Palestine Polytechnic University
Deanship of Graduate Studies and Scientific Research
Master of informatics

A Selective Format-Compliant JPEG2000 Image Encryption

Submitted by:

Sahar Ameen Natsheh

A Thesis submitted in partial fulfillment of requirements for the degree of Master of Science in Informatics
December, 2018

The undersigned hereby certify that they have read, examined and recommended to the Deanship of Graduate Studies and Scientific Research at Palestine Polytechnic University the approval of a thesis entitled: A Novel Selective Format-Compliant JPEG2000 Image Encryption, submitted by Sahar Ameen Natsheh in partial fulfillment of the requirements for the degree of Master in Informatics. **Graduate Advisory Committee:**

Dr. Mousa Farajallah (Supervisor),
Palestine Polytechnic University.
Signature:_____ Date:_____

Dr. Mohammad Abu Taha(Internal committee member),
Palestine Polytechnic University.
Signature:_____ Date:_____

Dr. Rushdi Hamamreh (External committee member),
Al-Quds University.
Signature:_____ Date:_____

Thesis Approved

Dr. Murad Abu Sbeih
Dean of Graduate Studies and Scientific Research
Palestine Polytechnic University
Signature:_____ Date:_____

Declaration

I declare that the Master Thesis entitled "A Selective Format-Compliant JPEG2000 Image Encryption" is my original work, and herby certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgement is made in the text.

Sahar Ameen Natsheh,

Signature:_____ Date:_____

STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for the master degree in Informatics at Palestine Polytechnic University, I agree that the library shall make it available to borrowers under rules of the library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made. Permission for extensive quotation from, reproduction, or publication of this thesis may be granted by my main supervisor, or in his absence, by the Dean of Graduate Studies and Scientific Research when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any coping or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Sahar Ameen Natsheh,

Signature:_____ Date:_____

Dedication

To my Father and Mother:

For being a great source of motivation, inspiration and endless support.

Thank you for all your sacrifices to help me becoming what I am now.

Thank you for being there during the hardest times.

Thank you for believing in me.

To my dear husband:

For believing in me and being patient with me.

For encouraging me and hold me up everytime I go down.

For making my life worth living by your support and endless love.

To my in laws:

For your support and for every advice you gave me.

To my lovely sisters and brothers for being their for me.

To my real friends for being there for me, for their true love and continuous encouragement.

Acknowledgements

This thesis could have not been concluded without the guidance, help and support of many people. I would like to express my appreciation to every person who supported me throughout the thesis project of this Masters of Informatics. It gives me a great pleasure to acknowledge Dr. Mousa Farajallah the unstoppable support, encouragement and the continuous supervision for the success of this project.

الملخص

يختلف تشفير الصور اختلافًا كبيرًا عن تشفير النص ، نظرًا لسعة البيانات المجمعة ، والتكرار العالي للبيانات في الصور ، والارتباط العالي بين البيانات في الصورة
[1]
. وبالتالي ، يصعب استخدام الطرق التقليدية في تشفير الصور حيث أن التسلسلات العشوائية المستخدمة فيها تقوم بإنشاء عدد محدود من البيانات ، مما يؤدي إلى تقييد حجم الصورة المشفرة.

في هذه الأطروحة ، أظهرنا أنواعًا مختلفة من تقنيات التشفير لنظام ضغط الصور من نوع

JPEG2000

وناقشناها من ناحية الأمان و فعاليتها في نظام الضغط المستهدف، اقترحنا نظام تشفير غير معقد يجمع بين الية التشفير البسيطة

Exclusive -Or

بالاضافة الى خوارزمية شبيهة لخوارزمية

Cipher Block Chaining (CBC)

لتحقيق مستوى الأمان المطلوب بأقل وقت تشفير؛ نظام التشفير المقترح يستهدف فقط ٧ % من بيانات الصورة.

لقد تم فحص متانة نظام التشفير المقترح

Robustness

من خلال الأداء والتحليل الأمني

security evaluation

، بالإضافة إلى سرعة التشفير. اعتمادًا على نتائج التحليل الأمني الذي تم إجراؤه على نظام التشفير لدينا؛ فإن نظامنا المطروح يظهر نتائج امان تتناسب مع معايير التشفير الانتاقائي للصور

selective encryption

؛ حيث ان مستوى الأمان في نظام التشفير يناسب تطبيقات تشفير الصور في الوقت الحقيقي

real time applications

. تم دمج عملية التشفير مع عملية ضغط الصور للحصول على افضل سرعة ممكنة لنظام التشفير.

Abstract

The image encryption is different from the text encryption; as a result of the bulk data capacity, high redundancy of image data, and the high correlation between the image pixels [1]. Thus, traditional methods are difficult to be used for image encryption as their pseudo-random sequences have a small space, which causes a restriction in the image size.

In this thesis, we showed different types of JPEG2000 encryption techniques, and discussed them in a secured and compressed (friendly) based aspects. We proposed a selective stream cipher scheme that combines Exclusive-Or encryption with Cipher Block Chaining (CBC)-like algorithm to achieve the required level of security with the minimum encryption time; the encryption scheme targets only 7% of the image data, and the encryption process is applied jointly in the compression code before the data is written to the compressed image.

The strength of the proposed cryptosystem is investigated by the performance and the security analysis, as well as the encryption speed. Depending on the results of the security analysis that is performed on our cryptosystem, our proposed system has a better key space than the previous ones (the key space is approximately as twice as the previous encryption schemes keys) based on the key space analysis, and the achieved security level is suitable for most of real time applications since it only targets a small fraction of image data.

Contents

List of Figures

List of Tables

List of Abbreviations

AES	Advanced Encryption Standard
BBCW	Block Based Cycle Walking
CBC	Cipher Block Chaining
CCP	Codeblocks Contribution to Packet
DES	Data Encryption Standard
DWT	Discrete Wavelet Transform
EBCOT	Embeded Block Coding with Optimized Transaction
EOC	End of Codestream
IV	Inintial Vector
JPEG	Joint Photographic Experts Group
LPS	Least Probable Symbol
LZB	Leading Zeros Bitplanes
MPS	Most Probable Symbol
MSE	Mean Square Error
MSSIM	Mean Strctural Similarity Measure
NPCR	Number of Pixel Change Rate
PRBG	Pseudo Random Bit Generator
PRNG	Pseudo Random Number Generator
PSNR	Peak Signal to Noise Ratio
PWLCM	Piecewise Linear Chaotic Map
SSIM	Structural Similarity Measure
UACI	Unified Average Changing Intensity
XOR	Execlusive Or

Chapter 1

Introduction

Recently, the JPEG2000 has been employed in many applications like digital cinema applications, archival of visual content, geospatial imaging, medical imaging, and video surveillance. [2]. This adoption is resulting from the different features that JPEG2000 has over the older JPEG standard. These features include achieving lossy and lossless compression using the same algorithm; while in JPEG two different algorithms are used (ordinary JPEG and LOCO-I algorithm)[5], and the optimized compression efficiency in the very low bit-rates; by discarding less important coding passes from each sub bit-stream; such that the distortion is minimized while the target rate is met and the compression process has been speeded up [6].This feature is useful for transmission of compressed images through a low-bandwidth transmission channel. Recently, it has been included in the Adobe Acrobat Saving/exporting formats. Lately, the awareness for JPEG2000 security has grown as a result of the wide area of adaptation for this standard in image compression. The most secure approach for the encryption was the naive method; which refers to the encryption of the whole multimedia stream with a strong cipher algorithm like AES [7]. But such an approach was inadmissible for the several requirements such as [8]:

- Maintaining the format compliance and the associated functionalities of JPEG2000 like scalability; the packets headers must not be altered or encrypted to achieve format compliance.

- Achieving higher robustness against channel and storage errors. For example, the marker codes play a role in error resilience for JPEG2000 images, and encrypting those marker codes will omit this feature[9].

- Reducing the computational effort.

Nowadays, researchers are in the hunt for more feasible encryption models;

or what is been called lightweight encryption models. They are trying to develop a secure encryption models by encrypting some parts of the original image instead of applying a naive encryption; for the sake of securing images with minimal computation complexity. In other words, those schemes use the structure of the multimedia content, and partially encrypt the content to cause an insertion of satisfactory noise to make the content incomprehensible [10].

Several methods were proposed to achieve the previous mentioned requirements; to maintain a format compliance and to minimize computational effort. Those approaches differ in their areas of applications, level of security, computational demand, and the functionalities they provide. The presented approaches fall into two categories; bit-stream-compliant and compression integrated encryption algorithms. The bit-stream- compliant algorithms encrypt only the part of JPEG2000 message that contains the actual data of the image (packet body data). As for the compression integrated techniques, the encryption occurs within the compression pipeline; we will provide more discussion on those types of encryption in the next chapter.

1.1 Problem Statement

Along with the development of network and multimedia technologies, digital images are being used more and more commonly in our lives. The digital images' security has been a concern; because they can be accessed on the Internet by anyone without any effort. The security of digital images involves several different aspects. One of the aspects includes the content confidentiality and access control; they can be addressed by encryption, meantime only authorized parties holding decryption keys can access content in clear text. This thesis focuses on protecting the confidentiality and achieving access control of JPEG2000 images.

JPEG2000 is the most recent and comprehensive suite of standards for scalable coding of the visual data. It has filled areas of application that JPEG could not provide for, especially were applications necessitate a scalable representation of the visual data. Security techniques specifically tailored for JPEG2000 media; there was a assorted types of encryption models. Those models differ in the computational complexity, security, and some of them had some effects on the standard operational structure.

Nowadays, the research of JPEG2000 image encryption is heading for the lightweight encryption; to cope with the limited resources for the real time applications. However, the amount of targeted data must tuned to meet an acceptable security level.

In this thesis, we studied different selective encryption scenarios for JPEG2000 images, provided the security and encrypted data estimation on each one, identified the most practical encryption model of them (less encrypted data with better hiding of image data), made further evaluation on it, and compared it with previous models.

1.2 Contribution

In this thesis we have produced a secure selective JPEG2000 image encryption scheme. The proposed model achieves a good hiding for image data, and the additional time to the compression time is small regarding to the simple exclusive-or operation that is provided.

In our encryption scheme, we only target the resolutions of the image that include the most sensitive data; the targeted data includes only 7% of image data. That assures having minimum encryption time and high degradation effects; while maintaining the compression ratio and compression friendliness.

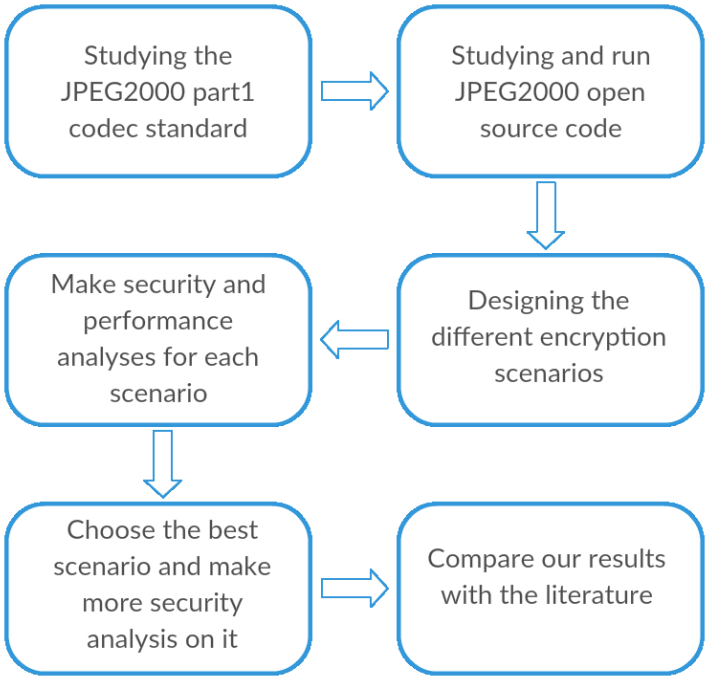
1.3 Research Methodology

Figure 1.1 represents our research methodology.

1.4 Thesis Structure

The thesis is organized as follows: the needed information and the background about thesis content is presented in Chapter 2. Chapter 3 reviews the various JPEG2000 encryption models. Where Chapter 4 covers the different encryption scenarios that are proposed in this thesis, with the most important security analysis. Chapter 5, includes additional security analysis for the final cryptographic system. And finally, chapter 6 is conclusion and future work.

Figure 1.1: Research Methodology



Chapter 2

Background

This chapter provides us with the background needed to understand this thesis. First of all, we will define the cryptography and its objectives with some security tests declaration. Then a brief elucidation for JPEG2000 image compression standard. And finally, we will discuss the different encryption technique types for JPEG2000 images.

2.1 Cryptography

In the latest decade; along with the increase of digital form of communication on the internet; multimedia data security is becoming increasingly important. The use of images and videos in the different types of applications have brought a huge attention towards security and privacy issues nowadays. Multimedia content encryption helps us to prevent unwanted and unauthorized disclosure of a confidential information in transit or storage. In general, there are three major objectives of cryptography regarding to security; confidentiality, data integrity, and authentication[11]. Confidentiality means protecting of personal information from unauthorized access. The adversary (unauthorized user) should not be able to access the data. Data integrity makes sure that the information has not been altered in any way. The authentication methods are[11]:

- Entity Authentication: It makes sure that the receiver of the message receives both the identity of the sender and his active participation during the transmission time.
- Message Authentication: It provides verification of the message senders' identity. It also holds all evidence of data integrity; if it is modified

during the transmission, then the sender is not the originator of the message.

The implicit information without any protection is called the plaintext. Data encryption is the process of hiding a particular content of the plaintext; it makes a message incomprehensible except to the intended receiver. Encrypting plaintext grants a strenuous bunk called ciphertext. Moreover, the process of retrieving the plaintext from the ciphertext is called decryption[11].

2.2 Fully Versus Selective Encryption

There are two main types of image encryption techniques: fully and selective encryption. While the selective encryption encrypts a specific parts of the image data; the data is selected using either pseudo-random sequence for the locations, based on a secret step size, or based on a specific criteria. The fully encryption encrypts the whole image data and it has a large complexity compared to the selective encryption [12]. In the other hand, selective encryption leaves some parts of the image without encryption. Nowadays, researchers are tending to use selective encryption and tune the selectivity in a manner that ensures an acceptable data security level.

