# ENHANCED IMAGE ENCRYPTION SCHEME WITH NEW MAPREDUCE APPROACH FOR BIG SIZE IMAGES

MAHMOUD AHMAD SALEM AL-KHASAWNEH

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

.

OCTOBER 2018

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

ٱقۡرَأۡ بِٱسۡمِ رَبِّكَ ٱلَّذِى خَلَقَ (١) خَلَقَ ٱلۡإِنسَٰنَ مِنۡ عَلَقٍ (٢) ٱقۡرَأۡ وَرَبُّكَ ٱلۡأَكۡرَمُ (٣)
ٱلَّذِى عَلَّمَ بِٱلۡقَلَمِ (٤) عَلَّمَ ٱلۡإِنسَٰنَ مَا لَمۡ يَعۡلَمۡ (٥)

***In the name of Allah, the Most Gracious, the Most Merciful***

**Read! In the Name of your Lord, Who has created (1) Has created man from a clot (2) Read! And your Lord is the Most Generous (3) Who has taught by the pen (4) Has taught man that which he knew not (5)**

*To soul of my mother, my father, brothers, sisters, wife, son (Keenan) …*

# ACKNOWLEDGEMENT

*In the Name of Allah, Most Gracious, Most Merciful*

*All praise and thanks are due to Allah, and peace and blessings be upon his messenger, Mohammed (peace be upon him).*

Alhamdulillah, it is with Allah S.W.T will that I accomplish this study, I would like to express my heartfelt gratitude to my supervisor **Prof. Dr. Siti Mariyam Shamsuddin** and without her guidance and advice this study would not have been possible. She has been incredibly wise, helpful, understanding, and generous throughout the process. Also, I would like to express my heartfelt to my Co-supervisor **Dr. Shafaatunnur Binti Hasan** for her support and guidance during my study. And I would like to thanks to my External supervisor **Asst. Prof. Dr. Adamu Abubakar Ibrahim** for his support and guidance during my study.

I am also immensely grateful to other faculty members for their kind cooperation, as well as to all staff of our faculty who extended their best cooperation during my study and stay here. And most importantly, I would like to thank to my family for their love and support, for their continuous support and supplication.

Finally, I would like to thank all my friends and colleagues for their support and help.

## ABSTRACT

Achieving a secured image encryption (IES) scheme for sensitive and confidential data communications, especially in a Hadoop environment is challenging. An accurate and secure cryptosystem for colour images requires the generation of intricate secret keys that protect the images from diverse attacks. To attain such a goal, this work proposed an improved shuffled confusion-diffusion based colour IES using a hyper-chaotic plain image. First, five different sequences of random numbers were generated. Then, two of the sequences were used to shuffle the image pixels and bits, while the remaining three were used to XOR the values of the image pixels. Performance of the developed IES was evaluated in terms of various measures such as key space size, correlation coefficient, entropy, mean squared error (MSE), peak signal to noise ratio (PSNR) and differential analysis. Values of correlation coefficient (0.000732), entropy (7.9997), PSNR (7.61), and MSE (11258) were determined to be better (against various attacks) compared to current existing techniques. The IES developed in this study was found to have outperformed other comparable cryptosystems. It is thus asserted that the developed IES can be advantageous for encrypting big data sets on parallel machines. Additionally, the developed IES was also implemented on a Hadoop environment using MapReduce to evaluate its performance against known attacks. In this process, the given image was first divided and characterized in a key-value format. Next, the *Map* function was invoked for every key-value pair by implementing a mapper. The *Map* function was used to process data splits, represented in the form of key-value pairs in parallel modes without any communication between other map processes. The *Map* function processed a series of key/value pairs and subsequently generated zero or more key/value pairs. Furthermore, the *Map* function also divided the input image into partitions before generating the secret key and XOR matrix. The secret key and XOR matrix were exploited to encrypt the image. The *Reduce* function merged the resultant images from the *Map* tasks in producing the final image. Furthermore, the value of PSNR did not exceed 7.61 when the developed IES was evaluated against known attacks for both the standard dataset and big data size images. As can be seen, the correlation coefficient value of the developed IES did not exceed 0.000732. As the handling of big data size images is different from that of standard data size images, findings of this study suggest that the developed IES could be most beneficial for big data and big size images.

## ABSTRAK

Mencapai skema penyulitan imej keselamatan (IES) untuk komunikasi data sensitif dan sulit, terutamanya dalam persekitaran Hadoop merupakan sesuatu yang mencabar. *Cryptosystem* yang tepat dan selamat untuk imej warna memerlukan penjanaan kunci rahsia rumit yang melindungi imej daripada pelbagai serangan. Untuk mencapai matlamat tersebut, kajian ini mencadangkan IES warna berasaskan kekeliruan yang diselaraskan dengan menggunakan imej kosong warna *hyper-chaotic*. Pertama, lima urutan nombor rawak yang berbeza akan dijana. Kedua, dua urutan ini digunakan untuk mengosongkan piksel dan bit imej, manakala tiga lagi baki digunakan untuk XOR nilai piksel imej. Prestasi IES yang dibangunkan telah dinilai dari segi pelbagai ukuran seperti saiz ruang kunci, pekali korelasi, entropi, min kesilapan kuasadua (MSE), isyarat puncak kepada nisbah kebisingan (PSNR) dan analisis berbeza. Nilai pekali korelasi (0.000732), entropi (7.9997), PSNR (7.61), dan MSE (11258) telah ditentukan menjadi lebih baik (untuk pelbagai serangan) berbanding teknik yang sedia ada. IES yang dicadangkan mengatasi *cryptosystem* serupa yang lain apabila perbandingan dibuat. Ia menunjukkn bahawa IES yang dicapai dapat memberi faedah kepada penyulitan set data besar pada mesin selari. Tambahan pula, IES yang dibangunkan telah dilaksanakan pada persekitaran Hadoop menggunakan *MapReduce* untuk menilai prestasi terhadap serangan yang diketahui. Dalam proses ini, pertamanya imej yang diberikan dibahagikan dan dicirikan ke dalam format nilai kunci. Seterusnya, fungsi peta dipanggil untuk setiap pasangan nilai utama melalui mapper. Teknik peta berjaya memecah data dalam bentuk pasangan nilai kunci dalam pendekatan selari tanpa menghaoungkan pemprosesan peta lain. Ia memproses penggantian pasangan kunci nilai dan kemudian menghasilkan kosong atau lebih daripada pasangan ini. Selain itu, fungsi peta membahagikan imej input ke dalam sekatan sebelum menghasilkan kunci rahsia dan matrik XOR. Kemudian, kunci rahsia dan matrik XOR dieksploitasi untuk menyulitkan imej. Funga pengurang mencantum imej yang dihasilkan dari peta tugas mengeluarkan imej akhir. Selain itu, nilai PSNR tidak melebihi 7.61 apabila IES yang dihangunkan dinilai berbanding serangan yang dketahui untuk kedua-dua imej set data standard dan data bersaiz besar. Sebagaimana yang dapat dilhat nilai pekali korelasi IES yang dibangunkan tidak melebihi 0.000732. Oleh kerana pengendalian imej saiz data besar berbeza dengan imej saiz data standard, kajian ini mencadangkan IES yang dibangunkan boleh memberi maafaat kepada data besar dan imej bersaiz besar.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVATIONS

