Chapter 1

Introduction

Image information security plays a vital role in computing and communication due to fast update technologies. Encryption is one way to secure image information. A brief idea about information in an image is explained in preamble section. Various existing image encryption and decryption techniques are discussed in literature review. Problem formulation and organisation of the thesis is discussed in last section.

1.1 Preamble

Images, one typical type of two dimensional data, are considered to contain a huge amount of information, for example a family photo with grandmother, grandfather, mother, father, brother, sister, son and daughter. It gives approximate information about the age of each, their heights, colors and similarity between grandfather, father and son. Because the information contained in a digital image and the information might be inferred beyond a digital image, it is very important to protect this information from any unauthorized use. One way of protecting digital images is called image scrambling,
which disorders pixel relationship in the original image so that the scrambled image with rearranged pixels become unintelligent and unrecognizable. On the other hand digital image is a massive two-dimensional data. The smallest unit of an image is a pixel. In a digital image, each pixel represents a different level of color intensity. According to the capacity of human visual perception in distinguishing different levels of intensity, the entire range of intensity is divided into 256 levels (gray scale image). Thus, the level of intensity in each pixel has a value between 0 and 255. This range is demonstrated by a byte (8 bits). Therefore, each pixel is equal to one byte. However, due to large data size, it is not reasonable to use conventional encryption methods. The basic idea of encryption is to modify the message in such a way that its content can be reconstructed only by a legal recipient.

Today's technology can be traced back to earliest ciphers, and have grown as a result of evolution. The initial ciphers were cracked, so new, stronger ciphers emerged. Code breakers set to work on these and eventually found flaws, forcing cryptographers to invent better ciphers and so on. With the advent of the computer age, the mechanical encryption techniques were replaced with computer ciphers. They operated according to the same principles of substitution and transposition (where the order of letters or bits are altered). Again each cipher depended on choosing a key, known only by the sender and the receiver which defined how a particular message would be. This meant that still there was a problem of getting the key to the receiver so that the message could be deciphered. This had to be done in advance, which was an expensive slow and risky process.

Encryption (sometimes called as encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment). Encryption and
decryption process is as shown in figure 1.1.

Figure 1.1: Block Diagram of Image Encryption and Decryption Process

1.2 Motivation of the Thesis

Considerations of privacy and confidentiality in a computer environment have given recognition to the need for protecting certain communications and stored data from theft and misuse. A suitable methodology for protecting communicated or stored data involves the use of cryptographic techniques. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. A message is plaintext. The process of disguising a message in such a way to hide its substance is encryption. An encrypted message is cipher text. The process of turning cipher text back into plain text is decryption. Basic operations that can be carried out in encryption/decryption are: substitution and transposition. Due to advent of computers, these operations are carried out on binary bits.

The field of encryption is becoming very important in the present era in which information security is of utmost concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet commu-
CHAPTER 1. INTRODUCTION

communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable.