2.3 Stream Cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream)[13]. In a stream cipher, each plaintext digit is encrypted with the corresponding digit of the keystream; one at a time, to generate a digit of the ciphertext stream. In practice, a digit represents a bit of the data, and the combining operation is an exclusive-or (XOR).

The keystream is typically generated successively from a random seed value using digital shift registers in a pseudorandom number generators. The seed value is considered to be a cryptographic key for decrypting the ciphertext stream. Stream ciphers represent a different approach from block ciphers. Block ciphers operate on large blocks of digits with a fixed transformation, while stream ciphers usually execute at a higher speed than block ciphers and have lower hardware complexity [11].

2.4 Pseudo Random Number Generator

A PRNG is an algorithm that generates a sequence of number-wise behavior based on a seed. It simulates the behaviour of original random number generators. Each generated number is independent of the other numbers, and therefore is unpredictable. Different PRNG's must have pass various requirements, such as randomness, unpredictability, and sensitivity to secret key[14].

A PRNG has an arbitrary starting state, which is generated using a seed state. With PRNG's , many numbers are generated in a short time and can also be reproduced any time[15]; if the starting point in the sequence is known. Generally, the PRNG consists of three main parts; see figure 2.1:

- Initialisation function: it takes a number (the seed), and puts the generator in the initial state.
- Transition function: it updates the state of the generator.
- Output function: it transforms the current state to create a fixed number of digits.

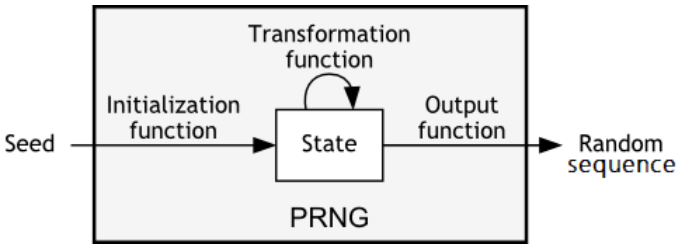


Figure 2.1: Generalization of a pseudo-random number generator.

Some examples of PRNGs are Lagged Fibonacci generator, linear congruential sequences [16], /dev/random number generator [17], Yarrow number generator [14], Salsa20 [18], Blum-Blum-Shub Generator [19], and the generator in [20] that uses three discrete chaotic maps. PRNGs are used in cryptography, AI algorithms, gaming and many other areas.

2.5 Security Analysis of Encrypted Image

Security investigation aims to discover the weakness of a cryptosystem, and recovers the entire ciphered message, or converts the secret key without knowing the decryption key or the algorithm. A good encryption scheme should

be immune to all kinds of known attacks; such as known-plain-text attack, cipher-text only attack, statistical attack, differential attack, and various brute-force attacks [21]. The most common cryptographic attacks are listed below:

2.5.1 Key Sensitivity Analysis

A secure algorithm must be totally sensitive to secret key, which indicates that the encrypted image can't be decrypted if any modification happens to the secret key. Which means that any slight change in the secret key will generate a completely different ciphered image [22].

2.5.2 Key Space Analysis

Key space analysis aims to investigate the immunity of a cryptosystem against the brute force attack. The key space should be huge in order to make exhaustion attack unworkable. It suggests that the secret key size must be at least 128 bits. The attempts to discover the decryption key by checking all possible key values and the number of attempts to discover the key space of a cryptosystem is called the key space analysis. An encryption algorithm with a 128 bit key size takes almost 1021 years with superior computers to check all possible keys[11]. Therefore, a key with an effective and independent bits sounds resistance against brute force attacks.

2.5.3 Statistical Analysis

Shannon hypothesis suggests that it is possible to solve many kinds of ciphers by statistical analysis [23]; there is a statistical relationship between original and encrypted images. So, the encrypted image must be poles apart from the original one. Some examples of statistical analysis measures are histograms, entropy analysis, and Peak Signal To Noise Ratio (PSNR.

2.5.3.1 Histogram Analysis

In statistical analysis, a histogram is used to show the frequency of pixel values appearance in an image. When applying the encryption algorithm, a uniform behaviour of the frequency counts gives conclusion to that all pixel values are effectively masked and no information about the original image can be extracted from its cipher one. Referring to histogram analysis, we can say that the proposed algorithm is robust against statistical attacks.

2.5.3.2 Entropy Analysis

Referring to Shanon's theory [23]; the information entropy of a source message m is a metric that measures the level of uncertainty in a random variable, and is defined using the following formula:

$$H(m) = \sum_{i=0}^{2^M-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{2.1}$$

Where $p(m_i)$ is the probability of occurrence for the symbol m_i and 2^M is the total states of the information source. The entropy for a perfectly random source is equal to 8 [24]. A statistically strong encryption algorithm must have an entropy for their cipher information close to the perfect value 8; where $M = 8$.

2.5.3.3 Peak Signal to Noise Ratio

The term PSNR is an expression for the ratio between the maximum possible value (power) of a signal and the power of altering noise that affects the quality of its representation[25]. Because many signals have a very wide dynamic range;ratio between the largest and smallest possible values of a changeable quantity; the PSNR is usually expressed in terms of the logarithmic decibel scale. In cryptography, the PSNR value must be as small as possible to insure that the encryption system is secure enough. The PSNR value is calculated as follows:

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right) \tag{2.2}$$

where the MSE (Mean Squared Error) is:

$$MSE = \frac{1}{mn} \sum_{0}^{m-1} \sum_{0}^{n-1} \|f(i,j) - g(i,j))\| \tag{2.3}$$

Where f represents the matrix data of the original image, g represents the matrix data of encrypted image, m and n represent the numbers of rows and columns of pixels of the images respectively, i and j represent the index of a specific row and column, MAX_f is the maximum signal value that exists in the original image.

2.5.4 Structuaral Similarity Index Measurement (SSIM)

SSIM measurement [26] has been presented to reflect the human visual system ability to extract the structural information from the images. It is used

to measure the loss of structural information between images. The SSIM measure between two images; x and y; is applied as follows:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{2.4}$$

Whereμ_x and μ_y denote the mean of the original and encrypted images respectively. σ_x , σ_y denotes the standard deviation of the original and encrypted images and σ_{xy} represents the covariance of both images.C_1 , C_2 , and C_3 are three constants that are introduced to deal with situations where the dominators are close to zero.

SSIM values range in the interval [0,1]. A value of 0 indicates that there is no correlation between the original image and its corresponding cipher image, while a value near to 1 means that both images are nearly the same. In this situation, we have measured the SSIM metric between the previously defined original images and its corresponding images after encryption.

Mean SSIM is a single overall quality measure of the entire image [26]. MSSIM index is used to evaluate the overall image quality:

$$MSSIM(X,Y) = \frac{1}{M}\sum_{j=1}^{M} SSIM(x_j, y_j) \tag{2.5}$$

where X and Y are the reference and the distorted images, respectively; x_j and y_j are the image contents at the j-th local window; and M is the number of local windows in the image. Depending on the application, it is also possible to calculate a weighted average of the different samples in the SSIM index map. For instance, region-of-interest image processing systems may give various weights to different segmented regions in the image.

2.6 JPEG2000 Compression Standard

JPEG2000 standard was released in December, 2000; the abbreviation JPEG is a short term for Joint Photographic Experts Group that developed the standard. It was developed based on the Discrete Wavelet Transform (DWT) principles; and time by time more developments and releases were made upon this standard. Nowadays, JPEG2000 contains 14 parts [8], each part presents a new release and modification of the standard. For example, part 1 is the core coding system and contains the basic characteristics of the JPEG2000 compression, and part 8 presents some security aspects on the standard.

In general, the JPEG2000 standard is much more complex than the JPEG standard and some analysis show that the JPEG2000 compression is 30 times

more complex than the JPEG [27]. That is due to the discrete wavelet transform (DWT) and the entropy encoding processes in JPEG2000. In the other hand, it presents some features over the JPEG like better visual quality and peak signal to noise ratio (PSNR) at very low bit-rates (under 0.25 bits/pixel)[8]; this feature is useful for transmitting images in low-bandwidth transmission channels. It is also capable of compressing and decompressing the grayscale, colored, and bi-level images [8]. In addition, it allows a maximum size of a compressed image to be equal to $(2^{32}-1)x(2^{32}-1)$. And it provides lossy and lossless compression using single unified compression architecture as for as decompression. It also allows the user to select some parts of the image; that have greater importance; to be encoded with higher fidelity (resolution) compared to the other parts of the image. It also adapts the addition of watermarks, fingerprints, and intellectual property information to insure some security level in the image. Figure 2.2 shows the architecture of JPEG2000 image compression part 1 standard.

The first phase is the preprocessing of the image, it has three major functions: tiling DC level shifting and multi-component transformation. In this phase an image is; optionally; partitioned into a number of rectangular non-overlapping blocks in the case of large images in the tiling step. After that; for mathematical computation need; the samples are converted into two's complement representation in order to have an input image sample with a dynamic range that is centered on zero in the DC level shifting step. Finally, in the multi-component transformation step, the redundancy of the multiple components is reduced in order to increase the compression performance.

The second phase is actual compression; where the real compression of the image stands and the compressed code of the image is generated, it consists of three steps as follows: (1) Discrete Wavelet Transform (DWT), (2) Quantization, and (3) Entropy encoding[5]. Firstly; in DWT; each component is decomposed into a number of subbands with different resolution levels. After that, each sub-band is quantized independently by a quantization parameter; in the case of lossy compression. Then, the quantized subbands are divided into a number of codeblocks; those codeblocks has smaller size than the sub-band and they have an equal size to each others; with usually $32x32$ or $64x64$ size for better memory handling.

In DWT step each component is wavelet transformed into N_L decomposition levels called resolutions. The resolutions by an index r; ranging from 0 to N. r = 0 is the lowest resolution, which is represented by the 0LL (zero LL) sub-band, while r = N is the highest resolution, which is reconstructed from the NLL, NHL, NLH and NHH sub-bands in a specific component[28]. Figure 2.3 shows the architecture of DWT decompositions and figure 2.4 shows an example of two levels of decompositions applied on lena image.

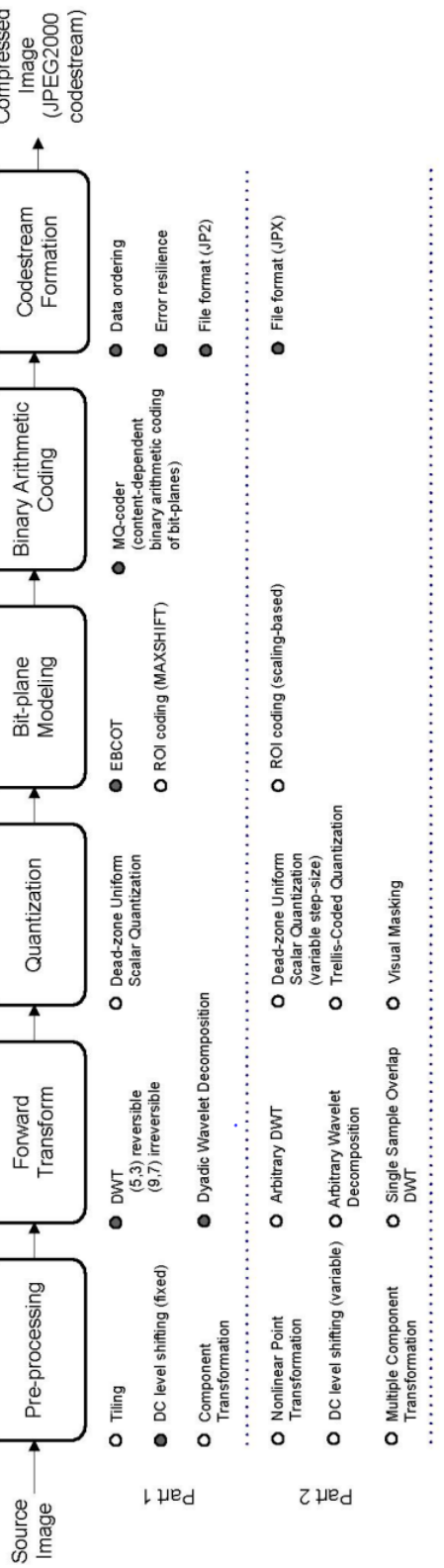


Figure 2.2: JPEG2000 image compression architecture [2].

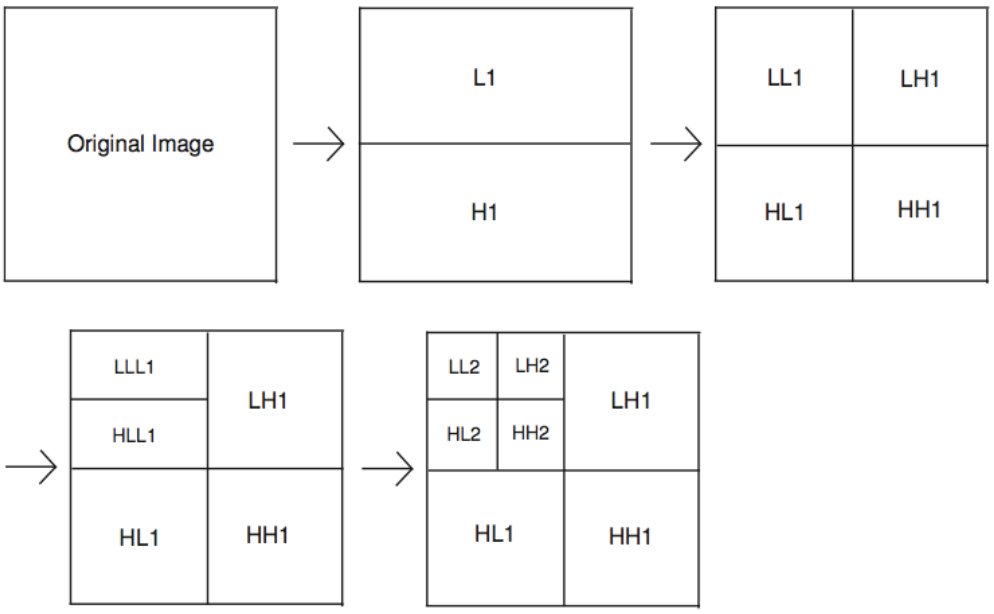


Figure 2.3: Architecture of DWT Decompositions.

Finally; in the entropy encoding step; the quantized wavelet coefficients of each codeblock in each subband are compressed in Tier-1 coding that employs the embedded block coding with optimized transaction (EBCOT) algorithm to generate a form of context and decision pairs for each bitplane; a bitplane is a binary representation of a specific value in the codeblock. Those context-decision pairs are used to select an estimated probability from a lookup table that is used by the MQ-coder to generate the compressed code.