| | | |
|---|---|---|
| AE | - | Authenticated Encryption |
| AES | - | Advanced Encryption Standard |
| BA | - | Blowfish Algorithm |
| BMP | - | Bitmap Image File |
| CC | - | Correlation Coefficient |
| CIA | - | Confidentiality, Integrity, and Availability |
| DDFS | - | Disco Distributed File System |
| DES | - | Data Encryption Standard |
| DICOM | - | Digital Imaging and Communications In Medicine |
| DNA | - | Deoxyribonucleic Acid |
| DSVSM | - | Dynamic State Variables Selection Mechanism |
| DT-CWT | - | Dual-Tree Complex Wavelet Transformations |
| FRFT | - | Fragmentary Fourier Changes |
| GB | - | Gigabyte |
| HDFS | - | Hadoop Distributed File System |
| HVS | - | Human Visual System |
| IE | - | Image Encryption |
| IOT | - | Internet of Things |
| LSB | - | Least Significant Bit |
| MACs | - | Message Authentication Codes |
| MSB | - | Most Significant Bit |
| MSE | - | Mean Square Error |
| NCPR | - | Number of Pixel Change Rate |
| PB | - | Petabyte |
| PSNR | - | Peak Signal to Noise Ratio |

| | | |
|---|---|---|
| PWLCM | - | Piecewise Direct-Disorderly Guide |
| RAM | - | Random-Access Memory |
| RGB | - | Red-Green-Blue |
| RSA | - | Rivest–Shamir–Adleman |
| SBLP | - | Spatial Bit-Level Permutations |
| SIE | - | Selective Image Encryption |
| SSIM | - | Structural Similarity Index Measure |
| TB | - | Terabyte |
| UACI | - | Unified Averaged Changing Intensity |
| UDF | - | User-Defined Function |
| USGS | - | United States Geological Survey’s |

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

In recent times, the world is characterised by high reliance of multimedia data so called digital world (in the form of video, audio and text files). Such reliance is ubiquitous in numerous applications and domains such as education, defense, health, marketing, banking, commerce, military, industry and others. Due to the exponential growth of information communication technology assisted Internet services such sensitive and private data can be exchanged freely at anytime from anywhere. This free access of wealth of data has resulted in increasing threats to the users. According to Patel and Belani (2011) and Radwan *et al.* (2016), images being the most common type of multimedia data (in digital form) owing to its ease capture and delivery are most susceptible to the attack from adversaries or illegal access. Consequently, the demand in achieving secure image transfer is constantly rising. In this regard, image encryption technique became the most effective scheme for secure image (data) transfer. Over the years, to protect the images from adversaries attack, various Image Encryption (IE) techniques have been developed. These include Advanced Encryption Standard (AES), Data Encryption Standard (DES) and (RSA) The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman.

In some ways, consideration of the large size image data has substantial amount of redundancy. Clearly the sizes that are categorised under big data becomes an issue. For instance, approximately 2.5 quintillion bytes of data are being emitted on daily frequency. The Big Data concept intends to deal with these volumes of data growth. Unfortunately, heterogeneity, scale, timeliness, complexity, and privacy are the major drawbacks of Big Data progress at all phases of the pipeline that can create value from data. These weaknesses engulf the entire big data analytics cycle from data acquisition up to the decisions making point. Crucial to these, is the heterogeneity nature of dataset; that is the state of different raw dataset based on different patterns or rules. This era of big data has posed a challenge to the big data analytics. Although, recently, prevalent research efforts in big data analytics have been devoted and is still active, though, tranquil in early stage. The issue of sizes, especially image files that make big data need to be understood in the context of number. This could be a standard that should cover all areas, specifically the size of image files that makes up a big data. The requirements applied to image data should be in terms of perception, acquisition storage and processing. When these requirements are translated into image data size, the generally acceptable range is from as technology advances overtime the size of the data set that qualified as big data will increase (Manyika *et al.*, 2011). However, limited Internet bandwidth and storage capacity are the two challenges that prevent many researchers from making use of the image big data set in their work (Kasemsap, 2017). As such, some researchers resolved to use sub-set of the big data sets that does not actually meet the definition of big data described by Manyika *et al.* (2011). Although some researches proposed the size of image data that will be qualified as big data. Kambatla *et al.* (2014) proposed that 2.5 PB was qualified to a be big data set, while Zhao *et al.* (2015) proposed 1.9 TB, Guzun *et al.* (2015) proposed that 98 GB is a big data set, and Chen *et al.* (2012) proposed that 600 TB is qualified to be a big data set. Therefore, with such amount of sizes, current IE techniques are not appropriate (Chen *et al.*, 2013a; Coppersmith, 1994; Wang *et al.*, 2012).

The existing IE techniques that suffer from several shortcomings and weaknesses need to be resolved. These limitations include high computational time and the requirement of powerful computing system. Ismail *et al.* (2010) and Jolfaei and Mirghadri (2010) revealed that these techniques are inefficient, in which the confidentiality and the security of data often remains insecure. Despite all, the multimedia technology is escalating at rapid space. Meanwhile, the Internet network system has restricted the bandwidth and the existing undersized storage capacity has been unrelentingly utilised for transmitting and storing the enormous amount of digital data. This in turn has invited a considerable degree of threat towards the security and safety of data (especially images). Image being the most extensively used multimedia information in innumerable domains of applications, Bashardoost *et al.* (2014) emphasised the importance of security in the image data transmission. Thus, IE technique has been popularly utilised to safeguard an image against illegal access or hackers. In IE scheme, a finite set of instructions is used to convert the original images in to other images. In this process, an algorithm containing one or more keys that remains obscure to the intruder is used. Kaur (2013) and Nagaraj *et al.* (2015) stated that the encrypted image still holds confidentiality even though the key is not known.

To date, cryptography remains the most commonly employed solution in the establishment of secure storage of big data satellite images (Usama and Khan, 2008; Zhu *et al.*, 2010b). The conventional cryptographic techniques are categorised into two types such as symmetric and asymmetric crypto systems. Symmetric cryptosystems use the exact key for both encryption and decryption, wherein the encryption calls for the secure key communication between the transmitter and the receiver. Conversely, asymmetric encryption algorithms employ different keys for encryption and decryption process. This type of encryption includes exponential operations and thus becoming weighty in terms of performance. The conventional encryption algorithms have numerous drawbacks including poor efficiency and considerable computational time particularly during the handling of large size imagery. Therefore, the conventional IE algorithms cannot be used in secured and efficient image cryptosystem.

Image encryption refers to the use of a group of instructions called algorithm for converting plain image into coded one in a manner that remains unrecoverable except by the sender and the intended receiver (Choudhary and Arun, 2014). For secured IE, several techniques have been proposed. Amongst all these techniques, chaos based IE scheme discerned to be most efficient (Jain, 2016). Chaos theory was first introduced in the 70s, which was initially applied in the area of engineering and basic sciences. Then, in the 80s, the cryptographic applications became popular (Liu *et al.,* 2009). The IE schemes based on chaos are advantageous because they are sensitive, random, unpredictable, and have topological transitivity (Alsafasfeh and Arfoa, 2011; Liu and Miao, 2016). These attributes including randomness, unpredictability, and sensitivity to initial conditions and control parameters make chaotic systems comparable to noisy systems (Nesakumari and Maruthuperumal, 2012; Shuangshuang and Min, 2014). Thus, chaotic systems are greatly preferred in cryptography (Sankpal and Vijaya, 2014). Furthermore, randomness of data and sensitivity to initial conditions make chaotic systems' randomness to be unpredictable. Consequently, chaotic systems can be regarded as the basis for decryption (Al-Maadeed *et al.*, 2012). Chaos maps and chaos cryptography are distinct from one another, in which the later are characterised by finite sets and the former (chaos maps) are described by actual numbers (Sankpal and Vijaya, 2014).

