Research Article Journal of Data Analytics and Engineering Decision Making

Classification of JPEG2000 Image Encryption Algorithms

Sahar Natsheh and Mousa Farajallah*

Deanship of Graduate Studies and Scientific Research Master of informatics Palestine Polytechnic University, Hebron, 198, Palestine

***Corresponding Author**
Mousa Farajallah, Deanship of Graduate Studies and Scientific Research Master of informatics Palestine Polytechnic University, Hebron, 198, Palestine.

Submitted: 2024, May 08; **Accepted:** 2024, May 30; **Published:** 2024, Jun 19

Citation: Natsheh, S., Farajallah, M. (2024). Classification of JPEG2000 Image Encryption Algorithms. *J Data Analytic Eng Decision Making, 1*(1), 01-09.

Abstract
Image encryption is different from text encryption; as a result of the bulk data capacity, high redundancy of image data, and the high correlation between the image pixels. Thus, traditional methods are difficult to be used for image encryption as their pseudo-random sequences have a small period without real modification, which causes a restriction in the security and encryption of the image. Different types of JPEG2000 encryption techniques are addressed and discussed in secured and compressed (friendly) based aspects. Moreover, a study of JPEG2000 codec in terms of encryption is achieved in order to be a good tutorial for researchers who have experience in image or video without crypto and selective encryption expertise. Finally, it is also suitable for beginners in the field of image and video security with good expertise in the encryption field. The importance and sensitive JPEG2000 codec structure is described in a manner that can help researchers to identify steps, requirements, and techniques that should be used to secure image and video content.

Keywords: JPEG2000, Selective Encryption, Real-time Application, Security Evaluation, Joint Encryption

1. Introduction

Recently, JPEG2000 has been employed in many applications like digital cinema applications, archival of visual content, geospatial imaging, medical imaging, and video surveillance [1]. 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), 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 [2,3]. This feature is useful for the 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 of 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 [4]. But such an approach was inadmissible for several requirements such as [5]:

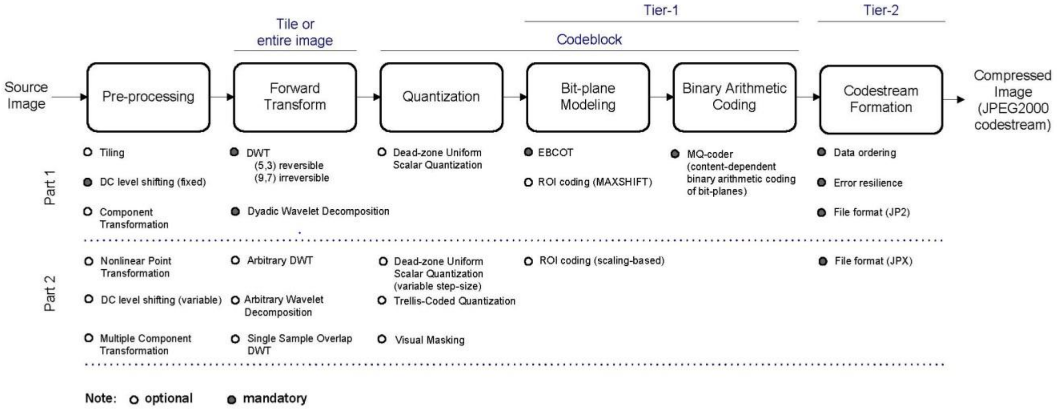
- Maintaining the format compliance and the associated functionalities of JPEG2000 like scalability; the packet headers must not be altered or encrypted to achieve format compliance.
- Achieving higher robustness against channel and storage errors. For example, the marker codes play a role in error resilience for JPEG2000 images, and encrypting those marker codes will omit this feature [6].
- Reducing the computational effort.

Nowadays, researchers are on the hunt for more feasible encryption models; or what is been called lightweight encryption models. They are trying to develop a secure encryption model by encrypting some parts of the original image instead of applying 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 the insertion of satisfactory noise to make the content incomprehensible [7]. Several methods were proposed to achieve the previously mentioned requirements; to maintain 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 the 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 related works section.