The final phase is the compressed bitstream formation or what is called the tier-2 coding, a representation of the layer and block summary information for each codeblock is formed in this phase. The block summary consists of the most significant magnitude bitplanes where any sample in the codeblock is non-zero, the length of the compressed codewords in the codeblock, truncation point between the bitstream layers and other information. This information is received at the decoders' side as a form of two tag trees; one for bitstream layers and the other for zero bitplanes information.

The JPEG2000 codestream consists of headers [3]; main header, tiles headers, and tile part header; and packets that each of which contain packet header and packet body. Main header and tile part header contain information about the compression parameters, such as image size, tile size, code-

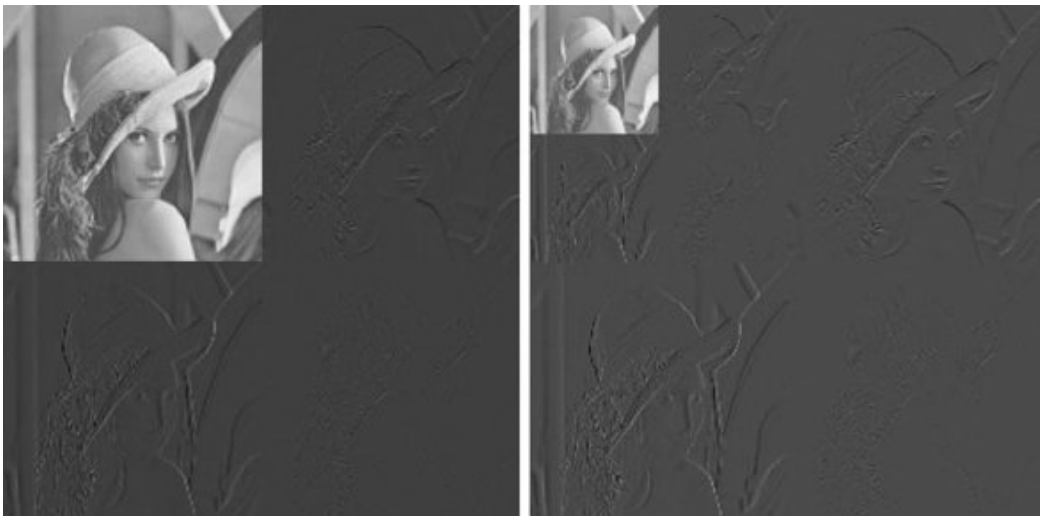


Figure 2.4: 2 Level Decomposition on Lena Image.

block size and the number of components. The packet header contains inclusion information for each codeblock, the lengths of codeblock contributions to the packet (CCPs), the number of contributed coding passes for each codeblock, and the number of leading zero bitplanes for each codeblock (LZB). Figure 2.4 shows the format of a JPEG2000 message.

Moreover, the JPEG2000 codestream has some preserved values called marker codes; each of which is a specific delimiter of the codestream content. The preserved codewords cause crash to the decoder; if they were generated within the codestream; are the codewords which marks the end of a codestream or packet; those marker codes exceed the value of $0xff8f$. Table 2.1 presents some marker codes for JPEG2000 part 1 standard[8].

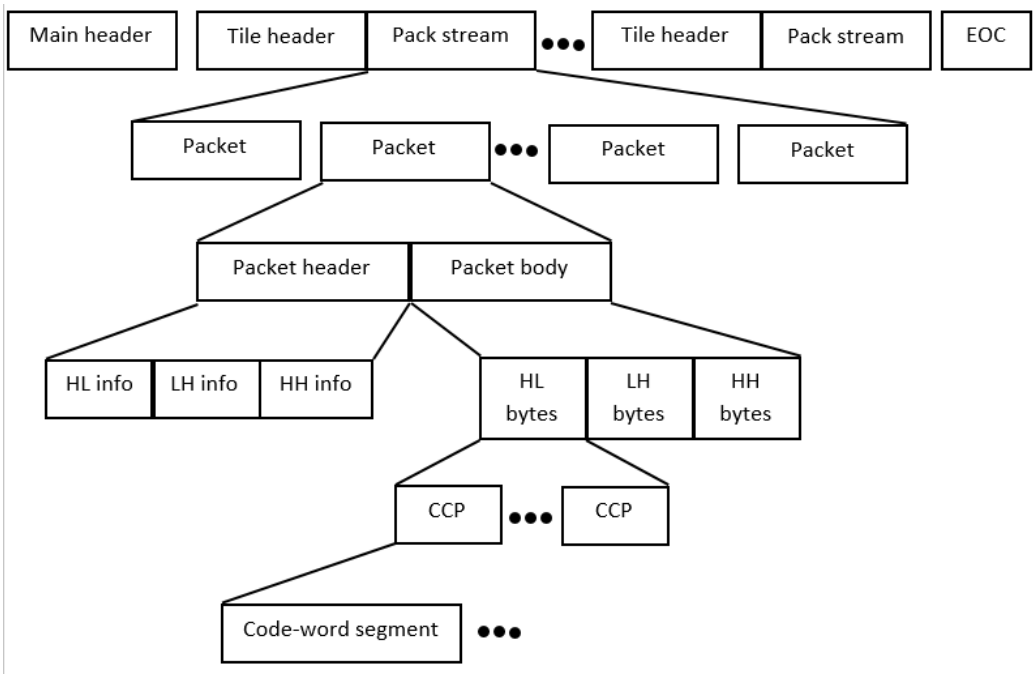


Figure 2.5: JPEG2000 Codestream Format. [3]

Table 2.1: JPEG2000 Part 1 Marker Codes.

Marker code name	Marker value
Start of code-stream	$0xff4f$
Start of tile	$0xff90$
Start of data	$0xff93$
End of code-stream	$0xffd9$
Image and tile size	$0xff51$
Coding style default	$0xff52$
Coding style component	$0xff53$
Region of interest	$0xff5e$
Quantization default	$0xff5c$
Quantization component	$0xff5d$
Progression order change	$0xff5f$
Tile-part lengths	$0xff55$
Packet length (main header)	$0xff57$
Packet length (tile-part header)	$0xff58$
Packed packet headers (main header)	$0xff60$
Packed packet headers (tile-part header)	$0xff61$
Start of packet	$0xff91$
End of packet header	$0xff92$
Component registration	$0xff63$
Comment	$0xff64$

Chapter 3

Literature Review

3.1 JPEG2000 encryption methods

The main idea in the image encryption is to transfer the image securely over the network so that unauthorized users cannot be able to decrypt the image. The image content have special properties such as bulk capacity, high redundancy and correlation between the pixels that require special necessities in any encryption technique [29]. The encryption techniques of JPEG2000 fall into two categories; bit-stream oriented and compression integrated.

In the following section we present the various approaches of JPEG2000 encryption that fall under the two categories. For further information about JPEG2000 encryption techniques, you can refer to [3].

3.2 Review on JPEG2000 Encryption Techniques

3.2.1 Compression Integrated Techniques

In the compression integrated techniques, the encryption occurs within the compression pipeline as a secret part of the compression; it can be located within one of the three main phases of JPEG2000 image compression (DWT, entropy encoding, or in MQ-coder), some of them encrypt all of the data and the others encrypt some specific parts of the JPEG2000 packets. The main constraint on those techniques is that whether they can be implemented with compliant encoders and decoders or not, also they have to maintain the compression ratio.

As for the DWT packets encryption techniques, before 2009 all of the researchers tended to make the wavelet decompositions occur based on a key (isotropic [30]or anisotropic wavelet decomposition[31]), this kind of encryp-

tion was insecure, adds a high level of complexity to the compression process, and needs some special decoders for the image. Nowadays, the researchers tend to encrypt the wavelet packets after they are decomposed (during the entropy encoding phase), they target the DWT coefficients along with the sign matrix related to them. This new trend is more secure than the old one, but there still a distortion occur in the decrypted images; because there are some losses in the data during the entropy encoding for coefficients in the image

As for the arithmetic coding techniques (that target the MQ-coder), they encrypt the coefficients that are to be contained in the packet bodies; by generating a secret lookup table in MQ-coder. It adds a negligible overhead to the compression process, differ in the security level, and the image cannot be decoded without the encryption key. But there are also some loss of data during this phase in compression process.

The compression integrated techniques are better than the bit-stream oriented techniques in the computational demand point of view; they are considered to be faster than the format compliant techniques because they intersect with the compression process. In the other hand, this type of compression usually affects the compression ratio and causes some distortion in the decrypted-decompressed image; because there are some losses in the data during the entropy encoding phase in the compression; and sometimes they modifies the JPEG2000 compression standard, which results on encrypted image not being decompressed with a standard decompresser, which is important for business applications.

3.2.1.1 Discrete Wavelet Transform Encryption

3.2.1.1.1 A New Algorithm of the Combination of Image Compression and Encryption Technology Based on Cross Chaotic Map

Tong et. al. algorithm consists a confusion-diffusion structure; the confusion process is proposed by cross-chaotic map and cipher-text feedback[32], and the diffusion process is applied using a key and modulus operation. Those processes are combined with the image compression and applied on the low frequency region in the wavelet packets that are formed from the DWT phase.

As for the confusion process, each row of image pixels is moved toward a direction as well as each column. Each row and each column has a moving direction variable q and a displacement variable p. when q=0, the row does a left loop or the column does an upward cycle movement, and when q=1, the row does a right loop or the column does a downward cycle movement; the movement of the row and the column is circular.

Compression performance: The provided a model that performs some

level of distortion in the image after decryption, the encryption time depends on the image size but it is fast compared to DES and AES. The PSNR of the proposed algorithm between original and decrypted images is 28.67; which indicates a moderate level of distortion in the decrypted image. As for the timing, the proposed model adds a negligible overhead to the JPEG2000 codec standard.

Security: The algorithm is immune to known plain-text. The histogram of the encrypted image is near to uniform, the average of NPCR and UACI values are 0.996 and 0.333 respectively; which means that the algorithm is resistant to differential attacks.

3.2.1.1.2 An Encryption Then Compression System for JPEG2000 Standard Watanabe et. al.'s procedure encrypts the image after DWT is applied [33]. The DWT coefficients are encrypted with two types of encryption schemes based on pseudo-random number generator (PRNG) with a secret key. The first scheme is sign scrambling, a sign matrix S is generated based on the secret key; the matrix has a size equal to the image size and each value in it is either 1 or -1. Then, the DWT coefficients are scrambled by multiplying each value with the corresponding value in S. The second scheme is block shuffling of DWT coefficients. The proposed technique combines the two encryption schemes by applying the sign-scrambling followed by the block- shuffling.

Compression performance: When applying lossless compression; if small sizes of blocks are used, some distortion in the reconstructed image will occur. In order to reduce distortion,larger block sizes must be used. But surely, there is a distortion in the case of lossy compression; because they apply their encryption before the quantization phase of JPEG2000, which is applied in the lossy compression. The method adds a small effect to the compression time.

Security: Their model is immune to brute force attack; the key size is 256 bits. The authors did not discuss any further security tests.

3.2.1.2 Entropy Encoding Encryption

3.2.1.2.1 JPEG2000 Compatible Layered Block Cipher Stream Memon built a method for joint compression [34]. Assuming we have a plain image p(x,y) with size of NN, after the image is wavelet transformed and a bit-plane decomposition to generate eight binary images of each sub-band is done, each one of those binary bit-planes is xored with a pseudo-random sequence that is generated by a chaotic neural network (CNN), then the first

four bit-planes are xored with a sequence generated by a 5^{th} order CNN model.

Compression performance: The effect of the encryption method on the compression ratio was not investigated, but it is known that there are some losses in the data during the arithmetic coding phase [35]. The proposed technique uses two types of neural networks, one is chaotic and the other is cellular neural network, the two neural networks are considered to be fast.

Security: The method uses a 256-bit key for the two neural networks which is considered to be secure against brute force attack. And all of the wavelet sub-bands are encrypted and no data is left in plain. In addition, a double encryption is applied to the four most significant bit-planes which increases the security of the proposed method. The histograms of the encrypted images are near to uniform which indicates the pixel distribution density against intensity level.

3.2.1.2.2 A New Joint Lossless Compression and Encryption Scheme Combining a Binary Arithmetic Coding With a Pseudo Random Bit Generator

In this paper, Masmoudi et. al. proposed a scheme which performs both lossless compression and encryption of data. The lossless compression is based on the arithmetic coding (AC) and the encryption is based on a pseudo random bit generator (PRBG). Thus, the plaintext is compressed with a binary arithmetic coding (BAC) whose two mapping intervals are swapped randomly by using a PRBG. They proposed a PRBG based on the standard chaotic map and the Engel Continued Fraction (ECF) map to generate a keystream with both good chaotic and statistical properties[36].

Compression performance: In this paper, they mentioned that the scheme conserves the compression efficiency. But the studies on JPEG2000 standard says that there are some loss in the data even in the lossless compression in entropy encoding [35]; which was assured during our studying and application for the standard. As for the computational time manner, there is a slight overhead added to the compression standard.

Security: The method uses a 157-bit key which is considered to be secure against brute force attack. And it is immune against statistical attacks.

3.2.1.3 MQ Coder Encryption

3.2.1.3.1 A New Lightweight JPEG2000 Encryption Technique Based On Arithmetic Coding

In JPEG2000, the MQ coder encodes the binary streams using a simple lookup table. The table consists of 47 states of quantised probabilities[8], each state corresponds to a different probability map which can be represented by probability of Least Probable Symbol

(LPS) and Most probable Symbol (MPS). At the beginning, the MQ coder generates an initial state i, and determines whether a received input bit is the LPS or MPS, the next state is determined to be M_i or L_i. However, if the switch flag is set, then the coder changes the value to MPS or LPS. The coding technique is based on interval swapping at each state of the MQ coder table. Tong et. al's. method linked the coding technique with the encryption key[37], the key of 94-bit length is generated for each code-block. The key is conjuncted with each destination state as k_i^M and k_i^L, each of which presents one key bit for state i and associated with M_i and L_i respectively.

Compression performance: The compression rate was not discussed in the work. The proposed method slightly influences the compression time, the additional time is the time it takes to generate the key for the current code-block.