Irrespective of their robustness, the conventional IE systems are susceptible to various cryptographic attacks such as brute force, chosen-ciphertext, chosen-plaintext and known-plaintext attacks. According to Alvarez and Li (2006), through these attacks the original plain image could still be recovered although the secret key is unknown. Chaos-based encryption can efficiently prevent the brute force attacks. In the IE systems based on chaotic map, the diffusion and the confusion key properties are embedded. Tong and Liu (2011) and Ahmad (2011) reported the usage of these properties by several conventional IE algorithms to improve the robustness of image cryptosystem. It was further acknowledged that the implementation of secure IE systems against all other cryptographic attacks require the enhancement of the key space comprising of a set of all possible keys via the combination of multiple chaotic algorithms. Using the XOR operation, binary files can be produced via the combination of multiple chaotic maps. Literature revealed that, the presence of reiterating sequences within the satellite images can lead to the production of binary files which in turn allows the IE system robust against cryptographic attacks (Padmapriya and Benazir, 2015; Zhang *et al.*, 2012b).

In cryptography, numerous chaotic map algorithms have been presented for generating secret keys (Khan and Shah, 2014; Sankpal and Vijaya, 2014). Nevertheless, these algorithms did not consider the time complexity of key generation and the selection procedure of the optimal set of chaotic algorithms. A combination of various chaotic map algorithms aids to improve the security level of the cryptosystem. However, multiple chaotic algorithms are not feasible for big size imagery due to presence of time complexity. Therefore, an optimal set of chaotic map algorithms needs to be implemented and simultaneously the security has to be preserved. Such implementation must maintain a suitable order among several chaotic map algorithms during the generation of key by ensuring the security level. It is worth noting that these set of algorithms appear to be more inter-linked and the generated key can reduced the space, leading to vulnerability of security. In short, preservation of improved trade-off between security and time complexity is essential for big data IE. Considering the significance of IE system related to big data security the present thesis intended to work on it. A brief background is provided in the following sub chapters to reveal the importance of developing a robust cryptosystem for big data imagery.

## 1.2 Problem Background

Cryptography is an integral part of big size data imaging system. It was reported that (Khan and Shah, 2014; Sankpal and Vijaya, 2014) some attacks can be facilitated by the security weakness of conventional cryptographic algorithms, allowing the hacking of the sensitive and critical images. Consequently, the chaotic map based IE systems were employed. It is customary to discuss the real time shortcomings of the conventional cryptography and chaotic map based IE techniques. In the past, the majority of researchers have focused on the conversion of a plain image into a coded form in order to safely hide the embedded information during the data transmission or storing (Divya *et al.*, 2012). Considering that the IE is a part of the information security (El-Deen *et al.*, 2014), it must protect information to fulfil its confidentiality, integrity, and availability (CIA) principles to achieve high criteria security system (Sattarova Feruza and Kim, 2007).

A modified AES has been used to enhanced IE (Tong and Liu (2011), . Ou *et al.* (2007)). Although, other various IE techniques namely: Rössler- and Lorenz-chaotic system (Alsafasfeh and Arfoa (2011)), the long-term chaotic (Chen *et al.* (2004)), large the key space size chaotic systems (Sakthidasan and Krishna (2011)) shows some remarkable over the years. Liu and Tian (2012) introduced a coloured IE algorithm grounded on chaotic map and spatial bit-level permutations (SBLP). A simple cryptographic method based on dual-tree complex wavelet transformations (DT-CWT) was proposed by Jain (2016). Wang (2016) mentioned the usability of the statistical properties of cipher image in deciphering the encryption algorithm. Wu and Preneel (2007) studied several methods of differential attacks for a stream of cipher analysis. Jolfaei and Mirghadri (2010) showed that the chaotic algorithm could produce the number sequence while the encryption process transforms the image blocks using these sequences since the pseudo-random generator produces the random sequences. Aihong *et al.* (2010) and Rodriguez-Sahagun *et al.* (2010) proposed an IE algorithm using the logistic map, in which the encryption was performed in two iterative steps. First, the logistic map was used to permute the pixels of the original image. Second, the diffusion process was applied to fulfil the security requirements. Zhang *et al.* (2009) used DCT to present the IE algorithm in the frequency domain.

If we consider a scenario on how people use image encryption in real world, for instance in Digital Imaging and Communications in Medicine (DICOM) where images are being processed and shared among various medical centres region, it will be catastrophic if the images are either diverted or stolen while on communication. As a result, DICOM employed image encryption (Hua *et al.*, 2018; Rajagopalan *et al.*, 2018; Ye and Huang, 2018). Most DICOM objects contain images and associated demographic and medical information about a patient, which need to be kept confidential. Encryption is one way to keep these data confidential. DICOM does not specify the encryption in detail (it refers to other standards for that), but several changes made to the DICOM Standard over the last decade have facilitated encryption, including the transfer of encrypted DICOM objects, and reading of encrypted DICOM objects on the receiver’s end. Unfortunately, the encryption techniques involved did not achieve the standard of the requirement for Big Data.

It is worthwhile to mention that the aforesaid works (El-Deen *et al.*, 2014; Liu and Tian, 2012; Rodriguez-Sahagun *et al.*, 2010; Tong and Liu, 2011; Wang *et al.*, 2016) are still focusing on chaotic image encryption. Nevertheless, how to employ chaotic and shuffling has not been greatly discussed. Hence, following the previous successful applications of chaotic (Xu *et al.*, 2017; Yuan *et al.*, 2017) for IE and motivated the works of (Chai *et al.*, 2017; Li *et al.*, 2017; Yang and Bai, 2017) , this work proposes techniques on exploring confusion and shuffling in image encryption.

In the domain of IE, several chaotic map-based cryptographic algorithms have been developed. The conventional cryptosystems appear to be vulnerable to classical attacks such as chosen-ciphertext, chosen-plaintext, and known-plaintext. Recovering the plain image even in the absence of secret key is indeed possible, wherein a pair of plain image/cipher-image is sufficient to fully break the cryptosystem. Besides, the cryptosystem is insensitive to the small changes in the plain image.

By combining chaotic map based algorithms, such issues can be resolved at the cost of increased time complexity. Therefore, it is important to identify the most optimum set of chaotic map algorithms and the defensive mechanism to make the cryptosystem resistant against cryptographic attacks. Usually, processing requirements on any IE scheme is quite high and efficient solution is inevitable (Ullah *et al.*, 2013). Extensive attempts have been made in reducing the encrypted digital contents through the Selective Image Encryption (SIE). The SIE encrypts only a portion of the image due to large size of image or to reduce encryption time (Puech *et al.*, 2013).  In short, it is emphasised that more strategies must be developed to secure the information (data in the form of video, text and images) on personal computers, especially those running through networks and big data environment considering the advancement of IOT platform.

## 1.3 Problem Statement

One of the important tools for measuring the encryption system in general and image encryption in particular is correlation coefficient. This is the measure that shows how well an image can be securely encrypted. To achieve a lower correlation the encryption technique is required to have a good shuffling method that could be able to shuffle the image in a way that it will conceal its information. This has been proven by many previous research (Ghebleh *et al.*, 2018; Janakiraman *et al.*, 2018; Ramalingam *et al.*, 2018). Unfortunately, the shuffling technique proposed by those past research studies mainly depend on the use of a secret key with the shuffling algorithms.