1.3 Literature Survey

Fundamentals of digital image processing are referred in [1–4]. Cryptography and encryption techniques are referred in [5–7]. Liu et. al [8] proposed image encryption by using gyrator transform and Arnold transform. Arnold transform (ART) scrambles the matrix-pixel sequence by encoding a single parameter and forms color noise-like image, and reduces key space for storage and transmission applications. GuoQ et. al [9] Color image encryption by using Arnold and discrete fractional random transforms in IHS space. The color image encryption method using discrete fractional random transform (DFRNT) and ART in the intensity-hue-saturation (IHS) color space has been proposed. In this technique, a color image is transformed into IHS color space and I component is encrypted by DFRNT whereas H and S components are encrypted using ART. LiuZ et. al [10] proposed color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains. The color image encryption using Arnold transform and color-blend operation in discrete cosine transform(DCT) has also been presented. In this method, Arnold transform scrambles the pixel position of the blocked sub images of original image at local area, color-blend operation defined by a 3x3 matrix(random angle) exchanges and mixes ran-
randomly scrambled RGB components and finally twice in DCTs encrypt the resulting image. Zhengjun Liu et al. [11] proposed Double image encryption by using Arnold transform and discrete fractional angular transform. Two original images are regarded as the amplitude and phase of a complex function. Arnold transform is introduced for scrambling the pixels at a local area of the complex function. Subsequently the changed complex function is converted by discrete fractional angular transform. The operations mentioned will be performed many times. S.S. Maniccam and N.G. Bourbakis [12] have presented a new methodology which perform both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. Chao-Shen Chen and Rongjain Chen [13] proposed an image encryption and decryption algorithm based on SCAN methodology. SCAN is a language-based two dimensional spatial-assessing methodology which can efficiently specify and generate a wide range of scanning paths. Here scanning path sequence fill the original image to generate the encrypted image. C. Kachris et al. [14] have designed a detailed architecture for SCAN algorithm. Two basic techniques to obscure high redundancies and strong correlations are confusion (substitution) and diffusion (permutation). Confusion increases the complexity between the key and the cipher text and bans all attempts to study the cipher text for redundancies and statistical patterns. Diffusion, on the other hand, spreads the redundancy of the plain text over the entire cipher text, thus decreasing redundancy. While either of these techniques alone is highly susceptible to being cracked, they generally make an excellent security solution when combined. Images, however, have various intrinsic features, such as bulk data capacity and high correlation among pixels, that render traditional encryption algorithms such as DES, IDEA and RSA unsuitable [15, 16]. Xindyuan
Wang et al. [17] presented a novel chaotic image encryption algorithm based on water wave motion and water drop diffusion models. Secret keys will be processed by key generator before they can really be used in the encryption scheme, and in this stage this paper associates plain image with secret keys; Secondly, by imitating the trajectory of water wave movement, encryption algorithm will do scrambling operations to the image. Finally combines water drop motion and dynamic look up table to realize diffusion operations. For an 8 bits pixel, this algorithm will just dispose the higher 4 bits, which is because the higher 4 bits contain the vast majority of information of the image. Ruisong Ye [18] presented a novel chaos based image encryption scheme with an efficient permutation diffusion mechanism. Generally permutation diffusion mechanism permuting the positions of image pixels in order to reduce the high correlation between adjacent pixels of plain image and change the pixel value in diffusion stage. In the permutation process, a generalized Arnold map is utilized to generate one chaotic orbit used to get two index order sequences for the permutation of image pixel positions; in the diffusion process, a generalized Arnold map and a generalized Bernoulli shift map are employed to yield two pseudo-random gray value sequences for a two-way diffusion of gray values. Encryption scheme is easy to manipulate and can be applied to any image with unequal width and height as well. Ahmed A. Abd El-Latif et al. [19] have proposed a hybrid chaotic system and cyclic elliptic curve for image encryption and provides a external secret key of 256 bit and one generalized chaotic logistic map. Using the cyclic elliptic curve to derive generated key stream are mixed with key sequences. Xingyuan Wang [20] has proposed a novel color image encryption algorithm based on chaos. They uses chaotic system to encrypt the R, G, B components of a color image at the same time and makes these three components effect each other. So it can reduces correlation between R, G, B components and security is increased and mixed with plain image. Vinod patidar et.al [21] presented a secure chaotic based permutation-substitution scheme of image encryption. This
is loss-less symmetric block cipher. They are used secret key of length 161 bit and this key can be used as initial condition and system parameter of chaotic map. Number of rounds depends on secret key. To increase the speed of encryption they convert 3D image matrix into 2 D image matrix. Permutations are done by row by row and column by column using pseudo random number sequence generated from chaotic sequence. In substitution process uses chaotic sequence and initial vector depends on secret key and mixed with plain image. Chong FU et.al [22] presented a novel chaos based bit level permutation scheme for digital image encryption and provides a fast and high security. To overcome the drawbacks of conventional algorithms they propose significant diffusion effect in permutation procedure through a two stage bit level shuffling algorithm. Arnald cat map and chaotic sequence are used for shuffle all bit planes. This method decreases computational complexity and real time image communication applications. Yue wu et al [23] have presented image encryption using the Sudoku matrix. Sudoku matrix define as no two digits in the same block can be aligned in the same row, column or box. Encryption of the image consists of three stages. In first stage, a reference Sudoku matrix is generated and it is used for scrambling process. The image pixels intensities are then changed by using the reference Sudoku matrix values, and then the pixels positions are shuffled using the Sudoku matrix as a mapping process. So using this matrix we can encrypt any digital images such as binary images, gray and RGB images. Logistic map used for control the size of Sudoku matrix. Yue Wu.et al [24] have proposed a novel Latin square image cipher. Provides a 256 bit key length for generating s Latin square and generates 256x256 square image and it looks like Sudoku matrix that is no two digit in the same block can be aligned- in the same row, column or box. LSIC achieve many desired properties of a secure cipher including a large key space, high key sensitivities, uniformly distributed cipher text, excellent confusion and diffusion properties, semantically secure, and robustness against channel noise. Yue Wu.et.al [25] have presented Sudoku
associated two dimensional bijections for image Scrambling. Sudoku configuration provides us a new alternative way of matrix element representation by using block-grid pair besides the conventional row-column pair. and also discovers six more representations by using row digit pair, digit row pair, column digit pair, digit column pair, digit block pair, block digit pair associated with a Sudoku matrix. Sudoku Associated Image Scrambler only using Sudoku associated two dimensional bijections for image scrambling without bandwidth expansion. The Duc Kieu et. al [26] have proposed a Sudoku based wet paper hiding scheme in which a secret key has been used to randomly select a subset of pixels from a cover image as dry pixels. Then a total automorphism is applied to the cover image to maximize the number of dry pixel pairs and each secret digit in the base-9 numeral system is embedded into one dry pixel pair. Chin-Chen Chang et. al [27] have presented a Sudoku based secret image sharing scheme to lossless reveal of secret image. And also their approach derives the secret shadows and generates the meaningful shadow images by adopting the Sudoku. Rohan Shetty et. al [28] have proposed a information scheme using Sudoku puzzle in which they used Sudoku solutions to guide cover pixels to modify pixel values so that secret messages can be embedded. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the messages, such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the cipher-text. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. A novel method of generating self-invertible matrix is proposed which can be used in Hill cipher algorithm [29]. Hill cipher is a type of mono alphabetic poly graphic substitution cipher. A novel method of generating self-invertible matrix is proposed which can be used in Hill cipher algorithm [30]. In this paper they try to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the matrix is not invertible.
Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use self-invertible key matrix for encryption [31]. Panigrahy, S.K .et al [32] have implemented image encryption using Self-Invertible key matrix of Hill Cipher algorithm. Han Shuihunaet. al [33] proposed the an asymmetric image encryption based on matrix transformation. How to adapt certain matrix transformation to create a novel asymmetric block encryption scheme and a scheme is especially useful for encryption of large amounts of data, such as digital images. First, pair of key are given by using matrix transformation; Second, the image is encrypted using private key in its transformation domain; Finally the receiver uses the public key to decrypt the encrypted messages. Ismet Ozturk et. al [34] have discussed the analysis and comparison of image encryption algorithms. And they classify the image encryption methods in to three major types: position permutation, value transformation and visual transformation. Mitra et. el [35] have presented a new approach for image encryption using combination of different permutation techniques. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. S. R. M. Prasanna et. el [36] have presented an image encryption method with magnitude and phase manipulation using carrier images. Here, they used the concept of carrier images and one dimensional Discrete Fourier Transform for encryption purpose and it deals with private key cryptosystem, works in the frequency domain. Sinha, K. Sing [37] proposed the technique for image encryption using digital signature. The digital signature of the orthogonal image is added to the encoded version of the original image. The encoding of image is done using Bose-Chaudhuri Hocquenghm (BCH) code. The digital signature are created and verified by means of cryptography . Komal D Patel, Sonal Belani have presented [38] a survey on existing work which is used different
techniques for image encryption and also given a general introduction about cryptography. There are several methods for image encryption with some advantages and disadvantages. H. S. Kwok et. al [39], a fast chaos-based image encryption system with stream cipher structure is proposed. In order to achieve a fast throughput and facilitate hardware realization, 32-bit precision representation with fixed point arithmetic is assumed. Chen T-H et. al [40] proposed the efficient multi-secret image sharing based on Boolean operations (n+1, n+1) visual secret sharing (VSS) is used to encode (encrypt) a secret image into n meaningless share images to be superimposed later to decode (decrypt) the original secret by human visual system after collecting all n+1 secret images. Pareek NK et al [41] explained the concept of image encryption using chaotic logistic map and verity of encryption methods are developed for image encryption using this chaotic map.

