DATA EMBEDDING AN IMAGE USING DCT: A REVIEW

[1] Sonali Bhujade
[1]M.Tech Student
[1]Department of Electronics & Communication,
[1]Anjuman College of Engineering and Technology, Nagpur, India

Abstract: ***In line with a growing need for data and information transmission in a safe and fast manner, researches on image protection and security through a combination of cryptographic and compression techniques have begin to take form. The combination of these two methods may include categories based on their process sequences. Data embedding an image with maximum security that uses conventional aspects with a twist of translation during compression is a prerequisite before cipher encryption is the area of interest. In this review we process various techniques that combine image compression and encryption to have an embedded image along with data that's secure and can be manipulated with a secure key. Transform coefficients that are utilized along with side information with a way to reduce network traffic and increase security is the base of the review. The performance of the algorithm of encryption along with image compression needs to be read, compared and enhanced so that it can be verified using various standard tests; so that it will not remain hostile to security breach.***

Index Terms - Compression, image processing, encryption, translation.

I. INTRODUCTION

The development of informational technology has a broad impact on human ways of communication from initial conventional means to digital ones. Communication through messaging service has also evolved from SMS (Short Message Service) to MMS (Multimedia Messaging Service). Messaging transmission service through internet media such as e-mail, and social media such as Twitter, WhatsApp, Facebook, BBM, etc., can also be done. One emerging problem is that a growing size of digital data, particularly still images, is inevitable due to the need for high-quality images. As a result, a need for larger storage spaces follows. Although storage techniques in digital computers have experienced rapid development, in many situations they require the reduction of digital data storage. One such reduction manifests in the form of bandwidth limitation in communication systems to provide a faster data transmission through communication lines and a smaller percentage of download and upload failure [1].

In addition to the speed of data exchange of a growing size, data safety is of utmost concern due to the susceptibility of data sent through communication lines to their being stolen or extracted by eavesdroppers. In theory, compression and cryptography are two opposing techniques. Encryption ensures that transmitted data is reliable and integral by converting it from legible into illegible data through an encoding process. Conversely, a compression method seeks to reduce the size of transferred or stored data by finding out and removing duplicate parts of evidence or patterns of data [2].

However, data compression and cryptographic system are so deeply connected and mutually useful that they are capable of being employed together. The aims are to generate a smaller size of data; to ensure a quality of data during reconstruction; to speed up data transmission; to reduce bandwidth requirement, and to ensure its safety [3].

II. METHODS

In line with a growing need for data and information transmission in a safe and fast manner, researches on image protection through a combination of cryptographic and compression techniques have begun to take form. Combination of these two methods may be classified into three categories based on their procession sequences:

1. a cryptographic technique followed by a compression technique [encryption-compression],
2. a compression technique followed by a cryptographic method [compression-encryption], and
3. both techniques employed in a single process [hybrid compression encryption].

The JPEG compression standard has been in use for almost a decade now. It has proved a valuable tool during all these years, but it cannot fulfill the advanced requirements of today. Today's digital imagery is extremely demanding, not only from the quality point of view, but also from the image size aspect. Current image size covers orders of magnitude, ranging from web logos of size of less than 100 Kbits to high quality scanned images of approximate size of 40 Gbits. The JPEG 2000 international standard represents advances in image compression technology where the image coding system is optimized not only for efficiency, but also for scalability and interoperability in network and mobile environments. Digital imaging has become an integral part of the Internet, and JPEG 2000 is a powerful new tool that provides power capabilities for designers and users of networked image applications. The JPEG 2000 standard provides a set of features that are of importance to many high-end and emerging applications by taking advantage of new technologies. It addresses areas where current standards fail to produce the best quality or performance and provides capabilities to markets that currently do not use compression. The markets and applications better served by the JPEG 2000 standard are Internet, color facsimile, printing, scanning (consumer and prepress), digital photography, remote sensing, mobile, medical imagery, digital libraries/archives, and E-commerce. Each application area imposes some requirements that the standard, up to a certain degree, should fulfill. Some of the most important features that this standard should possess are the following [20]:

- Superior low bit-rate performance: This standard should offer performance superior to the current standards at low bit rates (e.g., below 0.25 b/p for highly detailed gray-scale images). This significantly improved low bit-rate performance should be achieved without

sacrificing performance on the rest of the rate-distortion spectrum. Network image transmission and remote sensing are some of the applications that need this feature.