While in image encryption, the success of confusion process has do to with the weakening of high correlations between adjacent pixels, good confusion process must produce ciphered image with smaller correlations between adjacent pixels (Wang *et al.*, 2018). It is customary that the correlations between the plain image and its corresponding encrypted image are evaluated whenever the performance of a proposed IE algorithms is required (Choi *et al.*, 2016). Dong (2014) assessed his proposed image encryption technique using a correlation coefficient between the scrambling degree of his method and scrambling matrix of the image data. A moderate correlation value between adjacent pixels of encrypted aided image justified a proposed image encryption algorithm in Chen *et al.* (2004) and Wang (2016). It is also revealed that the more sophisticated image encryption technique is, the lower the correlation value would be obtained (Hu *et al.*, 2017).

Despite the success of these IE techniques, yet they faced some major drawbacks. One of the weaknesses is the state of the secret key, which can be exposed easily. And render the encryption technique useless if not properly generated. This can be in image pixel locations orientation (horizontal, vertical, and diagonal). Furthermore, the strength of IE lies with the strength of the key generation as a result of simple generated key will weaken any proposed IE.

Another important issue regarding image encryption is diffusion. This entails the degree of how the frequency values of pixel in the plain image over some pixel in the cipher image are carefully concealed. There are many previous research studies that depend on diffusion technique to strengthen their image encryption algorithm (Hua *et al.*, 2018; Zhang *et al.*, 2018). Results of such studies have shown a good impact of the statistical information of the encrypted image in which diffusion process was carried out (Chen *et al.*, 2018). Unfortunately, the application of the diffusion process on those studies do not strengthen an encryption technique at some certain high order. That is the only focus on applying single step diffusion. Furthermore, there is a lack of high key space, enhanced key sensitivity, improvement of histogram and information entropy, and strong resistance to differential attacks to those previous implemented system.

Even though image encryption has been implemented for many years, recently there is a new area that emerged based on size of data. Huge amount of image data now can be categorised under the phenomena called Big Data. Due to the fact that currently data sets that are so big and complex and required various data-processing techniques which also include image data have now emerged. Regrettably, image encryption of such type of data is ignored by research community.

The combined effect of having a low correlation in image encryption, high secured encrypted image and big size image encryption is crucial. Many research studies ignore investigating those effects. Therefore, there is a need to examine the current state and the future development of image encryption with regard to this concern.

## 1.4 Research Questions

Literature exhibited that chaos-based IE methods are advantageous to achieve enhanced security in the cryptosystem. However, several unresolved issues must be considered to propose a new IE system with improved security. Based on the aforementioned problem statement, the following research questions are emerged:

i. How to combine generated secret key and shuffling method to produce low correlation shuffled image?
ii. How to create a diffusion method on the shuffled image to improve histogram and entropy and produce high secured encrypted image?
iii. How to create mapper and reducer procedures for big size image encryption?

## 1.5 Research Aims and Objectives

The aim of this research is to propose new image encryption scheme based on MapReduce. Based on the research questions the following objectives are set for further accomplishments:

i. To combine generated secret key and shuffling method to produce low correlation shuffled image.
ii. To propose new diffusion method on the shuffled image to improve histogram and entropy and produce high secured encrypted image.
iii. To propose new mapper and reducer procedures for big size image encryption.

## 1.6 Research Scope

To achieve the goals of this study, the following significant research scopes determined:

i. Use of SIPI dataset to test the performance of the proposed IE scheme. This dataset contains many images suitable for the implementation of the proposed IE system. In addition to SIPI dataset, the system performance will be tested using remote sensing satellite images obtained from Earth Explorer portal Database.
ii. Testing the IE system via diverse performance analyses such as randomness, key space and key sensitivity, image histogram, information entropy, correlation between adjacent pixels, correlation coefficient between original and encrypted images, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR), encryption quality and differential analysis.

## 1.7 Research Contribution

The newly proposed IE system is expected to achieve cipher images with better security level. This will be accomplished using new random number generators with large key space, increasing robustness against differential attack and the introduction of new process in the proposed encryption system. This enhanced IE scheme will be able to encrypt large size images (satellite based remote sensing data) using MapReduce in Hadoop Environment.

## 1.8 Thesis Structure and Organisation

Present thesis is organised as follows:

Chapter 1 provides the rational of this research and emphasises the importance of developing a robust IE scheme to tackle the existing security problem with colour images data transmission. A brief background is provided to show the ongoing intensive activities in the field of image cryptography. The problem statement, research questions, objectives, research scopes, and contributions are underscored.

Chapter 2 reviews the works related to the existing issues and past development on image encryption (IE). A brief description on digital images followed by the preliminary terminologies in cryptology domain, then purpose of IE, and the classification of cryptography are discussed. Next, it introduces the cryptography domain, followed by chaos-based IE and the process of confusion and diffusion. Later, various IE techniques and ongoing investigations on big size images encryption, cryptanalysis, and the secret key generation techniques are presented. An overview of MapReduce implementations and apache Hadoop are emphasized.

Upon formulating the problem statement and investigating the image encryption (IE) methods, the research methodology used to achieve the proposed objectives will be discussed in Chapter 3.

Chapter 4 describes in detail the proposed image encryption (IE) method based on the methodology adopted in Chapter 3. The experimental results obtained from the developed IE algorithm are discussed and validated. An explanation for the design and development of the proposed IE method is provided. It is important to mention that this newly developed IE scheme was achieved in two phases to accomplish the set objectives (Chapter 1). In the first phase, the secret key matrix was generated. The IE procedure in phase 2 involved two major tasks including the confusion and the diffusion processes.

Chapter 5 introduces the Developed MapReduce method in Hadoop Environment for Big Image Size. The experimental results obtained from the developed IE algorithm in Hadoop Environment are discussed and validated. An explanation for the design and development of the proposed IE method using MapReduce method in Hadoop Environment is provided.

Chapter 6 concludes the thesis in terms of successful accomplishments of the proposed objectives, major contributions, and assertions. Conclusions are drawn based on the major results obtained in achieving the objectives. Furthermore, some recommendations are made for future work.

# REFERENCES


Abugharsa, A. B., and Almangush, H. (2011). A new image encryption approach using block-based on shifted algorithm. *International Journal of Computer Science and Network Security (IJCSNS), 11*(12), 123-130.

Abuturab, M. R. (2012a). Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. *Optics and Lasers in Engineering, 50*(9), 1209-1216.

Abuturab, M. R. (2012b). Securing color information using Arnold transform in gyrator transform domain. *Optics and Lasers in engineering, 50*(5), 772-779.

Ahmad, A., Paul, A., Din, S., Rathore, M. M., Choi, G. S., and Jeon, G. (2017). Multilevel data processing using parallel algorithms for analyzing big data in high-performance computing. *International Journal of Parallel Programming*, 1-20.

Ahmad, M. (2011). *Cryptanalysis of chaos based secure satellite imagery cryptosystem.* Paper presented at the International Conference on Contemporary Computing, 81-91.

Ahmad, M., and Farooq, O. (2011). Secure satellite images transmission scheme based on chaos and discrete wavelet transform. In *High Performance Architecture and Grid Computing* (pp. 257-264): Springer.

Ahmed, H. E.-d. H., Kalash, H. M., and Allah, O. S. F. (2006). Encryption quality analysis of the RC5 block cipher algorithm for digital images. *Optical Engineering, 45*(10), 107003.

Ahuja, R. (2018). Hadoop Framework for Handling Big Data Needs. In *Handbook of Research on Big Data Storage and Visualization Techniques* (pp. 101-122): IGI Global.

Aihong, Z., Lian, L., and Shuai, Z. (2010). *Research on method of color image protective transmission based on Logistic map.* Paper presented at the 2010

International Conference on Computer Application and System Modeling (ICCASM 2010), V9-266-V269-269.

Al-Maadeed, S., Al-Ali, A., and Abdalla, T. (2012). A new chaos-based image-encryption and compression algorithm. *Journal of Electrical and computer Engineering, 2012,* 15.