G. situ et. al [42,43] was proposed Multiple image encryption (MIE) algorithm and researched in recent three years. The advantage of MIE is that it can encrypt many images synchronously, a MIE scheme with wavelength multiplexing and position multiplexing. However, a cross-talk effect exist in the paper and decrypted images are not perfect at the aspect of quality. Jianhua Wu et. al [44] presented four image encryption method based on spectrum truncation, chaos and the MODFrFT. With the help of spectrum truncation, the spectra of four images gotten by the discrete cosine transform (DCT) are truncated and combined into a single array sequentially encrypted by the MODFrFT. The combined spectrum array is encoded with the MODFrFT twice and chaos is introduced to scramble the phases of complex matrix before each MODFrFT. The technology of rate-distortion control is introduced to balance the qualities of the decrypted images. Zhengjun Liu et. al [45] presented optical multi image encryption based on frequency shift and fractional fourier transforms. Lower frequency parts of the original images are selected, frequency shifted and encrypted by using double phase encoding in fractional Fourier domains. Multiple images are encrypted together into a single one
and it provides high optical efficiency. Nanrun Zhou et al. [46] proposed a novel single channel image encryption algorithm based on chaos and fractional Fourier transform. The colors of the original color image are converted to HSI (hue-saturation-intensity), and the S component is transformed by the random-phase encoding based on FrFT to obtain a new random phase. The I component is transformed by double random-phase encoding based on FrFT using the H component and the new random phase as two phase plates. Then chaos scrambling technology is used to encrypt the image, which makes the resulting image non-linear and disorder both in spatial domain and frequency domain. Zhengjun Liu et al. [47] proposed a triple image encryption scheme by use of fractional Fourier transform. Original image is encoded in amplitude part and other two images are encoded into phase information. The key of encryption algorithm is obtained from the difference between the third image and the output phase of transform. In general case, random phase encoding technology is not required in the proposed algorithm. Moreover, all information of images is preserved in theory when image is decrypted with correct key. Zhi Zhong et al. [48] proposed Double image encryption using double pixel scrambling and random phase encoding. One of the two original images is encoded into the phase of a complex signal after being scrambled by one matrix, and the other original image encoded into its amplitude after being scrambled by another matrix. The complex signal is then encrypted into stationary white noise by utilizing double random phase encoding in fractional Fourier domain. By applying the correct keys with fractional orders, the random phase masks and the pixel scrambling operation, the two original images can be retrieved without cross-talk. Wei Zhang et al. [49] presented a symmetric color image encryption algorithm using intrinsic features of bit distributions. Analyze the intrinsic features of the bit distributions, the high correlation among bit planes and other issues related to the bit information of an image. Due to the superior characteristics of bit-level operations and the intrinsic bit features of the image, an expand-and-shrink strategy is
employed to shuffle the image with reconstructed permuting plane. Saeed et. al [50] proposed Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm. To encrypt multimedia content, lightweight and fast algorithms are usually used in frequency transform domain and in a partial encryption form, having time efficiency, high execution speed and correspondence with compression structures. A lightweight and fast algorithm is proposed and two designs in partial encryption scheme of DCT transform coefficients are introduced based on three fundamental principles and confrontation the partial encryption attacks. Xinjun Zhang et. al [51] proposed Chaos-based partial encryption of SPIHT coded color images. Modifying the bit values of different types which are obtained by Color-SPIHT (CSPIHT) compression algorithm leads to varying degradation degree of retrieved images. This signifies that the six bit types have various contributions to decoding. As long as the most important bits that have the greatest contribution are encrypted, we can ensure no information leaking out and minimal computation. The piecewise linear chaotic map (PWLCM) is appropriate for generating random number sequence used in proposed cryptosystem for its perfect ergodicity and confusion. Shiguo Lian et. al [52] proposed On the design of partial encryption scheme for multimedia content. Partial encryption scheme is performed by using wavelet transform, which shows secure against existing attacks and efficient in practical implementation. Gaurav Bhatnagar et. al [53] presented a simple selective encryption technique based on Saw-Tooth space filling curve, pixels of interest, non-linear chaotic map and singular value decomposition. The core idea of this algorithm is to scramble the pixel positions by the means of Saw-Tooth space filling curve followed by the selection of significant pixels using pixels of interest method. Then the diffusion process is done on the significant pixels using a secret image key obtained from non-linear chaotic map and singular value decomposition. Zahia Brahimi et. al [54] presented novel selective encryption image schemes based on JPEG2000 are proposed.
CHAPTER 1. INTRODUCTION