JPEG2000 standard was released in December 2000; the abbreviation JPEG is a short term for the 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, and each part presents a new release and modification of the standard [5]. 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 of the standard.

In general, the JPEG2000 standard is much more complex than the JPEG standard and some analyses show that the JPEG2000 compression is 30 times more complex than the JPEG [8]. That is due to the DWT and the entropy encoding processes in JPEG2000. On 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); this feature is useful for transmitting images in low-bandwidth transmission channels [5]. It is also capable of compressing and decompressing the grayscale, colored, and bi-level images [5]. In addition, it allows a maximum size of a compressed image to be equal to (232 − 1)x(232 − 1). And it provides lossy and lossless compression using single unified compression architecture for 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 ensure some security level in the image. Figure 1 shows the architecture of JPEG2000 image compression part 1 standard.



JPEG2000 image compression architecture [1].

The first phase is the prepossessing 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 nonoverlapping blocks in the case of large images in the tiling step. After that; for mathematical computation needs; the samples are converted into two's complement representations in order to have an input image sample with a dynamic range that is cantered 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: Discrete Wavelet Transform (DWT), then Quantization, and Entropy encoding [2]. Firstly; in DWT; each component is decomposed into a number of sub-bands 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 sub bands are divided into a number of code blocks; those code blocks have a smaller size than the sub-band and they have an equal size to each other; with usually 32x32 or 64x64 size for better memory handling.

In DWT step each component is wavelet transformed into NL decomposition levels called resolutions. The resolutions by an index r; range 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 [9]. Figure 1 shows the architecture of DWT decompositions and figure 2 shows an example of two levels of decompositions applied to Lena's image.

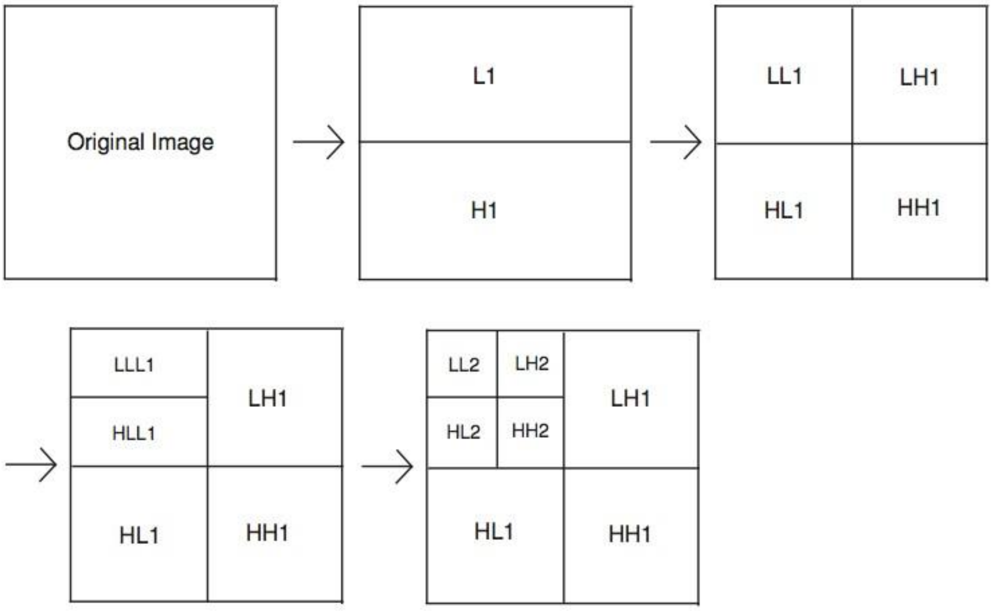


Figure 1: Architecture of DWT Decompositions

Finally; in the entropy encoding step; the quantized wavelet coefficients of each code block in each sub-band 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 bit-plane; a bit-plane is a binary representation of a specific value in the code-block. 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 bit-stream formation or what is called the tier-2 coding, a representation of the layer and block summary information for each code block is formed in this phase. The block summary consists of the most significant magnitude bit-planes where any sample in the code block is non-zero, the length of the compressed code words in the code block, the truncation point between the bit-stream layers, and other information. This information is received at the decoders' side in a form of two tag trees; one for bit-stream layers and the other for zero bit-planes information.