Security: The technique is immune against known plain and cipher text attacks. It uses 256 bit key to generate the sub-keys which make it immune against brute force attack. The maximum SSIM measured for the encrypted images was 0.389 for high resolution images and 0.15 for low resolution images. And the PSNR is 8.84dB. The proposed algorithm is sensitive to the key, if the encrypted data is decrypted using a different key a mean value of SSIM is 0.026 is resulted.

3.2.1.3.2 Secure MQ Coder: An Efficient Way to Protect JPEG2000 Images in Wireless Multimedia Sensor Networks Xiang et. al. model is a simple and fast joint encryption method [38]. The basic idea is altering the values of Qe in the probability estimation with some secret values. The secret values are generated using PRNG with a key then added to Qe value.

Compression performance: A proper value of R must be selected in order to not affect the compression performance while keeping an acceptable level of security strength, but in general there is a small degradation of the compression performance. On the other hand, the encryption method doesn't influence the compression time because the table is created once.

Security: The technique is immune against know plain-text attack. They used the initialization vector in order to make the result of encrypting the same image using the same key different any time. The mean structural similarity measure (MSSIM) values for the encrypted images are lower than 0.1.

3.2.1.3.3 Efficient Selective Encryption for JPEG2000 Image Using Private Initial Table Liu et. al. technique is a symmetric scheme that uses a secret key and a mapping function to generate a private initial

table to encrypt the selected DWT codeblocks in the entropy coding stage of JPEG2000 coding scheme. The private initial table replaces the default one used in the modified MQ decoder. It implies that if a standard JPEG2000 decoder is used or a wrong key is entered to the modified JPEG2000 decoder, the encrypted codeblocks will not be correctly decrypted[36].

Compression performance: When using the JPEG2000 codec system in lossless mode, the compressibility equivalent to the standard JPEG2000 encoder. And no additional time was produced by the proposed model.

Security: The image can only be decrypted using the same encryption key. And the image cannot be decrypted using a standard JPEG2000 decoder.

3.2.2 Bitstream Oriented Techniques

In the bitstream oriented techniques, the encryption process is separated from the compression process. The encryption occurs after the image is compressed; usually the packet body which contains the actual image data is encrypted. This type of encryption techniques don't affect the compression ratio; because it doesn't interfere with the compression process. Those methods need to maintain the format compliance with JPEG2000; i. e. the encryption method must not generate any preserved codeword that would cause a decoder crash, such as End Of Codestream (EOC) marker code; figure 3.1 shows an example on effects of EOC marker code generation within the codestream; the marker codes of JPEG2000 bitstream are listed in table 2.1. Also, the packet size is preserved in the packet header so the plaintext size must remain the same, or in case the data size has changed; the header must be modified.

a) Original image. *b) Compressed image with generation of EOC marker code.* *c) Decompressed image with generation of EOC marker code.*

Figure 3.1: Effects of EOC Marker Code Generation on JPEG2000 Image Compression/Decompression.

Generally, the encryption algorithm must not generate any sequence in

excess of $0xff8f$ and the last byte must not be equal to $0xff$. The different methods of bitstream compliant encryption only differ in the information leakage; some models leave several parts of the image in plain text to avoid marker codes; and the computational complexity.

As we mentioned before, the bit-stream oriented techniques encrypt only the packet bodies of the image and leaves the headers as they are, this causes leakage of some information about the image; it is presented in the image headers. However, it is still secure and appropriate for some applications that are not concerned with high security level. The leakage is caused by the information included in the image headers and the tag trees that are generated for the compressed image such as leading zero bit-planes tag tree and code-block contributions to packets.

3.2.2.1 Fully Encryption Techniques

3.2.2.1.1 Chaotic-Cipher-Based Packet Body Encryption Algorithm for JPEG2000 Images Gu et. al. used symmetrical JPEG2000 images encryption method based on iterating chaotic map and some primitive operations[39]. In order to maintain the structure of JPEG2000 standard, only packet body data is encrypted because it contains all of the compressed coefficients . The packet body is divided into two byte blocks and the encryption is applied on them block by block with cipher feedback. They applied the format compliance by making an iterative encryption to the generated marker codes.

Compression performance: The algorithm doesn't affect the compression ratio and no distortion occur in the decrypted image. In the proposed algorithm they make a repeated 2-block encryption until the encrypted codeword doesn't contain any marker code; this repeated process causes additional computational cost and time.

Security: The algorithm is immune to brute force attack since the size of the key is 256 bit, it is also immune to key sensitivity attacks. In the other hand, the dynamical degradation of the PWLCM destroys the uniform distribution of the key-stream generated from the chaotic iterations of the it, and introduces many weak keys that cause large information leaking[40]. By histogram analysis the proposed algorithm can effectively eliminate the statistical information of the original image. Also the proposed algorithm is sensitive to the secret key and any change in it will not leak any information of the plain image.

3.2.2.1.2 A Format-Compliant Encryption Scheme for JPEG2000 Codestream The algorithm by Wen et. al. encrypted the code-block

contribution to packet (CCP) [41]. Each CCP contains n bytes, consider the CCP M=$m_1||m_2||....||m_n$, where || denotes concatenation and mi is a byte in the CCP. The cipher-text C=$c_1||c_2||...||c_n$, and c_i is a one byte of the encrypted text. the key S Is generated as a byte sequence and denoted as S=$s_1||s_2||...||s_n$, where s_i is a byte of the key S. If an encryption process produces any markercode then only the least significant half of the byte is encrypted or left in plain condition.

Compression performance: The algorithm doesn't affect the compression rate. As for the time, several conditions must be evaluated for each byte of the image to ensure format compliance, this causes additional computational time and cost.

Security: There is a restricted information leakage because the $0xff$ bytes are preserved. And the histogram of the encrypted image shows a close to uniformity of the encrypted pixels.

3.2.2.1.3 An Encryption Algorithm of JPEG2000 Streams for Supporting Ciphertext-based Transcoding Fu et. al. proposed a ciphertext-based transcoding hierarchical encryption algorithm (CT-HEA) for JPEG2000 streams [42]. By utilizing the rate-distortion optimized truncation, CT-HEA rearranges the compressed bitstream depending on the quality layer and the resolution of the image, and then applies a hierarchical encryption scheme to the reorganized codestream by using cryptographic functions like AES and DES. A hierarchical encryption algorithm is proposed according to the hierarchical structure of the JPEG2000 compression codestream, which includes the graph based key generation and updating.

Compression performance: There is no change in the compression rate and there is a slight overhead added to the original codec system.

Security: The proposed algorithm is resistant to the ciphertext only attack and known plaintext attack. The key size is 128-bit which makes it invincible from brute force attack.

3.2.2.1.4 Format-Compliant Encryption of Regular Languages: Block--Based Cycle-Walking Stütz et. al. technique relys on block-based cycle-walking (BBCW) [43]. The idea is that the plain-text is divided into blocks, and each block is encrypted repeatedly until it's format compliant, After each block is encrypted, the last byte of it is passed to the next iteration of the encryption to ensure the format compliance of the next blocks' encryption.

Compression performance: The method doesn't affect the compression rate since the encryption process is not overlapping with the compression process. The BBCW reduces the complexity of the regular cycle-walking. In

the other hand, the encryption time is affected by the image size and the selected block size (if the block size is small then the BBCW is infeasible).

Security: As they mentioned in the paper, on average 1/256 blocks' last byte is a $0xff$ byte that will cause data preserving. The BBCW security level depends on the used encryption algorithm.

3.2.2.2 Selective Encryption Techniques

3.2.2.2.1 Generalized Hierarchical Encryption of JPEG2000 Codestreams for Access Control Imaizumi et. al. proposed a method that generates keys from a single master key dependently[44]. The master key is initially divided into two partial keys with the same length. Then, the dependent partial keys are generated from the initial two partial keys. The user receives a key for the most backward. The user divides the received key into two partial keys, $K_{layer,x}$ and $K_{resolution,y}$. Furthermore, Keys for the other packets are generated using a hash function. Then each packet is encrypted using the corresponding key pair. They tested their encryption method on the different hierarchy levels in JPEG2000 image.

Compression performance: The model does not affect the compression ratio since it doesn't intersect with the compression pipeline. The encryption time depends on the size of the hierarchy part to be encrypted.

Security: The algorithm is resilience to collusion attack and brute force attack; since it used a 60-byte master key.

3.2.2.2.2 Selective Encryption Scheme and Mode to Avoid Generating Marker Codes in JPEG2000 Code Streams with Block Cipher Ikeda et. al. applied an iterative encryption scheme with three scenarios; they encrypted the resolution part that contains the most sensitive data (resolution 0), they also encrypted the resolution 1 part of the image, and they encrypted the first component data of the image[45]. The encryption process is applied using one of the block cipher models (AES, DES, MISTY).

Compression performance: The scheme does not affect the compression ratio since it doesn't generate any marker codes. And the added time depends on the number of resolutions and components of the image.

Security: The encrypted code streams have robustness against ciphertext attacks, known plain-text attacks and chosen plain-text attacks. But that depends on the used block cipher algorithm.

Chapter 4

Encryption Scenarios Test and Analysis

In order to propose the best solution, we have studied and discussed several encryption scenarios. Each scenario differs in the amount of encrypted data and security level. In each solution, we have encrypted a specific part of the JPEG2000 bitstream. The classification of solutions depend on two aspects; resolution level and subband number. In each solution we studied the encryption of a specific combination of resolution and subband parts. In this chapter we will review the various solution scenarios and discuss the security aspects of each one.

4.1 Generalization of The Proposed Encryption Model

As we mentioned earlier, we have applied our encryption schema on different resolution and subband combinations, then studied the level of security for each scenario. The evaluation of security level is measured based on Peak-Signal-to-Noise ratio (PSNR) as well as the Structural Similarity Index Measure (SSIM). We have located our encryption model inside the bitstream generation part of tier-2 coding phase in JPEG2000. By locating the model in tier-2 coding we assure two pros of our model; minimizing the computational complexity by encrypting the image data jointly before it is written into the bitstream, guarantee the preservation of the JPEG2000 structure, and maintain the compression ratio of the standard.

The architecture of the used Pseudo Random Number Generator (PRNG)[4] is a modification of the work provided in [46]. The system consists of two recursive filters of order one. The first recursive cell contains a modified discrete Skew Tent map, and the second recursive cell holds a discrete piecewise

linear chaotic (PWLC) map. These maps are used as non-linear functions. In order to produce the final random sequence; map outputs are combined as follows: $F[N-1] = F1[N-1] \oplus F2[N-1]$ Where N is the input sequence, F1 is a modified version of the discrete Skew Tent map in [46], F2 is the discrete PWLC map, and F is the result of combining the two map outputs. Figure 4.1 shows the architecture of the used PRNG model.

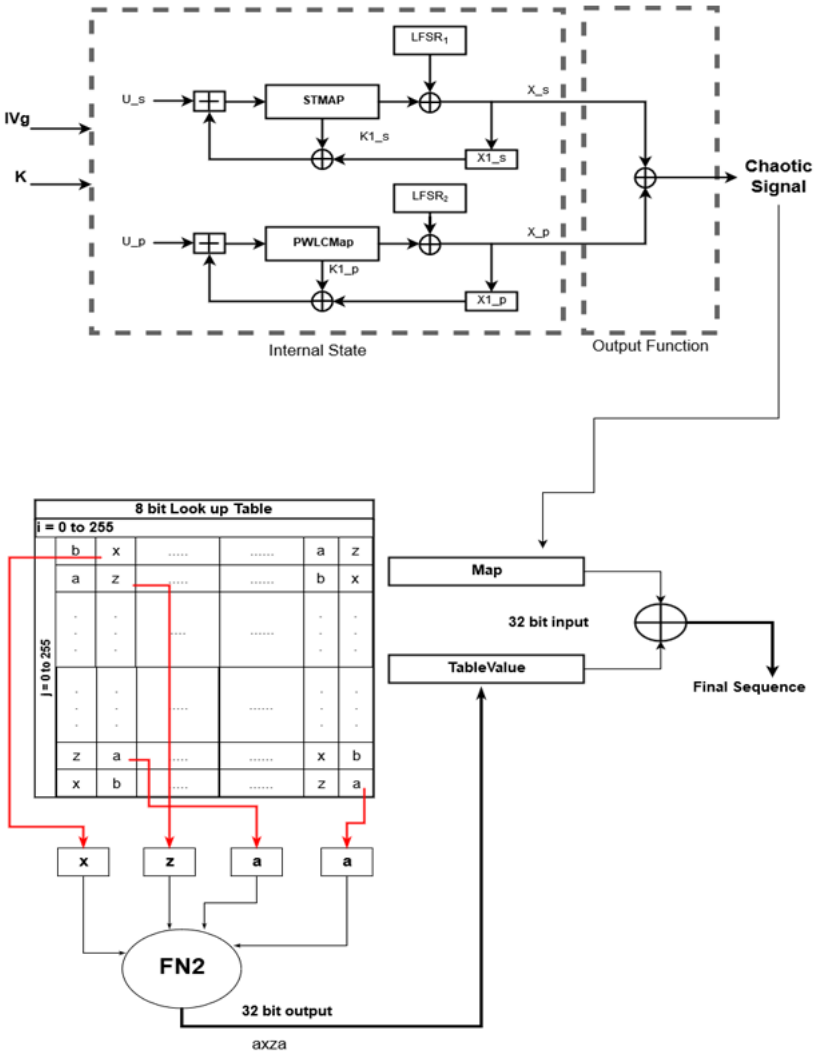


Figure 4.1: The PRNG model presented in [4]

To increase the complexity of chaotic signal, they have implemented a lookup table that is generated using the standard PRNG function; in order to guarantee that the numbers are not duplicated in the same row or column, which indicates that there is no relation between the number and its position.

Moreover, each number has the same probability distribution which confirms the random behavior. The results of the chaotic maps are combined with the results of the look-up table to generate a new sequence.

Our encryption model uses a 299 bits key as input to the pseudo-random number generator (PRNG) that is presented in [47] in order to generate a sequence of secret values. Then the secret values are used to initiate the initial vector (IV) and to encrypt the image pixels. The image values are xored with the corresponding bitstream data before it is written to the final image in CBC like stream cipher. Algorithm 1 summarizes our encryption model.