Alabaichi, A., Ahmad, F., and Mahmod, R. (2013). *Security analysis of blowfish algorithm.* Paper presented at the Informatics and Applications (ICIA), 2013 Second International Conference on, 12-18.

Alexopoulos, C., Bourbakis, N. G., and Ioannou, N. (1995). Image encryption method using a class of fractals. *Journal of Electronic Imaging, 4*(3), 251-260.

Alghamdi, A. S., Ullah, H., Khan, M. U., Ahmad, I., and Alnafajan, K. (2011). Satellite image encryption for C4I System. *International Journal of Physical Sciences, 6*(17), 4255-4263.

Alsafasfeh, Q. H., and Arfoa, A. A. (2011). Image encryption based on the general approach for multiple chaotic systems. *J. Signal and Information Processing, 2*(3), 238-244.

Alvarez, G., and Li, S. J. (2006). Breaking an encryption scheme based on chaotic baker map. *Physics Letters A, 352*(1-2), 78-82.

Bahrami, S., and Naderi, M. (2012). Image encryption using a lightweight stream encryption algorithm. *Advances in Multimedia, 2012,* 4.

Baptista, M. (1998). Cryptography with chaos. *Physics letters A, 240*(1-2), 50-54.

Barkan, E., and Biham, E. (2018). Cryptanalysis method and system: Google Patents.

Bashardoost, M., Rahim, M. S. M., Altameem, A., and Rehman, A. (2014). A Novel Approach to Enhance the Security of the LSB Image Steganography. *Research Journal of Applied Sciences, Engineering and Technology, 7*(19), 3957-3963.

Bashir, Z., Rashid, T., and Zafar, S. (2016). Hyperchaotic dynamical system based image encryption scheme with time-varying delays. *Pacific Science Review A: Natural Science and Engineering, 18*(3), 254-260.

Belazi, A., El-Latif, A. A. A., Diaconu, A.-V., Rhouma, R., and Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering, 88,* 37-50.

Bora, S., Sen, P., and Pradhan, C. (2015). *Novel color image encryption technique using Blowfish and Cross Chaos map.* Paper presented at the Communications and Signal Processing (ICCSP), 2015 International Conference on, 0879-0883.

Boriga, R. E., Dăscălescu, A. C., and Diaconu, A. V. (2014). A new fast image encryption scheme based on 2D chaotic maps. *IAENG International Journal of Computer Science, 41*(4), 249-258.

Boukhatem, M. B., and Lahdir, M. (2015). Meteosat Images Encryption based on AES and RSA Algorithms. *(IJACSA) International Journal of Advanced Computer Science and Applications, 6,* 203-208.

Bourbakis, N., and Alexopoulos, C. (1992). Picture data encryption using scan patterns. *Pattern Recognition, 25*(6), 567-581.

Cao, W., Zhou, Y., Chen, C. P., and Xia, L. (2017). Medical image encryption using edge maps. *Signal Processing, 132*, 96-109.

Cascading. (2018). Retrieved 25/02/2018, from http://www.cascading.org

Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., and Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons & Fractals, 95*, 92-101.

Chai, X. L., Gan, Z. H., and Zhang, M. H. (2017). A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimedia Tools and Applications, 76*(14), 15561-15585.

Chakraborty, S., Seal, A., Roy, M., and Mali, K. (2016). A novel lossless image encryption method using DNA substitution and chaotic Logistic map.

Chen, C. S., Wang, T., Kou, Y. Z., Chen, X. C., and Li, X. (2013a). Improvement of trace-driven I-Cache timing attack on the RSA algorithm. *Journal of Systems and Software, 86*(1), 100-107.

Chen, G., Mao, Y., and Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*(3), 749-761.

Chen, H., Du, X., Liu, Z., and Yang, C. (2013b). Color image encryption based on the affine transform and gyrator transform. *Optics and Lasers in Engineering, 51*(6), 768-775.

Chen, J., Zhu, Z.-l., Zhang, L.-b., Zhang, Y., and Yang, B.-q. (2018). Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. *Signal Processing, 142*, 340-353.

Chen, Y., Alspaugh, S., and Katz, R. (2012). Interactive analytical processing in big data systems: A cross-industry study of mapreduce workloads. *Proceedings of the VLDB Endowment, 5*(12), 1802-1813.

Chhotaray, S. K., Chhotaray, A., and Rath, G. S. (2015). *A new method of generating public key matrix and using it for image encryption.* Paper presented at the Signal Processing and Integrated Networks (SPIN), 2015 2nd International Conference on, 453-458.

Choi, J., Seok, S., Seo, H., and Kim, H. (2016). A fast ARX model-based image encryption scheme. *Multimedia Tools and Applications, 75*(22), 14685-14706.

Choudhary, R., and Arun, J. (2014). Secure Image Transmission and Evaluation of Image Encryption. *International Journal of Innovative Science, Engineering & Technology, 1*(2), 65-69.

Chung, K.-L., and Chang, L.-C. (1998). Large encrypting binary images with higher security. *Pattern Recognition Letters, 19*(5-6), 461-468.

Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM journal of research and development, 38*(3), 243-250.

Corrigan-Gibbs, H., Mu, W., Boneh, D., and Ford, B. (2013). *Ensuring high-quality randomness in cryptographic key generation.* Paper presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 685-696.

Cui, D., Shu, L., Chen, Y., and Wu, X. (2013). *Image encryption using block based transformation with fractional Fourier transform.* Paper presented at the Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on, 552-556.

Dean, J., and Ghemawat, S. (2008). MapReduce: simplified data processing on large clusters. *Communications of the ACM, 51*(1), 107-113.

Disco. (2018). Retrieved 25/02/2018, from http://discoproject.org/

Divya, V., Sudha, S., and Resmy, V. (2012). Simple and secure image encryption. *IJCSI International Journal of Computer Science Issues, 9*(6), 286-289.

Durstenfeld, R. (1964). Algorithm 235: random permutation. *Communications of the ACM, 7*(7), 420.

El-Deen, A., El-Badawy, E., and Gobran, S. (2014). Digital image encryption based on RSA algorithm. *J. Electron. Commun. Eng, 9*(1), 69-73.

El-Latif, A. A. A., Niu, X., and Amin, M. (2012). A new image cipher in time and frequency domains. *Optics Communications, 285*(21-22), 4241-4251.

Enayatifar, R., Abdullah, A. H., Isnin, I. F., Altameem, A., and Lee, M. (2017). Image encryption using a synchronous permutation-diffusion technique. *Optics and Lasers in Engineering, 90*, 146-154.

Eslami, Z., and Bakhshandeh, A. (2013). An improvement over an image encryption method based on total shuffling. *Optics Communications, 286*, 51-55.

Faragallah, O. S. (2011). Digital image encryption based on the RC5 Block Cipher Algorithm. *Sensing and Imaging: An International Journal, 12*(3-4), 73-94.

FileMap. Retrieved 06/02/2018, from http://mfisk.github.com/filemap/

Fisher, R. A., and Yates, F. (1938). Statistical tables for biological, agricultural and medical research.

Francois, M., Grosges, T., Barchiesi, D., and Erra, R. (2013). A new pseudo-random number generator based on two chaotic maps. *Informatica, 24*(2), 181-197.

Fridrich, J. (1997). *Image encryption based on chaotic maps.* Paper presented at the Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on, 1105-1110.

Gao, Y., Wang, Z., Ji, C., Xiao, P., Qin, J., and Li, Z. (2017). *Design and implementation of a mobile-health call system based on scalable kNN query*. Paper presented at the e-Health Networking, Applications and Services (Healthcom), 2017 IEEE 19th International Conference on, 1-6.