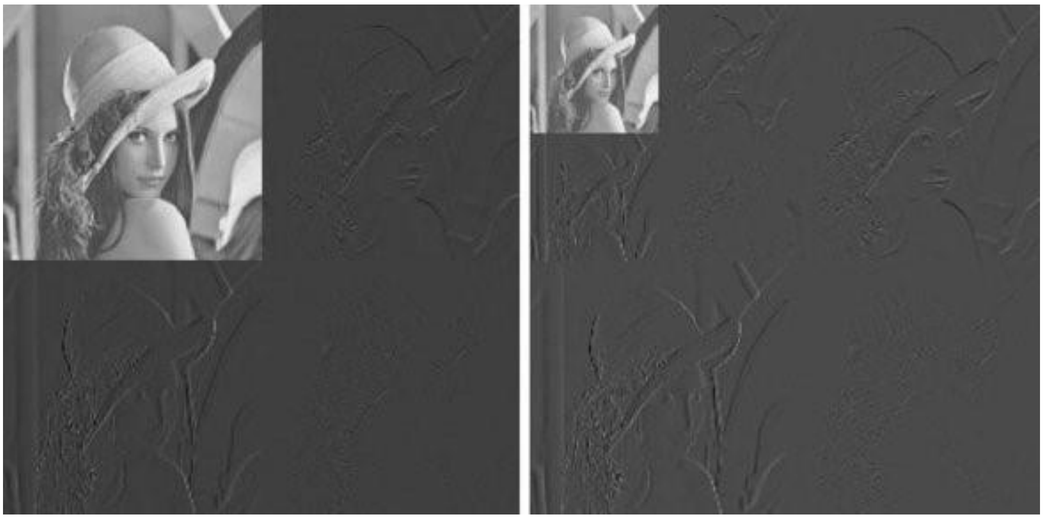


Figure 2: 2 Level Decomposition on Lena Image

The JPEG2000 code stream consists of headers; main header, tiles headers, and tile part header; and packets that each of which contains a packet header and packet body [10]. The main header and tile part header contains information about the compression parameters, such as image size, tile size, code-block size, and the number of components. The packet header contains inclusion information for each code block, the lengths of Code-block Contributions to the Packet (CCPs), the number of contributed coding passes for each code block, and the number of leading zero bit-planes for each code block (LZB). Figure 3 shows the format of a JPEG2000 message. Moreover, the JPEG2000 code stream has some preserved values called marker codes; each of which is a specific delimiter of the code-stream content. The preserved code words cause a crash to the decoder; if they were generated within the code stream; are the code-words which mark the end of a code stream or packet; those marker codes exceed the value of 0xff8f. Table 1 presents some marker codes for JPEG2000 part 1 standard [5].

2. JPEG2000 Encryption Algorithms: Related Works

The main idea of 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 has special properties such as bulk capacity, high redundancy, and correlation between the pixels that require special necessities in any encryption technique [11]. The encryption techniques of JPEG2000 fall into two categories; bit-stream oriented and compression integrated.