The encryption algorithm is applied as follows. First of all,a secret sequence is generated using a 299 bits master key; it is used to initialize the initial vector (IV); IV is used to encrypt the first value of the codestream in a CBC like mode; and to generate the random sequence of keys (S) that are used to encrypt image data. Then, before the data is written to the image, the encryption process occur. An application condition for the encryption scenario is checked on the current chunk of data. Then, a number r is read from the sequence S and apply modulo 255 operation in order to eliminate the values that would generate a marker code when encryption occur. And finally, the cipher value is a result of an exclusive-or operation for the plaintext value with the encryption key with cipher feedback (CBC like mode).

Algorithm 1 Generalization of encryption model.

Input: a compressed JPEG2000 bitstream, S sequence, C_{i-1}.

if scenario application condition **then**
  for $i \leftarrow 0$ to codeblock height **do**
    for $j \leftarrow 0$ to codeblock width **do**
      Get the next number r from S
      Encryption key $\leftarrow r\%255$
      $C_i \leftarrow codeblock[i,j] \oplus$ Encryption key $\oplus C_{i-1}$
      codeblock[i,j]$\leftarrow C_i$
    end for
  end for
end if

Output: The encrypted JPEG2000 stream.

Where S sequence is the generated sequence from key K_s, and C_{i-1} is the previous encrypted value; C_0 is initialized by the initial vector IV to encrypt the first block.

4.2 Encryption Scenarios

In this section, we present the different encryption scenarios, discuss the encrypted data rate, and evaluate the security level for each scenario. In the earlier chapters, we talked over the DWT in JPEG2000. In DWT, different resolutions levels are generated, and each resolution is divided into four subbands. In each new decomposition for the image the LL subband is divided into four subbands and so on. Figure 4.2 shows an example of JPEG2000 decompositions structure[44], the image has three levels of decompositions, four resolution levels, each of which contains four subbands.

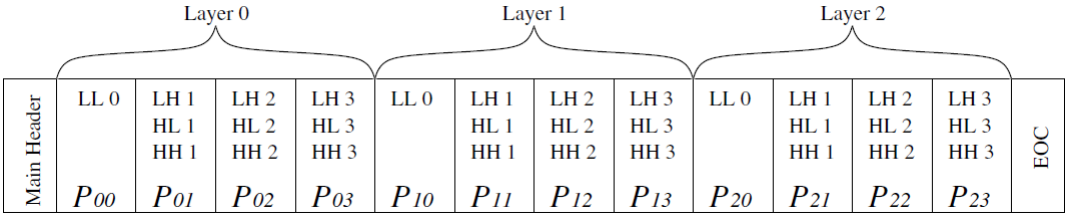


Figure 4.2: Structure of JPEG2000 Decompositions.

We applied the encryption model on several images including Lena, ship, mandril, pepper and other images, the images were taken from the USC-SIPI Image Database[48]. Each image has six resolution levels; based on the standard JPEG2000 codec system; we applied our model on different combinations of resolutions and subbands. The pursuing sections discuss the various scenarios. Figure 4.3 shows an example of test images for the encryption model that will be discussed in this documentation.

4.2.1 LL Subband Encryption

The LL subband includes the most important information of the image, any change in this subband will affect the whole of the image. When using six decomposition levels, the LL subband holds 0.097% of the image data. It is located in the first resolution of the image.

Table 4.1 presents SSIM and PSNR values for the test images. As noticed, despite the size of the LL subband; it's encryption had an accepted affect to the whole image. It had provided a good PSNR measures, but the SSIM values was not accepted.

Figure 4.4 shows the encryption results for LL subband on the different images.

It can be observed that the LL subband includes the most important data

Figure 4.3: Test images.

Table 4.1: Security Tests for LL Subband, percentage of encrypted data is 0.097 %.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.8	11.5
Lena	$512x512x1$	0.9	13.5
Pepper	$512x512x3$	0.5	8.8
Mandril	$512x512x3$	0.8	13.4

of the whole image. Although it contains only 0.09% of the image data, its encryption has a good affect on the image quality.

4.2.2 LH Subband Encryption

When using six decomposition levels, the LH subband holds 33% of the image data. It comes in the second level of data importance after LL subband. It is located in the second resolution, first subband of the image.

Table 4.2 presents SSIM and PSNR values for the test images. It had provided a good PSNR measures and SSIM values.

Figure 4.5 shows the encryption results for LH subband on the different

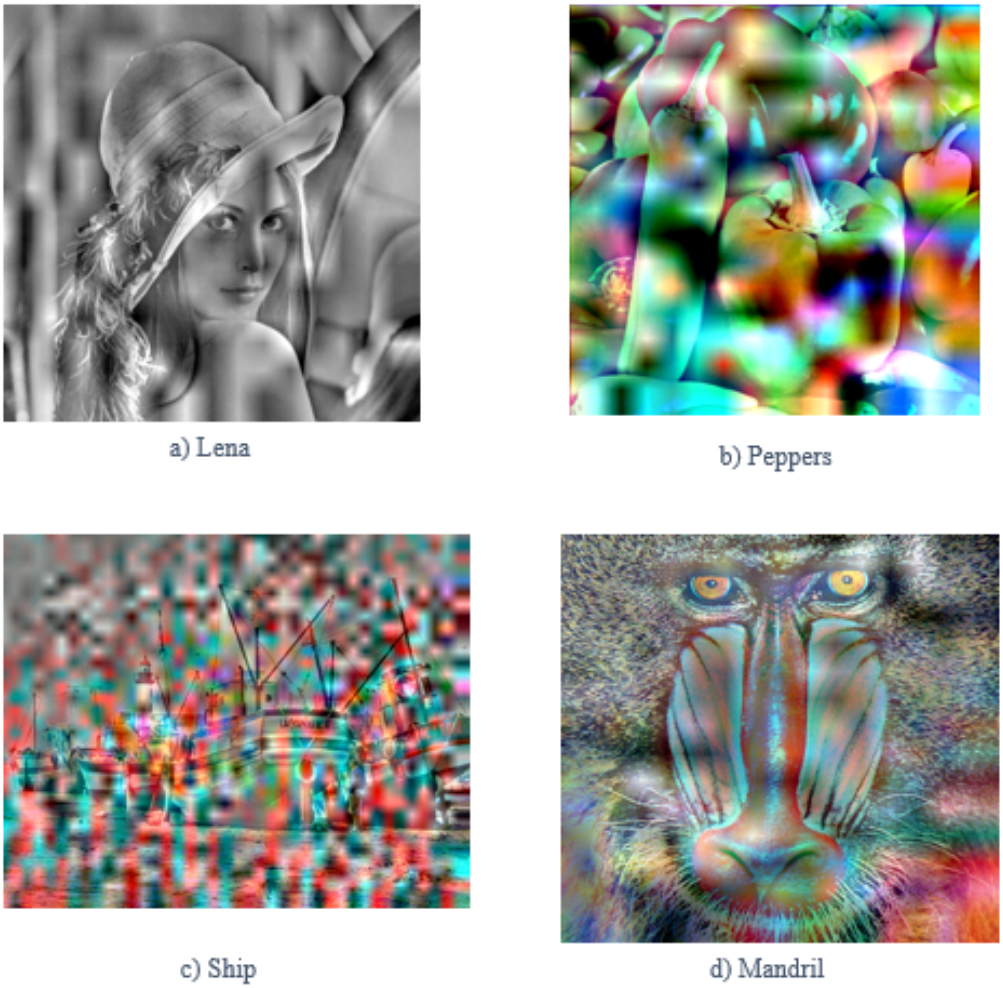


Figure 4.4: LL Subband Encryption.

Table 4.2: Security Tests for LH Subband, percentage of encrypted data is 33%.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.26	13.2
Lena	$512x512x1$	0.3	15.4
Pepper	$512x512x3$	0.2	13.7
Mandril	$512x512x3$	0.27	10.4

images.

In this scenario, the amount of encrypted data is moderate, and the security level is accepted. The results for HL and HH subbands were tested,

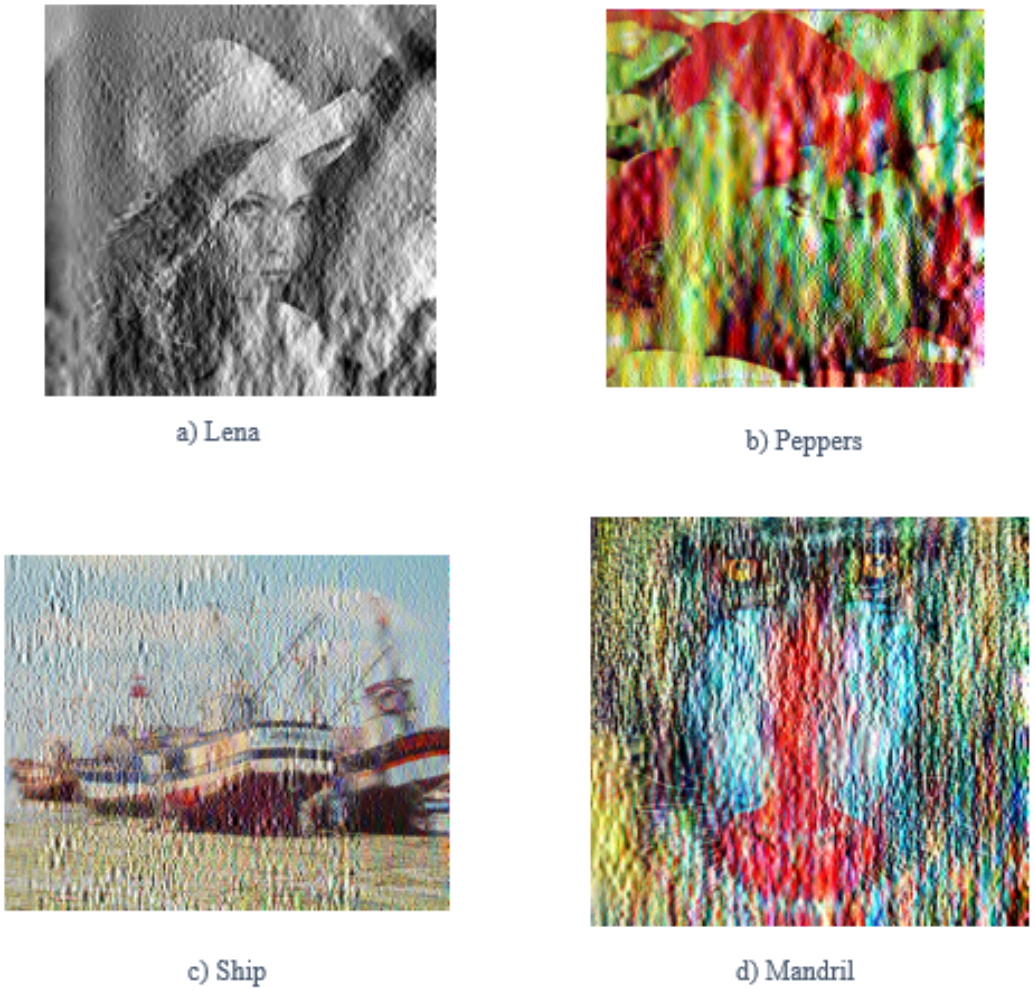


Figure 4.5: LH Subband Encryption.

they both have a close results to LH subband which concludes that their data have almost the same importance.

4.2.3 LL and LH Subbands Encryption

When using six decomposition levels, the LL and LH subbands hold 0.3339 of the image data. They are located in the first subband of the image.

Table 4.3 presents SSIM and PSNR values for the test images. It had provided a good PSNR measures and SSIM values. But there is a slight difference in the SSIM and PSNR values compared with LH subband.

figure 4.6 shows the encryption results for LL and LH subbands on the

Table 4.3: Security Tests for LL and LH subbands, percentage of encrypted data is 33.39%.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.23	8.8
Lena	$512x512x1$	0.25	11.01
Pepper	$512x512x3$	0.19	7.8
Mandril	$512x512x3$	0.29	9.02

different images.

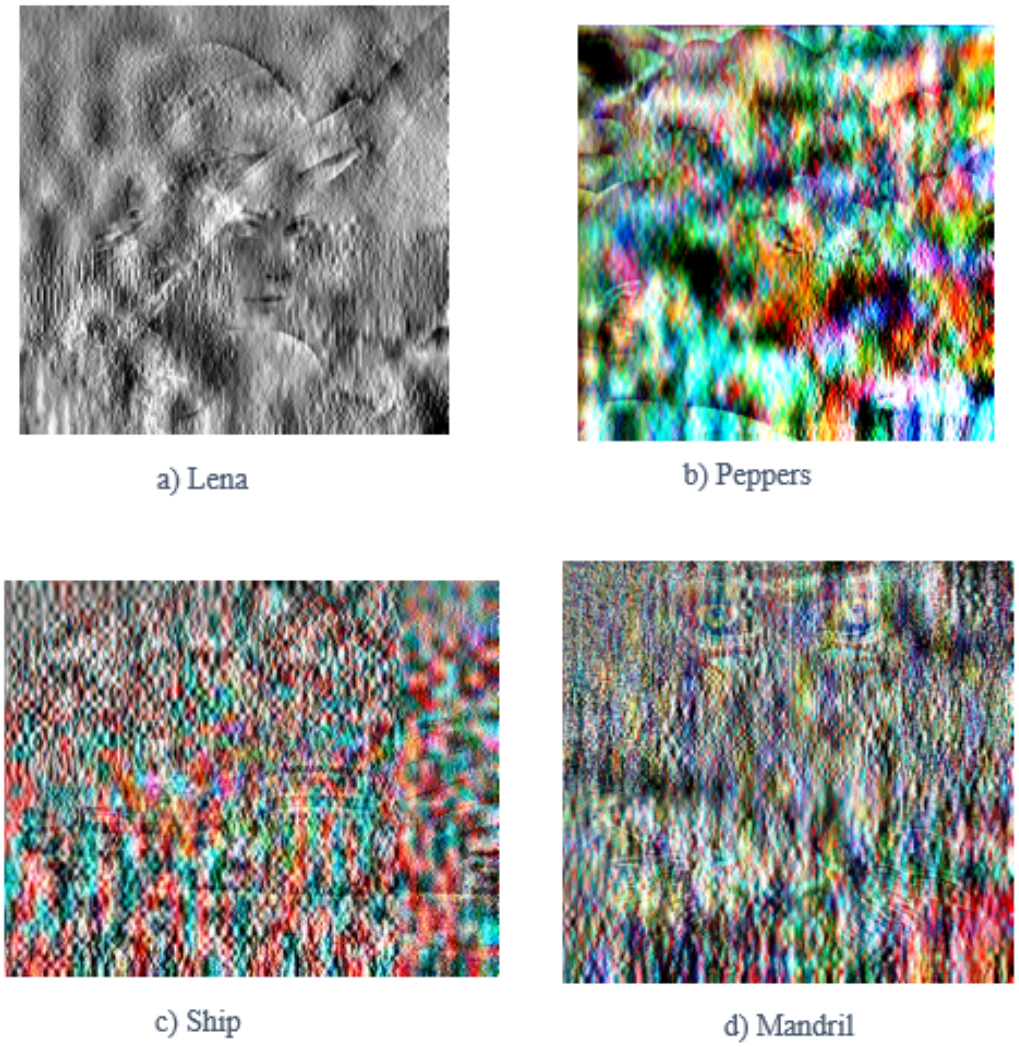


Figure 4.6: LL and LH Subbands Encryption.