- Continuous-tone and bilevel compression: It is desired to have a coding standard that is capable of compressing both continuous-tone and bilevel images. If feasible, this standard should strive to achieve this with similar system resources. The system should compress and decompress images with various dynamic ranges (e.g., 1 to 16 bits) for each colour component. Examples of applications that can use this feature include compound documents with images and text, medical images with annotation over lays, and graphic and computer generated images with binary and near to binary regions, alpha and transparency planes, and facsimile.
- Lossless and lossy compression: It is desired to provide lossless compression naturally in the course of progressive decoding. Examples of applications that can use this feature include medical images, where loss is not always tolerated; image archival applications, where the highest quality is vital for preservation but not necessary for display; network applications that supply devices with different capabilities and resources; and prepress imagery. It is also desired that the standard should have the property of creating embedded bit stream and allow progressive lossy to lossless buildup.
- Progressive transmission by pixel accuracy and resolution: Progressive transmission that allows images to be reconstructed with increasing pixel accuracy or spatial resolution is essential for many applications such as web browsing, image archival and printing.
- Region-of-interest (ROI) coding: Often there are parts of an image that are of greater importance than others. This feature allows users to define certain ROIs in the image to be coded and transmitted in a better quality and less distortion than the rest of the image.
- Open architecture: It is desirable to allow open architecture to optimize the system for different image types and applications. With this feature, a decoder is only required to implement the core tool set and the parser that understands the code stream.
- Robustness to bit errors: It is desirable to consider robustness to bit errors while designing the code stream. One application, where this is important, is transmission over wireless communication channels. Portions of the code stream may be more important than others in determining decoded image quality. Proper design of the code stream can aid subsequent error correction systems in all evading a strophic decoding failure.
- Protective image security: Protection of a digital image can be achieved by means of different approaches such as watermarking, labelling, stamping, or encryption.JPEG 2000 image files should have provisions for such possibilities.

III. LITERATURE REVIEW

3.1 Technique

- Encryption-compression technique

Symmetric Cryptography Method with Lossless Compression - Johnson et al.[4] and Liu et al.[5] used the combination of a symmetric cryptographic technique using stream cipher method followed by a lossless compression technique using Slepian-Wolf coding. Johnson et al.[4] used a Pseudo-Random Key Generator (PRG), whereas Liu et al.[5] proposed an efficient way of compressing encrypted images through resolution progressive compression (RPC) to avoid exploiting Markov properties in Slepian-Wolf decoding to reduce the complexities of a decoder significantly. In this method, incompatible pixels for encoder are re-correlated to make them closer to a decoder to generate access to low-resolution images. The testing result of entropy value shows that this method has a much better coding efficiency and less computational complexity. Mariselvi and Kumar[6] has also proposed the compression of encrypted images through RPC. The symmetric cryptographic employed is DES algorithm followed by lossless compression technique using Huffman coding or arithmetic coding. The colored images of encryption using DES algorithm are subsequently down sampled to generate sub -images. Each sub-image is then encoded using Huffman or arithmetic coder for performance comparison. Testing of the proposed method is done at four gray scale images to measure Peak Signal Noise Ratio(PSNR) and Compression Ratio (CR) when using arithmetic coding and Huffman coding. The testing result of PSNR values and their compression ratios indicates that Huffman Coding generates higher scores than those of arithmetic coder. Sharma et al.[7] conducted researches by combining symmetric cryptographic technique using 2D methods Fractional Multiple Parameter Discrete Fourier Transform (MPDFRFT) followed by lossless compression method using zigzag, Run Length methods, and Huffman encoding. The proposed scheme provides two freeways of data encryption and compression. The test is applied to 3 gray scale images and five colored images and shows a significant increase in their PSNR values. The highest PSNR values of Lena, a cameraman, a baboon, and a satellite image are 76.4, 74.1, 80 and 79.8 dB respectively, with their CR scores are 20%. The lowest PSNR values of each image are 39.8, 34.8, 36.1 and 23.2 dB and their CR is 70%. The proposed scheme also shows a high resistance to brute-force attack seen from the analysis of visual image that looks random cipher. It also provides astounding features in terms of time needed to execute the algorithm and of high sensitivity to the original key.