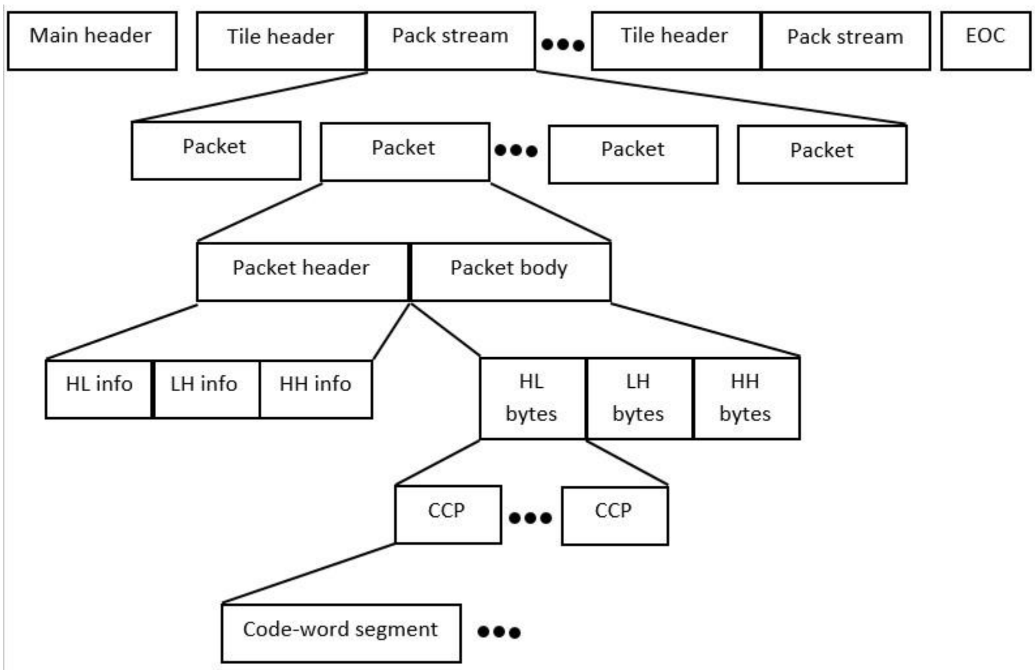
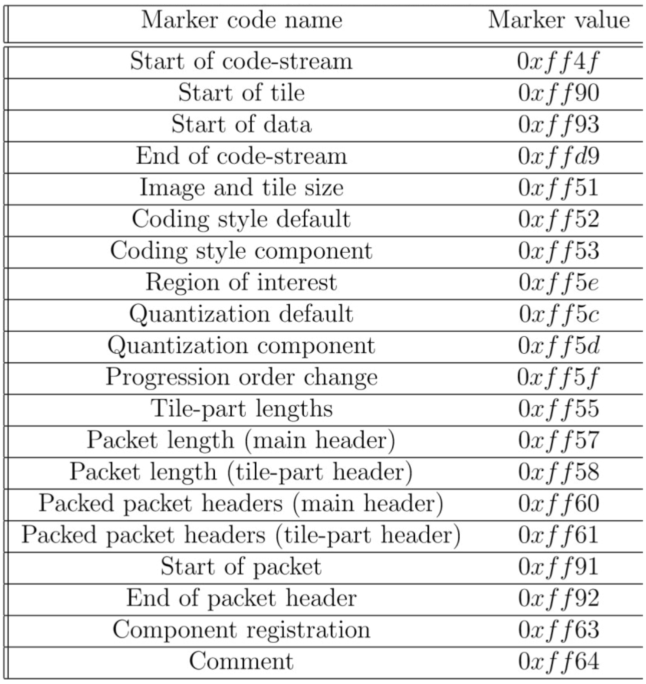


Figure 3: JPEG2000 Codestream Format [10]

In the following, various approaches to JPEG2000 encryption that fall under the two categories are presented. For further information about JPEG2000 encryption techniques, you can refer to [10].

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 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



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	$0xff64$

Table 1: JPEG2000 Part 1 Maker Codes

(isotropic or anisotropic wavelet decomposition), this kind of encryption was insecure, adds a high level of complexity to the compression process, and needs some special decoders for the image [12,13]. Nowadays, 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 is still a distortion occurs 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 negligible overhead to the compression process, differs in the security level, and the image cannot be decoded without the encryption key. But there is also some loss of data during this phase in the compression process.