This subbands combination includes almost the same amount of data for the previous scenario, but the security test results are better. The other combinations of subbands (LL and HL, LL and HH combinations) have adjacent test results, so they are not discussed in this thesis.

4.2.4 LL, LH, and HL Subbands Encryption

When using six decomposition levels, the LL, LH, and HL subbands hold 0.66 of the image data. It is located in the first and the second subbands of the image.

Table 4.4 summarizes the test results for the mentioned subbands combination. It ha an excellent security level, but the amount of encrypted data is large; so it will not be considered as a best encryption scheme.

Table 4.4: Security Tests for LL, LH, and HL subbands, percentage of encrypted data is 66%.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.15	8.2
Lena	$512x512x1$	0.17	10.5
Pepper	$512x512x3$	0.13	7.1
Mandril	$512x512x3$	0.1	7.16

Figure 4.7 shows the encryption results for LL, LH, and HL subbands on the different images.

We notice that this combination of subbands encryption has a high security level, but the amount of encrypted data is more than the half of the image size; which is considered to be large for a selective encryption model.

4.2.5 Smallest Decomposition Encryption

The smallest decomposition area of the image includes the lowest resolution data. In our case of compression, it holds 0.3% of image data. It is located in the first and second subbands of the image.

Table 4.5 summarizes the test results for the smallest decompision encryption.

Figure 4.8 shows the encryption results for the smallest decomposition encryption.

Although the percentage of encrypted data in this scenario is very small; but the security strength of it is still unacceptable, so it is not selected as a proposed solution.

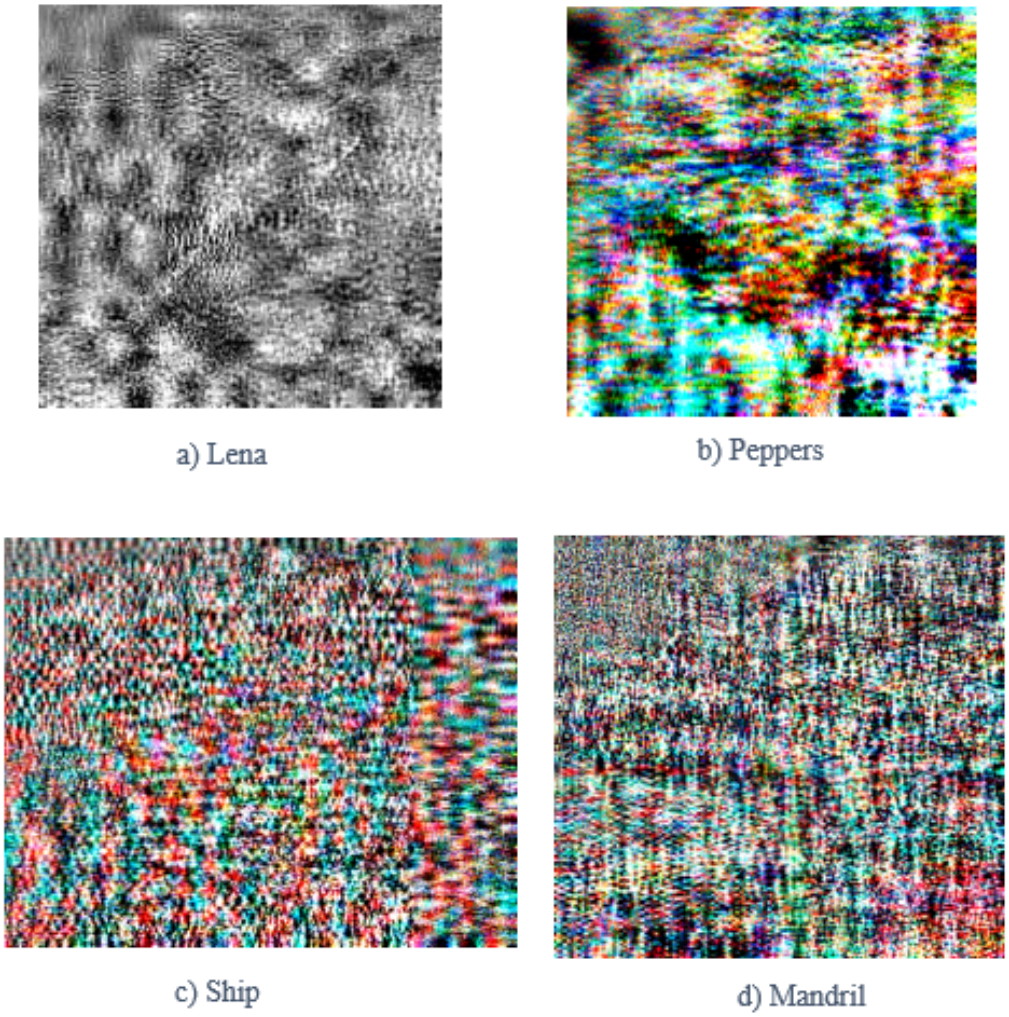


Figure 4.7: LL, LH, and HL Subbands Encryption.

Table 4.5: Security Tests for the Smallest Decomposition Encryption, percentage of encrypted data is 0.3%.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.74	10
Lena	$512x512x1$	0.84	12.9
Pepper	$512x512x3$	0.49	7.6
Mandril	$512x512x3$	0.58	10.89

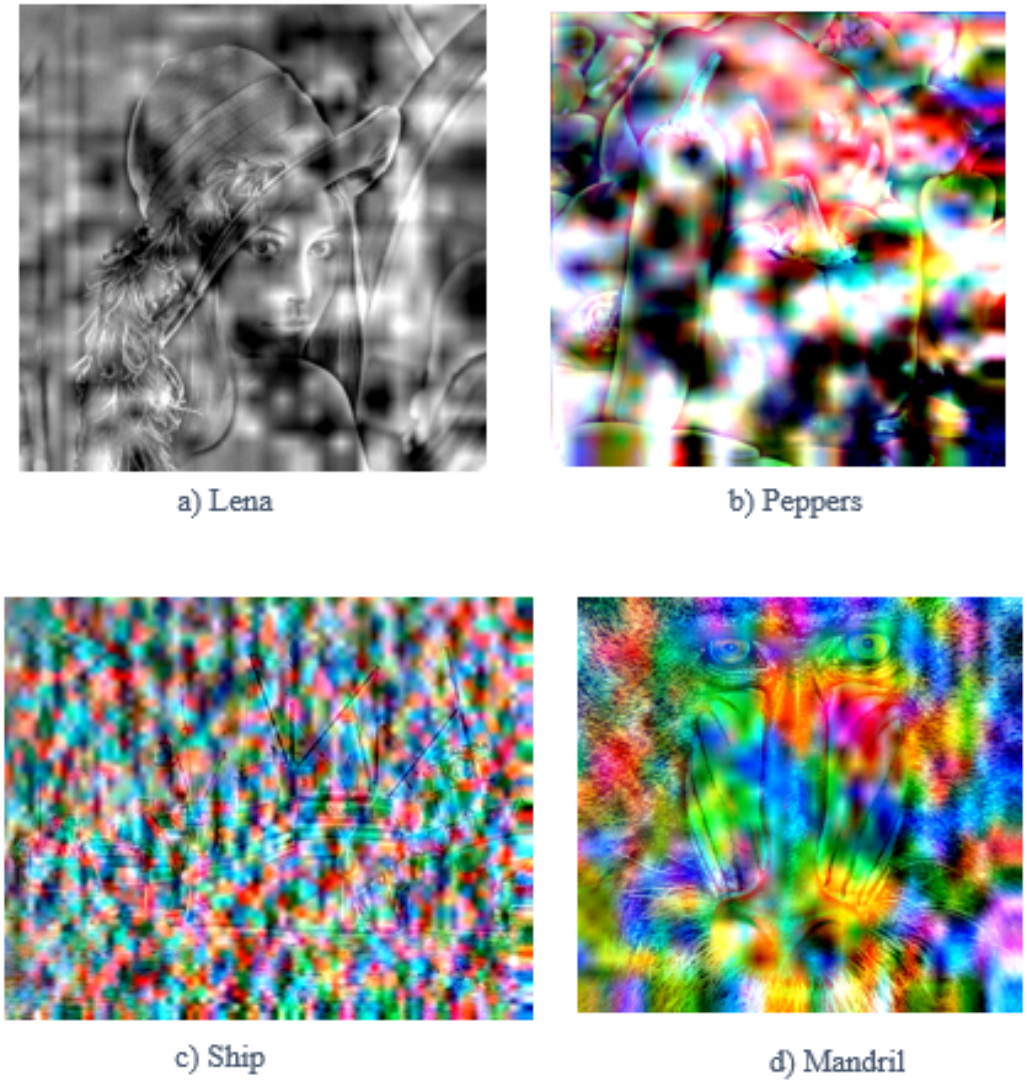


Figure 4.8: Smallest Decomposition Encryption.

4.2.6 Half of Decompositions Encryption

After studying several combinations of subbands and resolutions encryption scenarios, we came up with the most feasible solution; with a minimal data ratio encryption and accepted security level. The half of decompositions indicates the half number of resolutions in the image. For example, in the default JPEG2000 codec system the number of decompositions for the image is six, then the number of encrypted resolutions is three. The half number of decompositions contains only 7% of the whole image data. And in some

cases of small images, the encrypted data is equal to 6% of the image data.

Table 4.6 summarizes the test results for the half decomposition encryption.

Table 4.6: Security Tests for half decompositions, percentage of encrypted data is 7%.

image name	image size	SSIM	PSNR
Ship	$1280x1024x3$	0.28	8.0
Lena	$512x512x1$	0.32	10.16
Pepper	$512x512x3$	0.2	7.2
Mandril	$512x512x3$	0.37	8.2

Figure 4.9 shows the encryption results for the half decompositions encryption.

Figure 4.10 summarizes the average PSNR values along with each scenario percentage of data. We notice that the half of decompositions encryption had the best PSNR; regarding to the security level that is produced with respect to the small amount of encrypted data. The half number of decompositions encryption was selected as the best encryption model. It can be noticed that when we encrypt the half of decompositions; which include only 7% of image data; the security test results are better than the ones for LL and LH subbands combination encryption; which include 33% of the image data.

Table 4.7 summarizes the title of each encryption scenario with the percentage of encrypted data.

Table 4.7: Summarization of targeted data in each encryption scenario.

Scenario title	amuont of targeted data
LL subband	0.097 %
LH subband	33%
LL & LH subbands	33.4%
LL, LH, & HL subbands	66%
Smallest decomposition	0.3%
Half of decompositions	7%

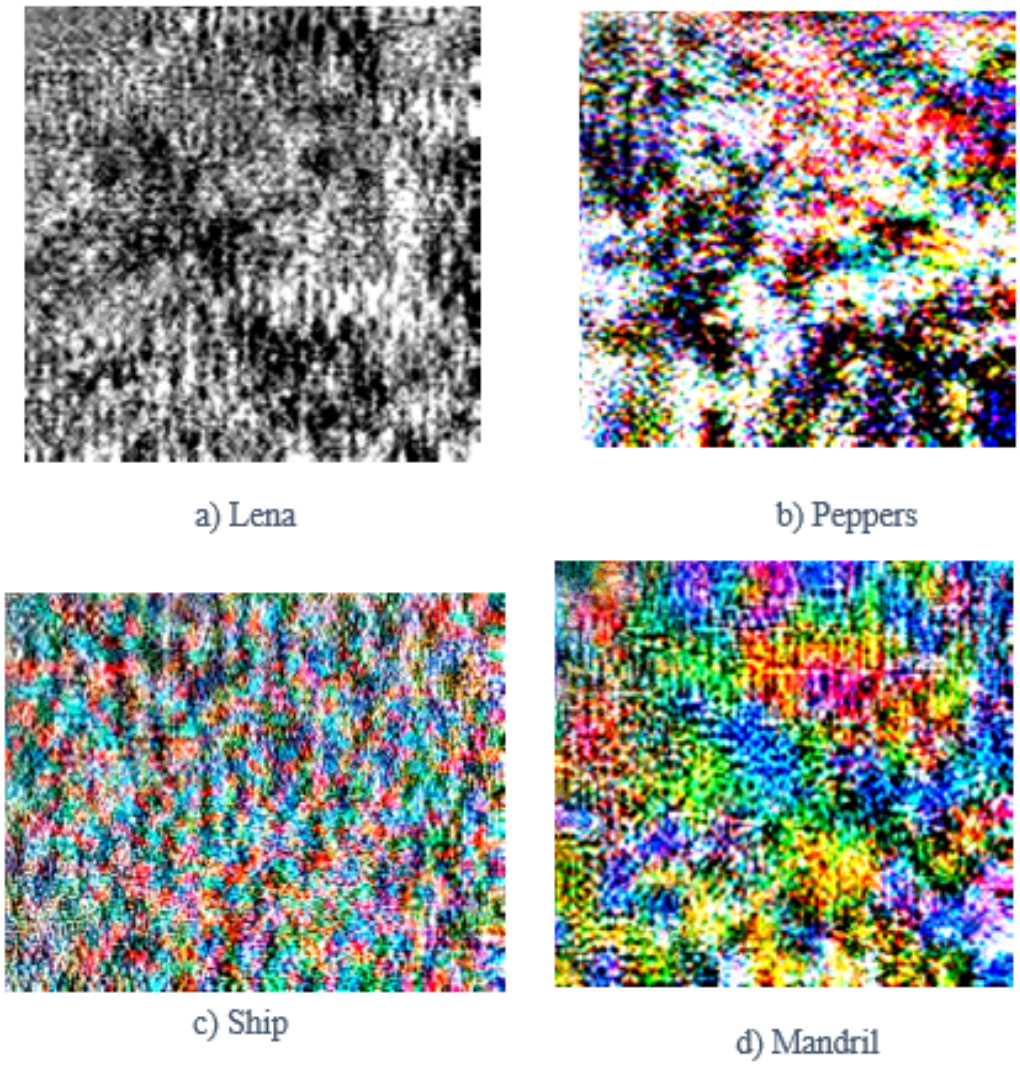


Figure 4.9: Half Decompositions Encryption.