- Compression –encryption technique

According to Sandoval and Uribe [2],the application of data compression before its encryption will reduce duplicate parts of data that are prone to cryptanalytic exploitation. Also, data compression can speed up an encryption process, and a decryption process will produce corresponding plaintexts. Sharma and Gandhi [15] also supported the idea. They claim that in as many as 70% of the cases studied, implementing cryptography and then compression is more efficient, because: first, compression techniques can eliminate data redundancy, and will work well if the data is random. Therefore, this method can be carried out first before the encryption process. Second: compression can reduce the effectiveness of some attacks. Compression works to reduce data redundancy, whereas cryptanalysis uses a concept of frequency analysis that relies on repeated/duplicate data findings. As a result, if compression is applied beforehand, it may reduce the effectiveness of cryptanalytic attacks that exploit frequency analysis. Third: brute force attacks will take longer time. Brute force attacks are launched in various ways: decrypting data and checking out if consistent output data exists. If a cracker was seeing a compressed data, then a cracker will have first to decrypt and then decompress it to see whether consistent output data exists. It takes a long time, and if the cracker has no idea or does not suspect the probability of data compression beforehand, cryptanalysis will probably not solve it. Fourth: an intruder lacks cipher-text data to do the analysis. An intruder needs enough data to analyze a cipher-text. The fewer clues about internal conditions of a cipher and its key, the better the method. If the compression technique followed by encryption is done, the resulted plain texts will have fewer data redundancies and are thus capable of blocking cryptanalytic attacks [15].

- Hybrid compression-encryption technique

This technique combined a compression method and cryptography, or vice versa. However, that combination is not worked out in a sequential order. Al-Maadeed et al.[16] proposed a joint method of a selective encryption of an image and a compression. The basic idea of this proposed algorithm is to demonstrate the effect of the application of several keys to enhance security by increasing the number of external keys in each encryption process. The encryption process uses an encryption algorithm based on chaos conducted on the approximation of the results of the DWT transformation. In contrast, DWT transformation results in a detailed component of the compression process. The encryption process of the proposed method uses a key length of 94 bits. It also conducted a comparison of a key length of 97 bits. The fundamental principle of encryption is to use random numbers dependent on original condition to generate this randomized number sequence. This technique creates a significant reduction in encryption and decryption time. The testing result shows a reduction of encryption time into about 0.218 seconds with one key, 0.453 second with two keys, and 0.5 seconds with three keys. Correlation coefficient value between an original image and an encrypted image decreases when the number of external encryption keys increase. And this Resulted in an increase in security (the more the key, the security of the data to be encrypted is also increasing). Al-Maadeed et al.[16] also show how correlation coefficient changes exponentially when it uses a value different from the controlling parameter. Also, they recommend the use of more than 128 bits external keys to enhance the overall security and also suggest other methods for compression.

3.2 Choice of Encryption and compression

Mostly the combination of the Encryption-Compression technique discussed above uses symmetric cryptographic and lossless compression method. In fact, it shows that the process focuses more on image security than on data size reduction. The application of lossless compression technique is to ensure that all data is reversible and can be reverted to the original while maintaining the high quality of reconstructed images and compression ratio. As such, this concept is most applicable when data accuracy is of paramount importance, such as textual information, biomedical image, and legal data. The majority of the measurements of the qualityof the decompression image against the original image, the compression ratio as well as the processing time are used to measure the success of the proposed method, while the measurement results cipher visual image is used to analyze the level of security of some of the proposed method.