The compression-integrated techniques are better than the bit-streamoriented techniques from the computational demand point of view; they are considered to be faster than the format-compliant techniques because they intersect with the compression process. On 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 modify the JPEG2000 compression standard, which results on encrypted image not being decompressed with a standard decompressor, which is important for business applications.

2.1.1. Discrete Wavelet Transform Encryption

A New Algorithm of the Combination of Image Compression and Encryption Technology Based on Cross Chaotic Map. Tong et. al. algorithm consists of a confusion-diffusion structure; the confusion process is proposed by the cross chaotic map and cipher-text feedback, and the diffusion process is applied using a key and modulus operation [14]. Those processes are combined with image compression and applied to 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 model 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 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, and the average NPCR and UACI values are 0.996 and 0.333 respectively; which means that the algorithm is resistant to differential attacks.

An Encryption Then Compression System for JPEG2000 Standard. Watanabe et. al.'s procedure encrypts the image after DWT is applied [15]. The DWT coefficients are encrypted with two types of encryption schemes based on a 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 blocked shuffling of DWT coefficients. The proposed technique combines the two encryption schemes by applying sign-scrambling followed by 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.

2.1.2. Entropy Encoding Encryption

JPEG2000 Compatible Layered Block Cipher Stream. Memon built a method for joint compression [16]. Assuming we have a plain image p(x,y) with the size of $N \times N$ 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 5th 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 [17]. The proposed technique uses two types of neural networks, one is chaotic and the other is a 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 attacks. And all of the wavelet sub-bands are encrypted and no data is left in plain. In addition, 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.

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 that performs both lossless compression and encryption of data. The lossless compression is based on 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 [18].

Compression Performance: In this paper, they mentioned that the scheme conserves compression efficiency. But the studies on the JPEG2000 standard says that there is some loss in the data even in the lossless compression in entropy encoding; which was assured during our studying and application for the standard [17]. 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 attacks. And it is immune to statistical attacks.

2.1.3. MQ Coder Encryption

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 quantized probabilities, each state corresponds to a different probability map which can be represented by the probability of the Least Probable Symbol (LPS) and Most probable Symbol (MPS) [5]. 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, the key of 94-bit length is generated for each code block [19]. The key is conjunct with each destination state as k_i^M and k_i^L, each of which presents one key bit for state i and is 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 a 256-bit key to generate the sub-keys which makes it immune to brute-force attacks. 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 the mean value of SSIM is 0.026.

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 [20]. 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 and 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 known plain-text attacks. They used the initialization vector in order to make the result of encrypting the same image using the same key different at any time. The mean structural similarity measure (MSSIM) values for the encrypted images are lower than 0.1.

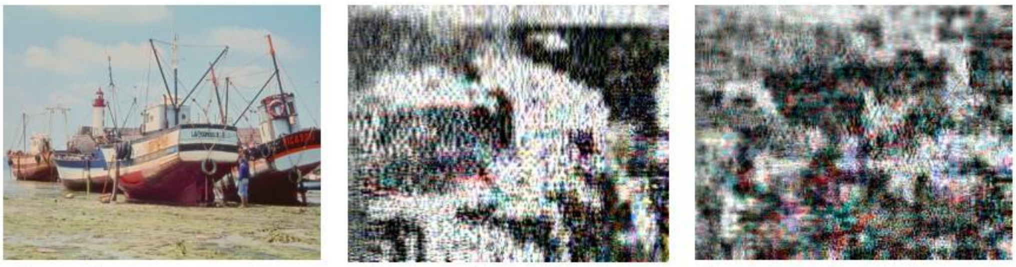
Efficient Selective Encryption for JPEG2000 Image Using Private Initial Table. Liu et. al. technique is a symmetric scheme that uses a secret key and a mapping function to generate a private initial table to encrypt the selected DWT code blocks in the entropy coding stage of the JPEG2000 coding scheme. 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 code blocks will not be correctly decrypted [18].

Compression performance: When using the JPEG2000 codec system in lossless mode, the compressibility is 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.