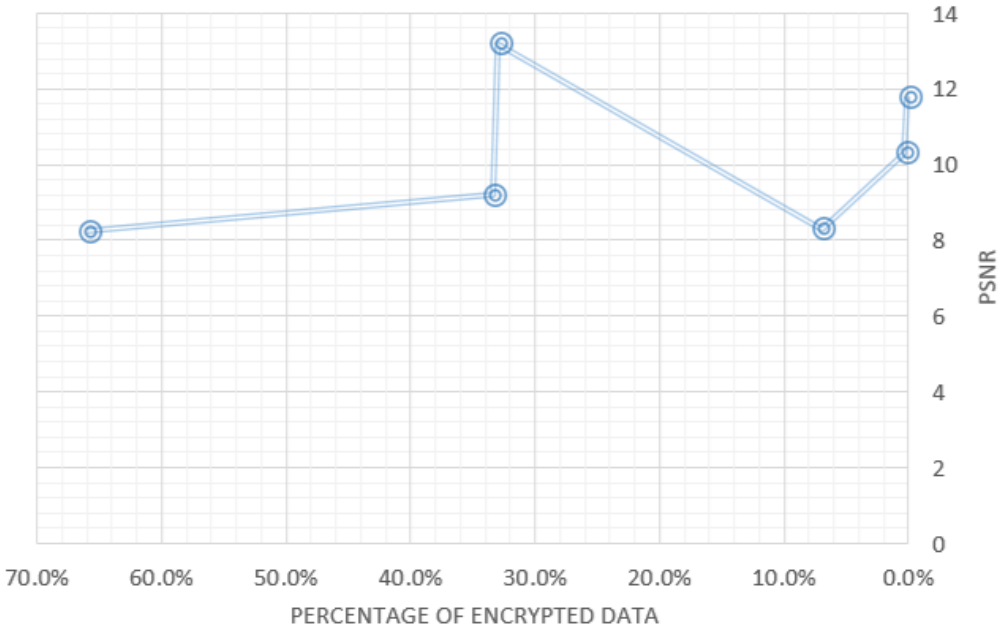


Figure 4.10: Summarization of PSNR values for testing scenarios.

Chapter 5

Proposed Solution

In the previous chapter, we discussed different scenarios for JPEG2000 image encryption. After studying the encryption strength and data encryption ratio, we found that the most feasible encryption scenario is the half decompositions encryption; regarding to the small amount of encrypted data (7% of image) and the values of PSNR and SSIM for the encrypted images.

In this chapter we will make further security tests on the proposed solution and discuss them.

5.1 Cryptosystem Design

The proposed stream cipher is applied to the encrypted JPEG2000 bitstream before it is written to the image. It is based on a simple Xor operation in cipher block chaining like encryption mode (CBC like mode). The CBC is considered to be more secure than the other encryption modes [49]; it ensures that each data chunk is encrypted differently even if it contains the same information; because it uses the cipher feedback in the encryption process. The initialization vector (IV) of the CBC mode is generated by the encryption key in order to make it unpredictable.

The encryption algorithm is listed below:

Algorithm 2 Generalization of encryption model.

Input: a compressed JPEG2000 bitstream, S sequence, C_{i-1}.

```
1: if scenario application condition then
2:     for i ← 0 to codeblock height do
3:         for j ← 0 to codeblock width do
4:             Get the next number r from S
5:             Encryption key ← r%255
6:             C_i ← codeblock[i, j]⊕ Encryption key ⊕C_{i-1}
7:             codeblock[i,j]← C_i
8:         end for
9:     end for
10: end if
```

Output: The encrypted JPEG2000 stream.

Where K_s is the 299 bit secret key, S sequence is the generated sequence from K_s, IV is the initial vector. In each iteration, a new value of the secret sequence that is generated by the secret key is used to encrypt the corresponding plain image value. Figure 4.8 shows the encryption results for the half decompositions encryption.

5.2 Security Analysis

In order to evaluate the strength of the proposed selective encryption algorithm, several quantitative metrics are employed in this chapter to measure the relationship between the plain and the JPEG2000 encrypted images, we used 20 test images to evaluate the model.

5.2.0.1 Structuaral Similarity Index Measurement (SSIM) And Peak Signal to Noise Ratio (PSNR)

SSIM values range in the interval [0,1]. A value of 0 indicates that there is no correlation between the original image and its corresponding cipher image, while a value near to 1 means that both images are nearly the same. In this situation, we have measured the SSIM metric between the previously defined original images and its corresponding images after encryption. And the results was as listed in table 5.1. The average of SSIM for the 20 test images is 0.29 which indicates that there is a good hiding for the image data regarding to the small amount of encrypted data.

Table 5.1: Some Statistical Tests and Encryption Strength Metrics for the Proposed Selective Encryption Approach.

image name	image size {in Bytes}	# of encrypted pixels	PSNR	SSIM	entropy
Ship	1280 * 1024 * 3	310272	8.1	0.28	6.5
Lena	512 * 512 * 1	16384	10.1	0.32	6.8
Pepper	512 * 512 * 3	16384	7.2	0.2	5.9
Mandril	512 * 512 * 3	16384	8.2	0.37	5.9

As for PSNR measurement, the indicator signal to noise ratio value must be as low as possible between the original and encrypted images, it signalizes that the amount of noise generated by the encryption system is good enough to hide the image data. We have tested our model on 20 images and the average PSNR was 8.03 which is secure enough for the encryption of only 7% of the image data. Table 5.1 presents a sample of PSNR values for the test images.

5.2.1 Statistical Analysis

On the subject of the cryptosystems being immune to statistical attacks, there must be a high level of randomness in the encrypted image [50]. To this conclusion, we have applied two main statistical tests to the encrypted images; histogram analysis and entropy analysis.

In Figure 5.1, histograms of the test images and their corresponding cipher ones are illustrated. Results show that histograms of the encrypted images follow a uniform distribution, which is obviously different from that of the plain images.

Table 5.1 presents the entropy results for the proposed encryption model, the average of entropy for our model is 6.2 which is close to the ideal randomness (ideal randomness is equal to 8).

5.2.2 Error Concealment Attacks

In error concealment attacks, one of the scenarios used to achieve it is by replacing all of the encrypted bits with zeros. Table 5.1 presents the PSNR and SSIM values for the test images after replacing all encrypted bits by zeros[51].

It is clear from Table 5.2, that after replacing all encryptable bits with zero, the PSNR and SSIM values keep on being low and far from the correct decoded and decrypted sequences. These results confirm the strength of the proposed scheme against this scenario of the known plain-text attacks.

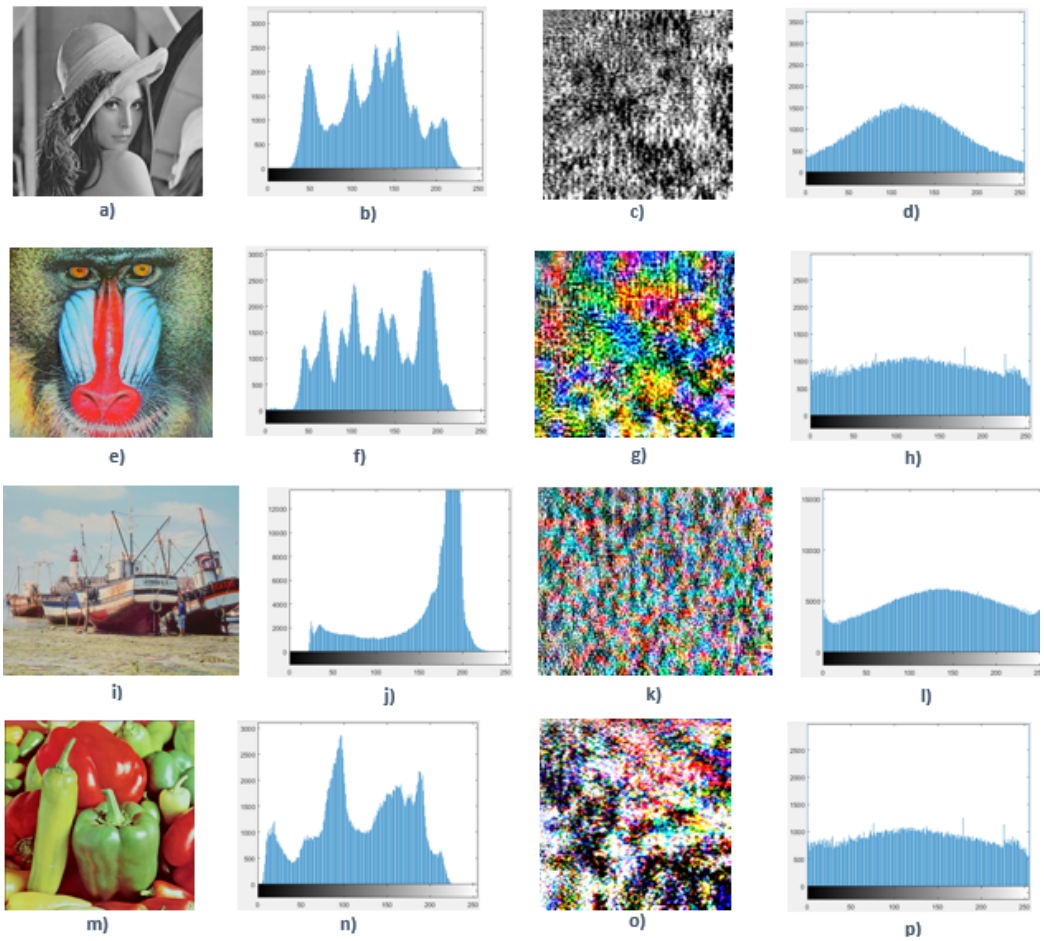


Figure 5.1: a, e, i, and m Original Lena, Ship, Mandril, and Pepper images, respectively. b, f, j, and n Histogram of Lena, Ship, Mandril, and Pepper images, respectively. c, g, k, and o JPEG-2000 encrypted Lena, Ship, Mandril, and Pepper images, respectively. d, h, l, and p Histogram of cipher Lena, Ship, Mandril, and Pepper, respectively.

5.2.3 Key Sensitivity Test

Key sensitivity test relies on how much a change on the key will affect the resulting security of the proposed cipher. A higher change means a better sensitivity of the encryption system.

In order to have enough strength against chosen plaintext and linear attacks, a selective encryption algorithm must be producing a high sensitivity against any change in the secret key. I.e. a tiny change in the key will make the decrypted image random and no information about the original image

Table 5.2: PSNR and SSIM for Replacing Encrypted Bits by Zeros.

Image name	PSNR	SSIM
Ship	7.14	0.19
Lena	7.9	0.2
Pepper	6.25	0.17
Mandril	7.2	0.17

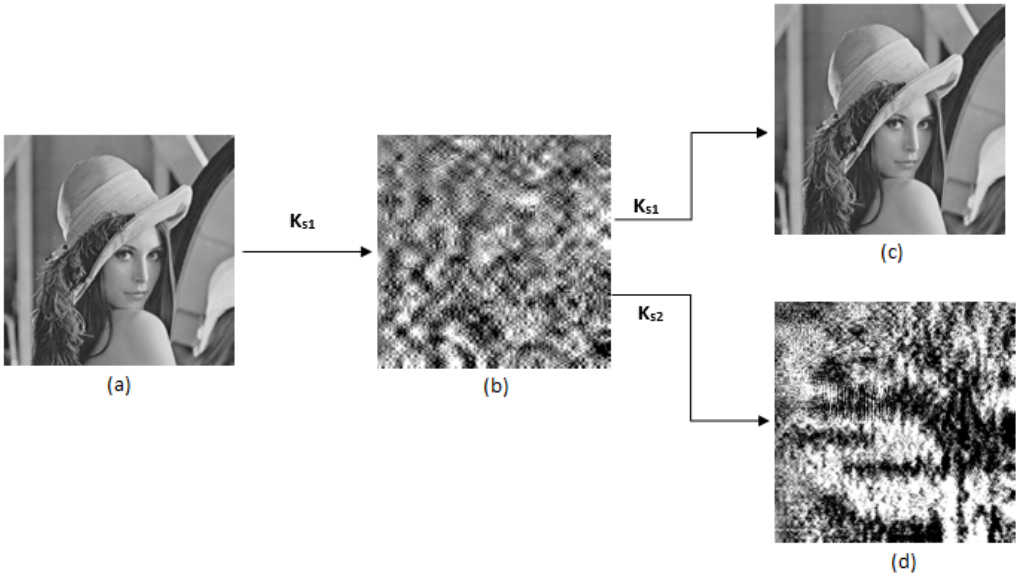


Figure 5.2: a) Lena Plain Image. b) Encrypted Lena Image using K_{s1} . c) and d) Decrypted Lena Image using K_{s1} and K_{s2} , respectively.

can be extracted from it. To test the key sensitivity of the proposed selective encryption scheme, the following scenario is performed: first, a key K_{s1} is used to encrypt the JPEG2000 Lena image. Since, K_{s1} is the right key; the decryption succeeds to recover the original image as illustrated in Figure 5.2 c. After that, another key K_{s2}; which differ from K_{s1} in one bit; is used to decrypt the same image. The decryption process is totally failed to reconstruct the original image, instead a like-random image is produced as shown in Fig. 5.2 d.

5.2.4 Key Space Analysis

From cryptography point of view, key space refers to the number of all possible combinations of keys used in encryption algorithm. This key space must

be no smaller than 128 bits long [50] to resist brute-force attacks. For this reason, the secret key; that is used to generate the secret sequence and the initial vector; in the proposed selective encryption approach consists of 299 bits. This is a fairly large key space to make brute-force attacks be infeasible.

5.3 Compression Analysis

In addition to ensuring a good security level; the proposed selective encryption model must be compression friendly. To assure that, two main concerns related to the compression aspect are evaluated in this section; the codestream compliant analysis as well as the compression friendliness assessment.