The combination of Compression-Encryption technique has some advantages because compression method can be lossy, lossless, or combination of both. In contrast, most cryptographic techniques use symmetric cryptography by developing a chaotic method to generate a symmetric key. As such, this approach applies to data image, either audio or video. Conversely, the proposal to use various chaotic methods aimed at generating a symmetric key to enhance its security.

The hybrid compression-encryption technique is capable of providing real data security assurance with such a low computational complexity that it is eligible for increasing the efficiency and security of data/information transmission. So the concept qualifies for and could improve transmission efficiency and data security by improving the performance of each compression and cryptographic technique through hybrid concept. This concept is expected to be able to combine excellent properties of lossy and lossless compression techniques and to offset the downside of symmetric and asymmetric cryptographic techniques, particularly about cipher key management, to obtain the much smaller size of data, maintaining good quality of data during reconstruction and security assurance.

i. The primary project objective is to utilize one of the best fit techniques as base of our work to provide a algorithm of encryption plus compression.
ii. Provide a fast algorithm that can compress the prerequisite image as soon as possible.
iii. Utilize a translation technique that uses one of the transform that provides ease of computation.
iv. Modification of the base algorithm to provide maximum security/cipher encryption that is least prone to attacks plus keeping the PSNR as low as possible.

3.3 Lossless versus Lossy Compression

Lossless compression has many applications and used generally for technical drawings, clip art, comics, archival purposes and often medical imaging. Lossy compression methods introduce compression artifacts, when it is used at low bit rates. When an image is formed by lossy compression technique than reconstructed image quality degraded as compared to original image. Lossy schemes can achieve higher compression ratio as compared to lossless scheme. An example of usage of lossy scheme includes natural images such as photos in applications where minor (sometimes imperceptible) loss of information can be considered to get a substantial reduction in bit rate [15]. With pace of time there has been improvement in technology and there are two type of compression lossy and lossless. Predictive coding is a spatial domain technique. In predictive coding, information already sent or available is used to predict future values, and the difference is coded. Since this is done in the image or spatial domain, it is relatively simple to implement and is readily adapted to local image characteristics.

Differential Pulse Code Modulation (DPCM) is one particular example of predictive coding. Transform coding, on the other hand, first transforms the image from its spatial domain representation to a different type of representation using some well-known transform and then codes the transformed values (coefficients). This method provides greater data compression compared to predictive methods, although at the expense of greater computational requirements [17]. One shall work over two method of image compression. However both are based on DCT but the encoding technique has been changed.

3.4 Performance Comparison

To judge the efficiency of the JPEG 2000 as compared to other standards, extensive comparisons have been reported with regard to lossy performance, lossless performance, resilience to errors, and other characteristics. The algorithms have been evaluated on several images, mainly from the JPEG 2000 test set, which cover a wide range of imagery types.

Table Functionality Evaluation Results				
	JPEG 2000	**JPEG-LS**	**JPEG**	**MPEG-4VTC**
Lossless Compression performance	●●●	●●●●	●	
Lossy compression performance	●●●●●	●	●●●	●●●●
Progressive bit streams	●●●●		●	●●
Region of Interest(IOC) coding	●●●			●
Arbitrary shaped objects				●●
Random access	●●			
Low complexity	●●	●●●●●	●●●●●	●
Error resilience	●●●	●	●	●●●
Non iterative rate control	●●●			●
Genericity	●●●	●●●	●●	●●
A bullet indicates that the corresponding functionality is supported. The number of bullets symbols characterizes the degree of support.				

Table 1: Functionality Evaluation Results [20].