The rest one encrypts only the code-blocks corresponding to some sensitive precincts. In order to improve the security level, they introduce the permutation of code blocks contributing in the selected precincts. The idea of combining permutation and selective encryption is used in order to minimize the amount of processed data encryption while ensuring the best possible degradation through the permutation. Nidhi S Kulkarni et. al [55] proposed a selective encryption technique in wavelet domain for conditional access systems. This encryption is applied only to a subset of multimedia data stream rather than the multimedia data in its entirety to save the computational time and computational resources. Thus controlling the transparency of the multimedia data at the time of encryption. Priyanka Agrawal et. al [56] explained a concept where important part of the image that can efficiently achieve by conceptually selecting the part of the image which is further used in its normal mode of operation for encryption. Once encryption is done, the encrypted data is sent along with remaining original part of the message, ensuring its secured transmission and distribution over public networks. The main idea behind the present work is to select the part of the image by the arranging the bit stream in grid form and choosing the diagonal of the grid. Tao Xiang et. al [57] most existing selective image encryption schemes are designed based on image compression algorithms, and thus they are codec specific. As different bit planes of an image contribute differently to visualization effect, a selective gray-level image encryption scheme is proposed in this paper. In this scheme, only a portion of significant bits of each pixel is encrypted by the key stream generated from a one-way coupled map lattice that exhibits good chaotic dynamics even after discretization. Marc Van Droogenbroeck and Raphal Benedett [58] presented a selective encryption of compressed image and they used JPEG compression, the Huffman coder aggregates zero coefficients into runs of zeros and uses symbols that combine the run of zeros with magnitude categories for the non-zero coefficients that terminate the runs. These symbols are assigned 8-bit code words by the
Huffman coder. The code words precede the appended bits that specify the sign and magnitude of the non-zero coefficients. In the proposed scheme, the appended bits corresponding to a selected number of AC coefficients are encrypted. The DC coefficients are left unencrypted because, it is argued, they carry important visible information and are highly predictable. Roman P. Farrhofer and Andreas Uhl [59] explained the concept of the gray scale image is decomposed into its 8 bit planes and the most significant bit planes are encrypted. After a number of experiments, it is observed that (1) the encryption of the 4 most significant bit plane is not secure enough, (2) selectively encrypting 2 bit planes are sufficient if severe alienation of the image data is acceptable, and (3) encryption of 4 bit planes provides high confidentiality (4) for selective encryption only the lowest resolution of 5 layers may be encrypted. We have proposed an hybrid approach that involves rearranging the mapping image according to SCAN patterns and selecting a pixel value of rearranged mapping image based on the mapping function. The basic idea of this technique lies in converting the pixel value of original image into a row and column values of mapping image.