Ghebleh, M., and Kanso, A. (2017). A novel efficient image encryption scheme based on chained skew tent maps. *Neural Computing and Applications*, 1-16.

Ghebleh, M., Kanso, A., and Stevanović, D. (2018). A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation. *Multimedia Tools and Applications, 77*(6), 7305-7326.

Goumidi, D. E., and Hachouf, F. (2010). *Modified confusion-diffusion based satellite image cipher using chaotic standard, logistic and sine maps.* Paper presented at the Visual Information Processing (EUVIP), 2010 2nd European Workshop on, 204-209.

Gu, G., Ling, J., Xie, G., and Li, Z. (2016). A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images. *Signal Processing: Image Communication, 40*, 52-64.

Gui, W., Liu, J., Yang, C., Chen, N., and Liao, X. (2013). Color co-occurrence matrix based froth image texture extraction for mineral flotation. *Minerals Engineering, 46*, 60-67.

Guzun, G., Tosado, J. E., and Canahuate, G. (2015). *Scalable preference queries for high-dimensional data using map-reduce.* Paper presented at the Big Data (Big Data), 2015 IEEE International Conference on, 2243-2252.

Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. (1990). A secret key cryptosystem using a chaotic map. *IEICE TRANSACTIONS (1976-1990), 73*(7), 1041-1044.

Hadoop. (2018). Retrieved 25/02/2018, from http://hadoop.apache.org/

Hamraz, H., Contreras, M. A., and Zhang, J. (2017). A scalable approach for tree segmentation within small-footprint airborne LiDAR data. *Computers & Geosciences, 102*, 139-147.

He, Y., Cao, Y., and Lu, X. (2012). Color image encryption based on orthogonal composite grating and double random phase encoding technique. *Optik-International Journal for Light and Electron Optics, 123*(17), 1592-1596.

Hu, F., Wang, J., Xu, X., Pu, C., and Peng, T. (2017). Batch Image Encryption Using Generated Deep Features Based on Stacked Autoencoder Network. *Mathematical Problems in Engineering, 2017*.

Hua, Z., Yi, S., and Zhou, Y. (2018). Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Processing, 144*, 134-144.

Huang, C. K., and Nien, H. H. (2009). Multi chaotic systems based pixel shuffle for image encryption. *Optics Communications, 282*(11), 2123-2127.

Ismail, I. A., Amin, M., and Diab, H. (2010). A digital image encryption algorithm based a composition of two chaotic logistic maps. *IJ Network Security, 11*(1), 1-10.

Jain, A. (2016). Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform. *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 6*(5), 8-11.

Janakiraman, S., Thenmozhi, K., Rayappan, J. B. B., and Amirtharajan, R. (2018). Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. *Microprocessors and Microsystems, 56*, 1-12.

Jolfaei, A., and Mirghadri, A. (2010). An image encryption approach using chaos and stream cipher. *Journal of Theoretical and Applied Information Technology, 19*(2), 117-125.

Kadir, A., Aili, M., and Sattar, M. (2017). Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections. *Optik-International Journal for Light and Electron Optics, 129*, 231-238.

Kaliski, B., and Yin, Y. L. (1998). *On the security of the RC5 encryption algorithm*: RSA Laboratories Technical Report TR-602. To appearo. Document Number)

Kamali, S. H., Shakerian, R., Hedayati, M., and Rahmani, M. (2010). *A new modified version of advanced encryption standard based algorithm for image encryption.* Paper presented at the Electronics and Information Engineering (ICEIE), 2010 International Conference On, V1-141-V141-145.

Kambatla, K., Kollias, G., Kumar, V., and Grama, A. (2014). Trends in big data analytics. *Journal of Parallel and Distributed Computing, 74*(7), 2561-2573.

Kar, M., Mandal, M., Nandi, D., Kumar, A., and Banik, S. (2016). Bit-plane encrypted image cryptosystem using chaotic, quadratic, and cubic maps. *IETE technical review, 33*(6), 651-661.

Kasemsap, K. (2017). Big Data Management: Advanced Issues and Approaches. *International Journal of Organizational and Collective Intelligence (IJOCI), 7*(3), 44-55.

Kaur, R. (2013). Comparative analysis and implementation of image encryption algorithms. *International Journal of Computer Science and Network Security (IJCSNS), 13*(12), 53.

Kaur, R., and Banga, V. (2012). *Image security using encryption based algorithm.* Paper presented at the International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP 2012), 15-16.

Kazlauskas, K., and Kazlauskas, J. (2009). Key-dependent S-box generation in AES block cipher system. *Informatica, 20*(1), 23-34.

Khan, M., and Shah, T. (2014). A literature review on image encryption techniques. *3D Research, 5*(4), 1-25.

Khashan, O. A., Zin, A. M., and Sundararajan, E. A. (2014). Performance study of selective encryption in comparison to full encryption for still visual images. *Journal of Zhejiang University SCIENCE C, 15*(6), 435-444.

Khezr, S. N., and Navimipour, N. J. (2017). MapReduce and Its Applications, Challenges, and Architecture: a Comprehensive Review and Directions for Future Research. *Journal of Grid Computing, 15*(3), 295-321.

Koitzsch, K. (2017). *Pro Hadoop Data Analytics*: Springer.

Kulsoom, A., Xiao, D., and Abbas, S. A. (2016). An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. *Multimedia Tools and Applications, 75*(1), 1-23.

Kumar, M., Mishra, D., and Sharma, R. (2014). A first approach on an RGB image encryption. *Optics and Lasers in Engineering, 52*, 27-34.

Kumar, M., Powduri, P., and Reddy, A. (2015). An RGB image encryption using diffusion process associated with chaotic map. *Journal of Information Security and Applications, 21*, 20-30.

Kuo, C. J. (1993). Novel image encryption technique and its application in progressive transmission. *Journal of Electronic Imaging, 2*(4), 345-352.

Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications, 11*(1), 62-67.

Li, F., Ooi, B. C., Özsu, M. T., and Wu, S. (2014). Distributed data management using MapReduce. *ACM Computing Surveys (CSUR), 46*(3), 31.

Li, Y. P., Wang, C. H., and Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering, 90*, 238-246.

Liu, L. F., and Miao, S. X. (2016). A new image encryption algorithm based on logistic chaotic map with varying parameter. *Springerplus, 5*, 12.

Liu, M., and Mostaghimi, P. (2017). High-resolution pore-scale simulation of dissolution in porous media. *Chemical Engineering Science, 161*, 360-369.

Liu, R., and Tian, X. (2012). New Algorithm for Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation. *Journal of Theoretical & Applied Information Technology, 43*(1).

Liu, S., Sun, J., and Xu, Z. (2009). An Improved Image Encryption Algorithm based on Chaotic System. *JCP, 4*(11), 1091-1100.

Luciano, D., and Prichett, G. (1987). Cryptology: From Caesar ciphers to public-key cryptosystems. *The College Mathematics Journal, 18*(1), 2-17.

Luo, Y., Du, M., and Liu, D. (2012). *JPEG Image Encryption Algorithm Based on Spatiotemporal Chaos.* Paper presented at the Chaos-Fractals Theories and Applications (IWCFTA), 2012 Fifth International Workshop on, 191-195.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., et al. (2011). Big data: The next frontier for innovation, competition, and productivity.

Mastan, J. M. K., Sathishkumar, G., and Bagan, K. B. (2011). *A color image encryption technique based on a substitution-permutation network.* Paper presented at the International conference on Advances in Computing and Communications, 524-533.