IV. METHODOLOGY

The Modified JPEG compression engine (encoder and decoder)is illustrated in methodology diagram fig form below. At the encoder, the discrete transform is first applied on the source image data. The transform coefficients are then quantized and entropy coded before forming the output code stream (bit stream). The decoder is the reverse of the encoder. The code stream is first entropy decoded, de-quantized, and inverse discrete transformed, thus resulting in the reconstructed image data.

Although this general block diagram looks like the one for the conventional JPEG, there will be radical differences in all of the processes of each block of the diagram implemented and compared. A quick overview of the whole probable system is as follows as shown in below figure:

- All the source images will be decomposed into compression like rectangular tiles as base components.
- A DCT/wavelet transform will be applied on each tile. The tile will be decomposed into different resolution levels.
- These decomposition levels are made up of sub bands of coefficients that describe the frequency characteristics of local areas of the tile components, rather than across the entire image component.
- These sub bands of coefficients will be quantized and collected into rectangular arrays of "code blocks."
- The bit planes of the coefficients in a code block (i.e. the bits of equal significance across the coefficients in a code block) are for example entropy coded.
- The encoding can be done in such a way that certain regions of interest can be coded at a higher quality than the background.
- Markers may be are added to the bit stream to allow for error resilience.
- The code stream shall have a main header at the beginning that describes the original image and the various decomposition and coding styles that are used to locate, extract, decode and reconstruct the image with the desired resolution, fidelity, region of interest or other characteristics.