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 technique doesn't affect the compression ratio; because it doesn't interfere with the compression process. Those methods need to maintain 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 Code stream (EOC) marker code; figure 3.1 shows an example of the effects of EOC marker code generation within the code stream; 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 4: 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 computational complexity. As we mentioned before, the bit-stream oriented techniques encrypt only the packet bodies of the image and leave 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 levels. 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 trees and code-block contributions to packets.

2.2.1. Fully Encryption Techniques

Chaotic-Cipher-Based Packet Body Encryption Algorithm for JPEG2000 Images. Gu et. al. used a symmetrical JPEG2000 image encryption method based on iterating chaotic maps and some primitive operations [21]. In order to maintain the structure of the 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 to them block by block with cipher feedback. They applied the format compliance by making 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 attacks since the size of the key is 256-bit, it is also immune to key sensitivity attacks. On the other hand, the dynamical degradation of the PWLCM destroys the uniform distribution of the key stream generated from the chaotic iterations of it and introduces many weak keys that cause large information leaking[22]. 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 about the plain image.

A Format-Compliant Encryption Scheme for JPEG2000 Codestream. The algorithm by Wen et. al. encrypted the code-block contribution to the packet (CCP) [23]. 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 ciphertext C=$c_1||c_2||...||c_n$, and ci is 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 si is a byte of the key S. If an encryption process produces any marker code 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.

An Encryption Algorithm of JPEG2000 Streams for Supporting Ciphertextbased Transcoding. Fu et. al. proposed a ciphertext-based transcoding hierarchical encryption algorithm (CT-HEA) for JPEG2000 streams [24]. 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 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 to brute force attack.

Format-Compliant Encryption of Regular Languages: Block-Based Cycle Walking. Stu¨tz et. al. technique relies on block-based cycle-walking (BBCW) [25]. 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 regular cycle walking. On 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.

2.2.2. Selective Encryption Techniques

Generalized Hierarchical Encryption of JPEG2000 Code streams for Access Control. Imaizumi et. al. proposed a method that generates keys from a single master key dependently [26]. 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, Klayer,x and Kresolution,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 images.

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 resilient to collusion attacks and brute force attacks; since it used a 60-byte master key.
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[27]. 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.

3. Conclusion

In this research, a comparative study regarding selective encryption of JPEG2000 techniques is proposed. The codec and sensitive parts, a speciality of JPEG2000 are presented in order to be considered by researchers in image encryption and in general in video-based JPEG2000 structure.