Masuda, N., and Aihara, K. (2002). Cryptosystems with discretized chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 49*(1), 28-40.

Mirzaei, O., Yaghoobi, M., and Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. *Nonlinear Dynamics, 67*(1), 557-566.

Muhaya, F. T. B. (2013). Chaotic and AES cryptosystem for satellite imagery. *Telecommunication Systems, 52*(2), 573-581.

Mukherjee, P., Rarhi, K., Bhattacharya, A., and Bhattacharya, R. (2017). Cryptanalysis of a Chaotic Key Based Image Encryption Scheme.

Nagaraj, S., Raju, G., and Rao, K. K. (2015). Image Encryption Using Elliptic Curve Cryptograhy and Matrix. *Procedia Computer Science, 48*, 276-281.

Nemade, V., and Wang, R. (2012). Image encryption using Blowfish and genetic algorithm. *Int. J. Comput. Technol. Appl, 3*(6), 1067-1070.

Nesakumari, G. R., and Maruthuperumal, S. (2012). Normalized image watermarking scheme using chaotic system. *International Journal of Information and Network Security, 1*(4), 255.

Ou, Y., Sur, C., and Rhee, K. H. (2007). *Region-based selective encryption for medical imaging.* Paper presented at the International Workshop on Frontiers in Algorithmics, 62-73.

Padmapriya, A., and Benazir, M. S. (2015). Elementary Matrix operation based Satellite image encryption. *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 4*(7), 367 -371.

Pareek, N. K. (2012). Design and analysis of a novel digital image encryption scheme. *arXiv preprint arXiv:1204.1603*.

Patel, K. D., and Belani, S. (2011). Image encryption using different techniques: A review. *International Journal of Emerging Technology and Advanced Engineering, 1*(1), 30-34.

Patidar, V., Pareek, N., Purohit, G., and Sud, K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *optics communications, 284*(19), 4331-4339.

Pavlo, A., Paulson, E., Rasin, A., Abadi, D. J., DeWitt, D. J., Madden, S., et al. (2009). *A comparison of approaches to large-scale data analysis.* Paper presented at the Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, 165-178.

Puech, W., Bors, A., and Rodrigues, J. (2013). Protection of colour images by selective encryption. In *Advanced Color Image Processing and Analysis* (pp. 397-421): Springer.

Rad, R. M., Attar, A., and Atani, R. E. (2013). A comprehensive layer based encryption method for visual data. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 6*(1), 37-48.

Radwan, A. G., AbdElHaleem, S. H., and Abd-El-Hafiz, S. K. (2016). Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. *Journal of Advanced Research, 7*(2), 193-208.

Rajagopalan, S., Janakiraman, S., Rengarajan, A., Rethinam, S., Arumugham, S., and Saravanan, G. (2018). *IoT Framework for Secure Medical Image Transmission.* Paper presented at the 2018 International Conference on Computer Communication and Informatics (ICCCI), 1-5.

Ramalingam, B., Ravichandran, D., Annadurai, A. A., Rengarajan, A., and Rayappan, J. B. B. (2018). Chaos triggered image encryption-a reconfigurable security solution. *Multimedia Tools and Applications, 77*(10), 11669-11692.

Rao, S., Ramakrishnan, R., Silberstein, A., Ovsiannikov, M., and Reeves, D. (2012). *Sailfish: A framework for large scale data processing.* Paper presented at the Proceedings of the Third ACM Symposium on Cloud Computing, 4.

Rasmussen, A., Conley, M., Porter, G., Kapoor, R., and Vahdat, A. (2012). *Themis: an i/o-efficient mapreduce.* Paper presented at the Proceedings of the Third ACM Symposium on Cloud Computing, 13.

Rehman, A. U., Liao, X. F., Kulsoom, A., and Abbas, S. A. (2015). Selective encryption for gray images based on chaos and DNA complementary rules. *Multimedia Tools and Applications*, *74*(13), 4655-4677.

Rhouma, R., Arroyo, D., and Belghith, S. (2009). *A new color image cryptosystem based on a piecewise linear chaotic map.* Paper presented at the Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on, 1-6.

Riman, C., and Abi-Char, P. E. (2015). Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. *Information Security and Computer Fraud, 3*(1), 1-7.

Rivest, R. L. (1994). *The RC5 encryption algorithm.* Paper presented at the International Workshop on Fast Software Encryption, 86-96.

Rodriguez-Sahagun, M., Mercado-Sanchez, J., Lopez-Mancilla, D., Jaimes-Reategui, R., and Garcia-Lopez, J. (2010). *Image encryption based on logistic chaotic map for secure communications.* Paper presented at the Electronics, Robotics and Automotive Mechanics Conference (CERMA), 2010, 319-324.

Sakthidasan, K., and Krishna, B. S. (2011). A new chaotic algorithm for image encryption and decryption of digital color images. *International Journal of Information and Education Technology, 1*(2), 137.

Sankpal, P. R., and Vijaya, P. (2014). *Image Encryption Using Chaotic Maps: A Survey*. Paper presented at the Signal and Image Processing (ICSIP), 2014 Fifth International Conference on, 102-107.

Sasidharan, S., and Philip, D. S. (2011). A fast partial image encryption scheme with wavelet transform and RC4. *International Journal of Advances in Engineering & Technology, 1*(4), 322-331.

Sattarova Feruza, Y., and Kim, T.-h. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering, 2*(2), 17-31.

Schneier, B. (1993). *Description of a new variable-length key, 64-bit block cipher (Blowfish).* Paper presented at the International Workshop on Fast Software Encryption, 191-204.

Schwartz, C. (1991). A new graphical method for encryption of computer data. *Cryptologia, 15*(1), 43-46.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal, 28*(4), 656-715.

Shuangshuang, H., and Min, L.-Q. (2014). A color image encryption scheme based on generalized synchronization theorem. *Indonesian Journal of Electrical Engineering and Computer Science, 12*(1), 685-692.

Singh, G., and Kinger, S. (2013). Integrating AES, DES, and 3-DES encryption algorithms for enhanced data security. *International Journal of Scientific & Engineering Research, 4*(7), 2058.

Singhal, N., and Raina, J. (2011). Comparative analysis of AES and RC4 algorithms for better utilization. *International Journal of Computer Trends and Technology, 2*(6), 177-181.

Skirnevskiy, I., Pustovit, A., and Abdrashitova, M. O. (2017). *Digital image processing using parallel computing based on CUDA technology.* Paper presented at the Journal of Physics: Conference Series, 012152.

Skynet. (2018). Retrieved 25/02/2018, from https://github.com/wonko9/skynet

Sobhy, M. I., and Shehata, A.-E. (2001). *Chaotic algorithms for data encryption.* Paper presented at the Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on, 997-1000.

Stonebraker, M., Abadi, D., DeWitt, D. J., Madden, S., Paulson, E., Pavlo, A., et al. (2010). MapReduce and parallel DBMSs: friends or foes? *Communications of the ACM, 53*(1), 64-71.

Stoyanov, B., and Kordov, K. (2015). Image Encryption Using Chebyshev Map and Rotation Equation. *Entropy, 17*(4), 2117-2139.

Su, Y., Tang, C., Chen, X., Li, B., Xu, W., and Lei, Z. (2017). Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. *Optics and Lasers in Engineering, 88*, 20-27.

Sui, L., and Gao, B. (2013). Single-channel color image encryption based on iterative fractional Fourier transform and chaos. *Optics & Laser Technology, 48*, 117-127.

Taneja, N., Raman, B., and Gupta, I. (2011). Chaos based partial encryption of spiht compressed images. *International Journal of Wavelets, Multiresolution and Information Processing, 9*(02), 317-331.