1.4 Problem Formulation

The goal of this research is to investigate new image encryption techniques and hybridise for better performance. Image encryption is categorized into

- **Spatial Domain**
  - Pixel Manipulation, Position Manipulation
- **Frequency Domain**
  - Phase Manipulation, Frequency Manipulation
- **Key Dependent**
  - Text key, Image key, Gesture Key
• Number of Images
  Dual image, Triple image, Multiple image

• Number of stages
  Single stage, Two stage, Multi stage

• Amount of Encryption
  Full, Selective, Partial/Visible Image

The principle objective of the research is to hybridise the existing encryption techniques with new technique to obtain better encryption technique.

1.5 Organization of thesis

In this section, a brief preview of the organization of this thesis is given. This thesis has been divided into 6 chapters as mentioned below.

• In Chapter 1, Preamble, Literature survey and problem formulation of the thesis have been discussed.

• In Chapter 2, brief introduction about existing and proposed method for image scrambling, image encryption and performance analysis for image encryption have been discussed.

• In chapter 3, Proposed multi stage and multiple image encryption methods have been discussed.

• In chapter 4, Proposed Partial image encryption and visible image encryption methods have been discussed.

• In chapter 5, Hardware software co-simulation for few proposed image encryption methods have been discussed.

• In Chapter 6, conclusion and future work of the thesis is addressed.