5.3.1 Codestream Compliance Analysis

A format-compliant property is one of the main characteristics that must be taken into consideration when dealing with JPEG2000 encryption. This is due to the fact that compliance allows to preserve the main characteristics and hierarchy of the original compression coding and hence it increases the robustness of image codec scheme. As a result, the decoder can correctly decode the encrypted codestream before decryption without any risk to crash.

In the proposed selective encryption approach, all values corresponding to $0xff$ are eliminated from the secret sequence before the encryption process by applying modulo 255 operation to it, then all $0xff$ values are eliminated from the packet data. Moreover, discarding the $0xff$ marker from the encrypted codestream ensures that both code-words $0xff90$ and $0xffff$ will not appear in the encrypted packet body. Which concludes that the encrypted codestream is compliant to the format of the original unencrypted codestream, and preserves all its characteristics and functionality. Table 5.3 presents an example of PSNR and SSIM values for the decrypted images compared to the original ones. the values of PSNR for all of the images are equal to infinity; which indicates that the original and decrypted images are identical, and we can assure that through the SSIM values. That confirms that the compression ratio for the images is not affected after the decryption occur, we had maintained constant bitrate, and that the proposed model is format compliant.

Table 5.3: PSNR and SSIM values for the decrypted images.

Image name	PSNR	SSIM
Ship	Inf	1
Lena	Inf	1
Pepper	Inf	1
Mandril	Inf	1

5.3.2 Compression Friendliness Assessment

To make the selective encryption approach expressive, combining compression with encryption need not influence the compression performance. Actually, most of joint compression–encryption algorithms decrease the compression ratio; since the encryption is applied before the quantization process or during the encoding process. However; by using the codestream oriented encryption schemes; encryption is applied to the compressed data in a selective manner, using the knowledge of the bitstream partitions and studying the affect of each partition encryption. Thus, it provides no influence on the compression performance; unless a marked code is generated. Also; in our scheme; no padding for bitstream were made and no additional data was inserted to the bitstream, so the packet and image sizes remain the same with/without encryption.

The proposed encryption method scheme is format compliant and the encryption is applied before the image is generated. So, the encrypted image is compliant to the format structure of the standard image. Therefore, the proposed algorithm does not affect the compression performance pointedly and satisfies the compression friendless property.

5.4 Execution Time Analysis

Time complexity of the encryption model is one of the most important constraints. Especially when dealing with limited power source or delay sensitive communications. The proposed cryptographic system encrypts only the most important 7% of the image data, and it is based on simple exclusive-or operation; the calculation of encrypted data percentage is more accurate regarding to the various operating systems and hardware resources on different computers.

5.5 Comparison with Other Works

In this section, we will compare our proposed model with other models depending on two aspects, the PSNR values along with the amount of targeted data in the encryption technique. In addition, we compared two of our scenarios in the same context, because we assume that each one is appropriate for a different application. The half of decompositions encryption is appropriate for the applications that are more concerned with the security of the encryption model. In the other hand the smallest decompositions encryption is appropriate for the real time applications that are more concerned with the encryption time than the encryption quality. Table 5.4 summarize the average PSNR values for our model compared to other three models.

Table 5.4: Comparison with other works.

Work	Amount of encrypted data	Average PSNR (dB)
A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images (2016) [39]	Whole image	8.15
Selective Encryption of the JPEG2000 Bitstream (2003)[52]	30% of image	9
Secure and low cost selective encryption for JPEG2000 (2008) [53]	5.5% of image	8.1
PS1-Half of decompositions	7% of image	8.03
PS2-Smallest decomposition	0.3% of image	10.1

It is clear from table 5.4 that the proposed solution PS1 had a lower PSNR values for the encrypted images than other two models[39] and [52] ; which target at least three times of data more than the proposed solution. As for the model in [53] it had a results close to our model but they used the AES encryption which is a complicated model compared to our model.

Chapter 6

Conclusion and Future Work

Since the wireless communication became the basement for information transmission, a secure transmission between sender and receiver has become a necessity. Also, several applications require a lightweight encryption techniques for resource limitations; such as energy and memory.

Various encryption techniques are presented in the thesis, every algorithm has its own bros and cons based on their security analysis, which were being practiced on some test images.

The proposed solution achieves configurable, format compliant, compression friendly partial encryption algorithm. It encrypts a small fraction of image data to reach a good visual distortion while guaranteeing proposing a fast selective encryption for the bitstream. In our sheme, we target the most sensitive data in the JPEG2000 bitstream; which includes 7% of image data in the default JPEG2000 codec system; this allows achieving significant time saving. We have located our encryption model inside the bitstream generation part of tier-2 coding phase in JPEG2000. By locating the model in tier-2 coding we assure two pros of our model; minimizing the computational complexity by encrypting the image data jointly before it is written into the bitstream, guarantee the preservation of the JPEG2000 structure, and maintain the compression ratio of the standard.

In the upcoming time, we intend to upgrade our scheme in order to increase the security level and apply a selective encryption combined with diffusion process.

Bibliography

[1] Xiaoling Huang and Guodong Ye. An image encryption algorithm based on time-delay and random insertion. Entropy, 20(12):974, 2018.

[2] Athanassios N Skodras and Touradj Ebrahimi. Jpeg2000 image coding system theory and applications. In 2006 IEEE International Symposium on Circuits and Systems, pages 4–pp. IEEE, 2006.

[3] Dominik Engel, Thomas Stütz, and Andreas Uhl. A survey on jpeg2000 encryption. Multimedia systems, 15(4):243–270, 2009.

[4] Mousa Farajallah, Mohammed Abu Taha, Omar Salhab, Mohammed Abu Judeh, and Noor Jweihan. Pseudo random number generator based on look-up table and chaotic maps. 2018.

[5] Athanassios Skodras, Charilaos Christopoulos, and Touradj Ebrahimi. The jpeg 2000 still image compression standard. IEEE Signal processing magazine, 18(5):36–58, 2001.

[6] KN Vikram, V Vasudevan, and S Srinivasan. Rate-distortion estimation for fast jpeg2000 compression at low bit-rates. Electronics Letters, 41(1):16–18, 2005.

[7] Joan Daemen and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[8] Tinku Acharya and Ping-Sing Tsai. JPEG2000 standard for image compression: concepts, algorithms and VLSI architectures. John Wiley & Sons, 2005.

[9] Iole Moccagatta, Salma Soudagar, Jie Liang, and Homer Chen. Error-resilient coding in jpeg-2000 and mpeg-4. IEEE Journal on Selected Areas in Communications, 18(6):899–914, 2000.

[10] Anil Kr Yekkala, Narendranath Udupa, Nagaraju Bussa, and CE Veni Madhavan. Lightweight encryption for images. In Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on, pages 1–2. IEEE, 2007.

[11] Jonathan Katz, Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Handbook of applied cryptography. CRC press, 1996.

[12] Ayoub Massoudi, Frédéric Lefebvre, Christophe De Vleeschouwer, Benoit Macq, and J-J Quisquater. Overview on selective encryption of image and video: challenges and perspectives. Eurasip Journal on information security, 2008(1):179290, 2008.

[13] Christof Paar and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

[14] Andrea Röck. Pseudorandom number generators for cryptographic applications. na, 2005.

[15] Frederick James. A review of pseudorandom number generators. Computer physics communications, 60(3):329–344, 1990.

[16] George Marsaglia. The structure of linear congruential sequences. In Applications of number theory to numerical analysis, pages 249–285. Elsevier, 1972.

[17] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to/dev/random. In Proceedings of the 12th ACM conference on Computer and communications security, pages 203–212. ACM, 2005.

[18] Daniel J Bernstein. The salsa20 family of stream ciphers. In New stream cipher designs, pages 84–97. Springer, 2008.

[19] Pascal Junod. Cryptographic secure pseudo-random bits generation: The blum-blum-shub generator, 1999.

[20] Ons Jallouli, Safwan El Assad, Mohammed Abu Taha, Maryline Chetto, René Lozi, and Daniel Caragata. An efficient pseudo chaotic number generator based on coupling and multiplexing techniques. In International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016), pages 35–40, 2016.

[21] M John Justin and S Manimurugan. A survey on various encryption techniques. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231:2307, 2012.

[22] J-R Ohm, Gary J Sullivan, Heiko Schwarz, Thiow Keng Tan, and Thomas Wiegand. Comparison of the coding efficiency of video coding standards—including high efficiency video coding (hevc). IEEE Transactions on circuits and systems for video technology, 22(12):1669–1684, 2012.

[23] Claude E Shannon. Communication theory of secrecy systems. Bell system technical journal, 28(4):656–715, 1949.

[24] Benyamin Norouzi, Seyed Mohammad Seyedzadeh, Sattar Mirzakuchaki, and Mohammad Reza Mosavi. A novel image encryption based on hash function with only two-round diffusion process. Multimedia systems, 20(1):45–64, 2014.

[25] Johannes F De Boer, Barry Cense, B Hyle Park, Mark C Pierce, Guillermo J Tearney, and Brett E Bouma. Improved signal-to-noise ratio in spectral-domain compared with time-domain optical coherence tomography. Optics letters, 28(21):2067–2069, 2003.

[26] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing, 13(4):600–612, 2004.

[27] Diego Santa-Cruz and Touradj Ebrahimi. An analytical study of jpeg 2000 functionalities. In Image Processing, 2000. Proceedings. 2000 International Conference on, volume 2, pages 49–52. IEEE, 2000.

[28] Clifford Lui. A study of the jpeg-2000 image compression standard. no. May, pages 9–14, 2001.

[29] Eduardo Bayro Corrochano. Handbook of Geometric Computing. Springer, 2005.

[30] Dominik Engel and Andreas Uhl. Secret wavelet packet decompositions for jpeg 2000 lightweight encryption. In 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, volume 5, pages V–V. IEEE, 2006.

[31] Dominik Engel and Andreas Uhl. Lightweight jpeg2000 encryption with anisotropic wavelet packets. In ICME, pages 2177–2180, 2006.

[32] Xiao-Jun Tong, Zhu Wang, Miao Zhang, and Yang Liu. A new algorithm of the combination of image compression and encryption technology based on cross chaotic map. Nonlinear Dynamics, 72(1-2):229–241, 2013.

[33] Osamu Watanabe, Akira Uchida, Takahiro Fukuhara, and Hitoshi Kiya. An encryption-then-compression system for jpeg 2000 standard. In 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 1226–1230. IEEE, 2015.

[34] Qurban A Memon. Jpeg2000 compatible layered block cipher. In Multimedia Forensics and Security, pages 253–275. Springer, 2017.

[35] Jin Li. Image compression: The mathematics of jpeg 2000. Modern Signal Processing, 46:185–221, 2003.

[36] Atef Masmoudi, William Puech, and Mohamed Selim Bouhlel. A new joint lossless compression and encryption scheme combining a binary arithmetic coding with a pseudo random bit generator. International Journal of Computer Science and Information Security, 8(1):170–175, 2010.

[37] Hassan Yakout El-Arsh and Yahya Z Mohasseb. A new light-weight jpeg2000 encryption technique based on arithmetic coding. In MILCOM 2013-2013 IEEE Military Communications Conference, pages 1844–1849. IEEE, 2013.

[38] Tao Xiang, Chenyun Yu, and Fei Chen. Secure mq coder: An efficient way to protect jpeg 2000 images in wireless multimedia sensor networks. Signal Processing: Image Communication, 29(9):1015–1027, 2014.

[39] Guosheng Gu, Jie Ling, Guobo Xie, and Zheng Li. A chaotic-cipher-based packet body encryption algorithm for jpeg2000 images. Signal Processing: Image Communication, 40:52–64, 2016.

[40] Shujun Li, Xuanqin Mou, Yuanlong Cai, Zhen Ji, and Jihong Zhang. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Computer physics communications, 153(1):52–58, 2003.

[41] Jiafu Wen, Jiazhen Wang, Bin Zhang, Zhande Li, and Zilong Huang. A format-compliant encryption scheme for jpeg2000 codestream. In Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on, pages 1038–1041. IEEE, 2010.

[42] Yong Fu, Xiaowei Yi, and Hengtai Ma. An encryption algorithm of jpeg2000 streams for supporting ciphertext-based transcoding. In Multisensor Fusion and Information Integration for Intelligent Systems (MFI), 2014 International Conference on, pages 1–7. IEEE, 2014.

[43] Thomas Stütz and Andreas Uhl. Efficient format-compliant encryption of regular languages: Block-based cycle-walking. In IFIP International Conference on Communications and Multimedia Security, pages 81–92. Springer, 2010.

[44] Shoko Imaizumi, Osamu Watanabe, Masaaki Fujiyoshi, and Hitoshi Kiya. Generalized hierarchical encryption of jpeg 2000 codestreams for access control. In Image Processing, 2005. ICIP 2005. IEEE International Conference on, volume 2, pages II–1094. IEEE, 2005.

[45] Hiroki Ikeda and Keiichi Iwamura. Selective encryption scheme and mode to avoid generating marker codes in jpeg2000 code streams with block cipher. In Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on, pages 593–600. IEEE, 2011.

[46] Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, and Mohammad Odeh. Survey paper: cryptography is the science of information security. 2011.

[47] OMAR SALHAB, NOUR JWEIHAN, MOHAMMED ABU JODEH, MOHAMMED ABU TAHA, and MOUSA FARAJALLAH. Survey paper: Pseudo random number generators and security tests. Journal of Theoretical & Applied Information Technology, 96(7), 2018.

[48] USC. The usc-sipi image database, 1977.

[49] Serge Vaudenay. Security flaws induced by cbc padding—applications to ssl, ipsec, wtls... In International Conference on the Theory and Applications of Cryptographic Techniques, pages 534–545. Springer, 2002.

[50] JS Armand Eyebe Fouda, J Yves Effa, Samrat L Sabat, and Maaruf Ali. A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation, 19(3):578–588, 2014.

[51] Wassim Hamidouche, Mousa Farajallah, Naty Sidaty, Safwan El Assad, and Olivier Déforges. Real-time selective video encryption based on

the chaos system in scalable hevc extension. Signal Processing: Image Communication, 58:73–86, 2017.

[52] Roland Norcen and Andreas Uhl. Selective encryption of the jpeg2000 bitstream. In IFIP International Conference on Communications and Multimedia Security, pages 194–204. Springer, 2003.

[53] Ayoub Massoudi, Frédéric Lefebvre, Christophe De Vleeschouwer, and François-Olivier Devaux. Secure and low cost selective encryption for jpeg2000. In 2008 Tenth IEEE International Symposium on Multimedia, pages 31–38. IEEE, 2008.