Taneja, N., Raman, B., and Gupta, I. (2012). Combinational domain encryption for still visual data. *Multimedia tools and applications, 59*(3), 775-793.

Tedmori, S., and Al-Najdawi, N. (2014). Image cryptographic algorithm based on the Haar wavelet transform. *Information Sciences, 269*, 21-34.

Tong, X., Cui, M., and Wang, Z. (2009). A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator. *Optics Communications, 282*(14), 2722-2728.

Tong, X., and Liu, Y. (2011). *An Image Encryption Algorithm for New Multiple Chaos-Based.* Paper presented at the International Conference on Computer Science, Environment, Ecoinformatics, and Education, 88-93.

Tong, X. J. (2013). Design of an image encryption scheme based on a multiple chaotic map. *Communications in Nonlinear Science and Numerical Simulation, 18*(7), 1725-1733.

Ullah, I., Iqbal, W., and Masood, A. (2013). *Selective region based images encryption.* Paper presented at the Information Assurance (NCIA), 2013 2nd National Conference on, 125-128.

Usama, M., and Khan, M. K. (2008). *Satellite Imagery Security Application (SISA).* Paper presented at the Multitopic Conference, 2008. INMIC 2008. IEEE International, 232-238.

Usama, M., Khan, M. K., Alghathbar, K., and Lee, C. (2010). Chaos-based secure satellite imagery cryptosystem. *Computers & Mathematics with Applications, 60*(2), 326-337.

Waghmare, S., Sikhwal, S., Nimje, S., and Pawar, T. (2017). History of Cryptography. *International Journal for Technological Research in Engineering, 4*(8), 1210-1211.

Wang, J. (2016). Digital image encryption algorithm design based on genetic hyperchaos. *International Journal of Optics, 2016*, 16.

Wang, L. Y., Song, H. J., and Liu, P. (2016). A novel hybrid color image encryption algorithm using two complex chaotic systems. *Optics and Lasers in Engineering, 77*, 118-125.

Wang, X., Qin, X., and Liu, C. (2018). Color image encryption algorithm based on customized globally coupled map lattices. *Multimedia Tools and Applications*, 1-19.

Wang, X., and Wang, Q. (2014). A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. *Nonlinear Dynamics, 75*(3), 567-576.

Wang, X. Y., Teng, L., and Qin, X. (2012). A novel colour image encryption algorithm based on chaos. *Signal Processing, 92*(4), 1101-1108.

Wang, Z., Bovik, A. C., Sheikh, H. R., and Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing, 13*(4), 600-612.

Wang, Z., Xu, Y., Suo, B., Wang, Z., Xu, J., Chen, Q., et al. (2015). *A Provenance Storage Method Based on Parallel Database.* Paper presented at the Information Science and Control Engineering (ICISCE), 2015 2nd International Conference on, 63-66.

Wei, W., Fen-lin, L., Xinl, G., and Yebin, Y. (2010). *Color image encryption algorithm based on hyper chaos.* Paper presented at the Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on, 271-274.

Wu, H., and Preneel, B. (2007). *Differential cryptanalysis of the stream ciphers Py, Py6 and Pypy.* Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 276-290.

Xiao, H.-P., and Zhang, G.-J. (2006). *An image encryption scheme based on chaotic systems.* Paper presented at the Machine Learning and Cybernetics, 2006 International Conference on, 2707-2711.

Xie, E. Y., Li, C., Yu, S., and Lü, J. (2017). On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Processing, 132*, 150-154.

Xu, L., Gou, X., Li, Z., and Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering, 91*, 41-52.

Yadav, N., and Tanwar, S. (2013). Implementation of white-box cryptography in credit card processing combined with code obfuscation. *International Journal of Computer Applications, 70*(2).

Yang, H.-G., and Kim, E.-S. (1996). Practical image encryption scheme by real-valued data. *Optical Engineering, 35*(9), 2473-2479.

Yang, Q. G., and Bai, M. L. (2017). A new 5D hyperchaotic system based on modified generalized Lorenz system. *Nonlinear Dynamics, 88*(1), 189-221.

Ye, G., and Huang, X. (2015). A novel block chaotic encryption scheme for remote sensing image. *Multimedia Tools and Applications*, 1-14.

Ye, G. D., and Huang, X. L. (2018). Spatial image encryption algorithm based on chaotic map and pixel frequency. *Science China-Information Sciences, 61*(5), 3.

Yen, J.-C., and Guo, J.-I. (2000). A new chaotic mirror-like image encryption algorithm and its VLSI architecture. *Pattern Recognition and Image Analysis (Advances in Mathematical Theory and Applications), 10*(2), 236-247.

Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., and Yunpeng, Z. (2010). *A chaos-based image encryption algorithm using wavelet transform.* Paper presented at the Advanced Computer Control (ICACC), 2010 2nd International Conference on, 217-222.

Yuan, H. M., Liu, Y., Gong, L. H., and Wang, J. (2017). A new image cryptosystem based on 2D hyper-chaotic system. *Multimedia Tools and Applications, 76*(6), 8087-8108.

Zhang, G. J., and Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications, 284*(12), 2775-2780.

Zhang, L., Wu, J., and Zhou, N. (2009). *Image Encryption with Discrete Fractional Cosine Transform and Chaos.* Paper presented at the Information Assurance and Security, 2009. IAS'09. Fifth International Conference on, 61-64.

Zhang, L. Y., Liu, Y., Pareschi, F., Zhang, Y., Wong, K.-W., Rovatti, R., et al. (2018). On the security of a class of diffusion mechanisms for image encryption. *IEEE transactions on cybernetics, 48*(4), 1163-1175.

Zhang, W., Wong, K.-w., Yu, H., and Zhu, Z.-l. (2013a). A symmetric color image encryption algorithm using the intrinsic features of bit distributions.

*Communications in Nonlinear Science and Numerical Simulation, 18*(3), 584-600.

Zhang, X., Zhu, G., and Ma, S. (2012a). Remote-sensing image encryption in hybrid domains. *Optics Communications*, *285*(7), 1736-1743.

Zhang, Y., Xia, J., Cai, P., and Chen, B. (2012b). Plaintext related two-level secret key image encryption scheme. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(6), 1254-1262.

Zhang, Y., and Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. *Communications in Nonlinear Science and Numerical Simulation, 19*(1), 74-82.

Zhang, Y., Xiao, D., Wen, W., and Tian, Y. (2013b). Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Optics & Laser Technology, 54*, 1-6.

Zhao, X., Ma, H., Zhang, H., Tang, Y., and Kou, Y. (2015). *HVPI: extending Hadoop to support video analytic applications.* Paper presented at the 2015 IEEE 8th International Conference on Cloud Computing (CLOUD), 789-796.

Zhou, N., Wang, Y., Gong, L., Chen, X., and Yang, Y. (2012). Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. *Optics & Laser Technology, 44*(7), 2270-2281.

Zhou, N., Zhang, A., Zheng, F., and Gong, L. (2014a). Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics & Laser Technology, 62*, 152-160.

Zhou, N. R., Zhang, A. D., Zheng, F., and Gong, L. H. (2014b). Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optics and Laser Technology, 62*, 152-160.

Zhu, A., Li, L., and Chen, M. (2010a). *An improved BMP image encryption algorithm based on logistic map.* Paper presented at the Computer and Communication Technologies in Agriculture Engineering (CCTAE), 2010 International Conference On, 576-578.

Zhu, G., Wang, W., Zhang, X., and Wang, M. (2010b). *Digital image encryption algorithm based on pixels.* Paper presented at the Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, 769-772.