographic Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>[27],2000</td>
<td>No</td>
<td>Satisfied</td>
<td>Satisfied</td>
<td>No</td>
<td>depending on content</td>
<td>Fast</td>
<td>not satisfied</td>
</tr>
<tr>
<td>[28],2002</td>
<td>No</td>
<td>High</td>
<td>Yes</td>
<td>No</td>
<td>depending on content</td>
<td>Fast</td>
<td>Low</td>
</tr>
<tr>
<td>[29],2002</td>
<td>No</td>
<td>High</td>
<td>No</td>
<td>Yes</td>
<td>&gt;37.5%</td>
<td>Fast</td>
<td>Medium</td>
</tr>
<tr>
<td>[30],2002</td>
<td>Yes</td>
<td>High</td>
<td>Yes</td>
<td>No</td>
<td>50-60%</td>
<td>Fast</td>
<td>Low</td>
</tr>
<tr>
<td>[32],2003</td>
<td>No</td>
<td>High</td>
<td>Compression drop &lt;5%</td>
<td>Yes</td>
<td>20%</td>
<td>Fast</td>
<td>Low</td>
</tr>
<tr>
<td>[33],2005</td>
<td>No</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>depending on content</td>
<td>Fast</td>
<td>low</td>
</tr>
<tr>
<td>[34],2006</td>
<td>Yes</td>
<td>Variable</td>
<td>Yes</td>
<td>Yes</td>
<td>Variable</td>
<td>Fast</td>
<td>low</td>
</tr>
<tr>
<td>[48],2006</td>
<td>No</td>
<td>High</td>
<td>No</td>
<td>No</td>
<td>High</td>
<td>Fast</td>
<td>High</td>
</tr>
<tr>
<td>[35],2007</td>
<td>Unspecified</td>
<td>Satisfied</td>
<td>Yes</td>
<td>Unspecified</td>
<td>depending on content</td>
<td>Fast</td>
<td>High</td>
</tr>
<tr>
<td>[43],2008</td>
<td>Unspecified</td>
<td>High</td>
<td>Yes</td>
<td>Unspecified</td>
<td>100%</td>
<td>Fast</td>
<td>moderate</td>
</tr>
<tr>
<td>[44],2009</td>
<td>Unspecified</td>
<td>Variable</td>
<td>Yes</td>
<td>Unspecified</td>
<td>6.25% to 25%</td>
<td>Fast</td>
<td>moderate</td>
</tr>
<tr>
<td>[40],2010</td>
<td>Unspecified</td>
<td>Satisfied</td>
<td>Yes</td>
<td>Unspecified</td>
<td>&gt;35%</td>
<td>Fast</td>
<td>High</td>
</tr>
<tr>
<td>[49],2011</td>
<td>No</td>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
<td>Variable</td>
<td>Fast</td>
<td>High</td>
</tr>
<tr>
<td>[53],2012</td>
<td>Yes</td>
<td>High</td>
<td>Yes</td>
<td>Unspecified</td>
<td>Variable</td>
<td>Fast</td>
<td>High</td>
</tr>
<tr>
<td>[78],2013</td>
<td>Yes</td>
<td>High</td>
<td>Yes</td>
<td>Unspecified</td>
<td>Variable</td>
<td>Fast</td>
<td>High</td>
</tr>
</tbody>
</table>

➢ Format Compliance (FC)

The aim of format-compliant encryption is to preserve carefully the selected parts of the information in the codestream so that the encrypted data is compliant to the format of the unencrypted data. If format compliance is desired, the classical cryptographic approach cannot be employed as no information is preserved. In many cases, header information is left in plaintext and the actual visual information is encrypted avoiding
the emulation of marker and header sequences in the ciphertext parts. In this manner the properties of the original codestream carry over to the encrypted stream. For example, rate adaptation may be done in the encrypted domain easily, provided the original codestream facilitates this functionality (which is true for scalable or embedded codestreams, for example). Headers are not encrypted in most approaches proposed to date they may be encrypted in a format-compliant way as well [70].

- **Encryption Ratio (ER)**

  This criterion measures the amount of data to be encrypted. Encryption ratio has to be minimized to reduce computational complexity.

- **Speed (S)**

  In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real-time requirements.

- **Cryptographic Security (CS)**

  Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-ciphertext attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security.

This chapter has presented a survey and classification of a number of encryption schemes in the literature. The key harms related among the majority of existing methods are inadequate security, lessen the compression performance and insignificant computational reduction with respect to total encryption. There are also a lack of bit stream compliance and increase in encryption key size. Future directions of research include more emphasis on key management, resolving the conflict between encryption, and compression and determining the approaches to change the criteria for selection dynamically. The most effective methods of cryptography are separated in frequency and spatial domain. All of these methods indicate that a development of purely partial image encryption being external to the digital computer domain have not yet made impact on sufficient. There is extensive fracture for investigating purely partial image encryption techniques to enhance image and multimedia encryption and
Investigation on Partial Image Encryption Methods

security over communication and computer network links. Different parameters are used to explore features of existing partial encryption schemes.

To reduce the computational necessities of investor devices in real-time applications one of the techniques is Partial encryption, which is a process of encrypting only parts of the data. This chapter presented a survey and classification of the proposed schemes in the open literature. The advantage of partial image encryption is that well studied encryption algorithms can be used for encryption and so if the parts to be encrypted are carefully chosen, high security can obtained.

The next chapter in this thesis concentrates the methodologies adopted for the proposed partial image encryption techniques.