References

1. Skodras, A. N., & Ebrahimi, T. (2006, May). JPEG2000 image coding system theory and applications. In *2006 IEEE International Symposium on Circuits and Systems* (pp. 4-pp). IEEE.
2. Skodras, A., Christopoulos, C., & Ebrahimi, T. (2001). The JPEG 2000 still image compression standard. *IEEE Signal processing magazine, 18*(5), 36-58.
3. Vikram, K. N., Vasudevan, V., & Srinivasan, S. (2005). Rate-distortion estimation for fast JPEG2000 compression at low bit-rates. *Electronics Letters, 41*(1), 16-18.
4. Joan, D., & Vincent, R. (2002). The design of Rijndael: AES-the advanced encryption standard. *Information Security and Cryptography, 196*.
5. Acharya, T., & Tsai, P. S. (2004). *JPEG2000 standard for image compression: concepts, algorithms and VLSI architectures.* John Wiley & Sons.
6. Moccagatta, I., Soudagar, S., Liang, J., & Chen, H. (2000). Error-resilient coding in JPEG-2000 and MPEG-4. IEEE *Journal on Selected Areas in Communications, 18*(6), 899-914.
7. Yekkala, A. K., Udupa, N., Bussa, N., & Madhavan, C. V. (2007, January). Lightweight encryption for images. In *2007 Digest of Technical Papers International Conference on Consumer Electronics* (pp. 1-2). IEEE.
8. Santa-Cruz, D., & Ebrahimi, T. (2000, September). An analytical study of JPEG 2000 functionalities. In *Proceedings 2000 International Conference on Image Processing* (Cat. No. 00CH37101) (Vol. 2, pp. 49-52). IEEE.
9. Lui, C. (2001). A study of the JPEG-2000 image compression standard. Queen's University, Kingston.
10. Engel, D., Stütz, T., & Uhl, A. (2009). A survey on JPEG2000 encryption. *Multimedia systems, 15*(4), 243-270.
11. E. B. Corrochano, Handbook of Geometric Computing, Springer, 2005.
12. Engel, D., & Uhl, A. (2006, May). Secret wavelet packet decompositions for JPEG 2000 lightweight encryption. In *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings* (Vol. 5, pp. V-V). IEEE.
13. Engel, D., & Uhl, A. (2006, July). Lightweight JPEG2000 encryption with anisotropic wavelet packets. In *2006 IEEE International Conference on Multimedia and Expo* (pp. 2177-2180). IEEE.
14. Tong, X. J., Wang, Z., Zhang, M., & Liu, Y. (2013). A new algorithm of the combination of image compression and encryption technology based on cross chaotic map. *Nonlinear Dynamics, 72*, 229-241.
15. Watanabe, O., Uchida, A., Fukuhara, T., & Kiya, H. (2015, April). An Encryption-then-Compression system for JPEG 2000 standard. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1226-1230). IEEE.
16. Memon, Q. A. (2017). Jpeg2000 compatible layered block cipher. *Multimedia Forensics and Security: Foundations, Innovations, and Applications,* 253-275.
17. Li, J. (2003). Image compression: The mathematics of JPEG 2000. *Modern Signal Processing, 46*, 185-221.
18. Masmoudi, A., Puech, W., & Bouhlel, M. S. (2010). 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.

19. El-Arsh, H. Y., & Mohasseb, Y. Z. (2013, November). A new light-weight jpeg2000 encryption technique based on arithmetic coding. In *MILCOM 2013-2013 IEEE Military Communications Conference* (pp. 1844-1849). IEEE.
20. Xiang, T., Yu, C., & Chen, F. (2014). Secure MQ coder: An efficient way to protect JPEG 2000 images in wireless multimedia sensor networks. *Signal Processing: Image Communication, 29*(9), 1015-1027.
21. Gu, G., Ling, J., Xie, G., & Li, Z. (2016). A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images. *Signal Processing: Image Communication, 40,* 52-64.
22. Li, S., Mou, X., Cai, Y., Ji, Z., & Zhang, J. (2003). On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Computer physics communications, 153*(1), 52-58.
23. Wen, J., Wang, J., Zhang, B., Li, Z., & Huang, Z. (2010, December). A format-compliant encryption scheme for JPEG2000 codestream. In *2010 IEEE International Conference on Information Theory and Information Security* (pp. 1038-1041). IEEE.
24. Fu, Y., Yi, X., & Ma, H. (2014, September). An encryption algorithm of jpeg2000 streams for supporting ciphertext-based transcoding. In *2014 International Conference on Multisensor Fusion and Information Integration for Intelligent Systems (MFI)* (pp. 1-7). IEEE.
25. Stütz, T., & Uhl, A. (2010, May). Efficient format-compliant encryption of regular languages: Block-based cycle-walking. In *IFIP International Conference on Communications and Multimedia Security* (pp. 81-92). Berlin, Heidelberg: Springer Berlin Heidelberg.
26. Imaizumi, S., Watanabe, O., Fujiyoshi, M., & Kiya, H. (2005, September). Generalized hierarchical encryption of JPEG 2000 codestreams for access control. In *IEEE International Conference on Image Processing 2005* (Vol. 2, pp. II-1094). IEEE.
27. Ikeda, H., & Iwamura, K. (2011, March). Selective encryption scheme and mode to avoid generating marker codes in JPEG2000 code streams with block cipher. In *2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications* (pp. 593-600). IEEE.