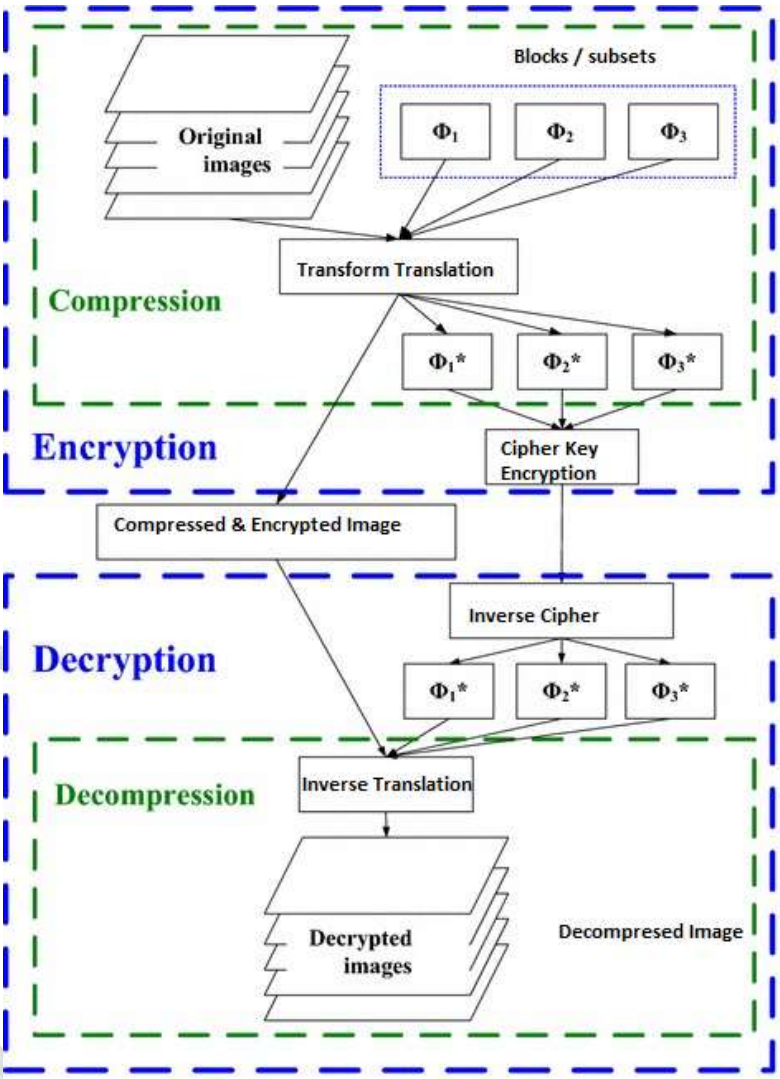

Figure 1: Modified JPEG Compression Engine

V. CONCLUSION AND FUTURE SCOPE

JPEG 2000 is the new standard for still image compression. It provides a new framework and an integrated toolbox to better address increasing needs for compression. It also provides a wide range of compression standards. Work is still needed for optimizing its implementation performance. A good insight of morphology needs to be carried out to justify the role of DCT translation vs DWT translation.

REFERENCES

[1] M.Merdiyan and W. Indarto, "ImplementasiAlgoritma Run Length, Half Byte, dan Huffman untukKompresi File," in Seminar NasionalAplikasiTeknologiInformasi 2005 (SNATI 2005), 2005, pp. 79–84.

[2] M.M. Sandoval and C. F. Uribe, "A Hardware Architecture for Elliptic Curve Cryptography and Lossless Data Compression," in 15th International Conference on Electronics, Communications and Computers (CONIELECOMP'05), 2005, no. March, pp. 113–118.

[3] A. Loussert, A. Alfalou, R. El Sawda, and A. Alkholidi, "Enhanced System for Image's Compression and Encryption by Addition of Biometric Characteristics," International Journal of Software Engineering and Its Applications., vol. 2, no. 2, pp. 111–118, 2008.

[4] M. Johnson, D. Wagner, and K. Ramchandran, "On Compressing Encrypted Data without the Encryption Key," in Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, 2004, pp. 491–504.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient Compression of Encrypted Grayscale Images," IEEE Transactions on Image Processing., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] C. MariSelvi and A. Kumar, "A Modified Encryption Algorithm for Compression of Color Image," International Journal of Recent Development in Engineering and Technology, vol. 2, no. 3, pp. 94–98, 2014.

[7] D. Sharma, R. Saxena, and N. Singh, "Hybrid Encryption-Compression Scheme Based on Multiple Parameter Discrete Fractional Fourier Transform with Eigen Vector Decomposition Algorithm," International Journal of Computer Network and Information Security., vol. 6, no. 10, pp. 1–12, Sep. 2014.

[8] K. Shafinah and M. M. Ikram, "File Security based on Pretty Good Privacy (PGP) File Security based on Pretty Good Privacy (PGP) Concept," Computer and Information Science., vol. 4, no. 4, p. 10–28, 2011.

[9] N. A. Kale and S. B. Natikar, "Secured Mobile Messaging for Android Application," International Journal of Advance Researchin Computer Science and Management Studies, vol. 2, no. 11, pp. 304–311, 2014.

[10] M.Arunkumar and S. Prabu, "Implementation of Encrypted Image Compression using Resolution Progressive Compression Scheme," International Journal of Computer Science and MobileComputing (IJCSMC), vol. 3, no. 6, pp. 585–590, 2014.

[11] A. Razzaque and N. V Thakur, "An Approach to Image Compression with Partial Encryption without sharing the Secret Key," International Journal of Computer Science and Network Security (IJCSNS), vol. 12, no. 7, pp. 1–6, 2012.

[12] X. Kang, A. Peng, X. Xu, and X. Cao, "Performing Scalable Lossy Compression on Pixel Encrypted Images," EURASIP Journal on Image and Video Processing, vol. 2013, no. 1, p. 32, 2013.
[13] H. K. Aujla and R. Sharma, "Designing an Efficient Image Encryption Then Compression System with Haar and Daubechies Wavelet," International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, no. 6, pp. 7784–7788, 2014.
[14] Y. M. Kamble and K. B. Manwade, "Secure Data Communication using Image Encryption and Compression," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 3, no. 12, pp. 8–11, 2014.
[15] M. Sharma and S. Gandhi, "Compression and Encryption : An Integrated Approach," International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 5, pp. 1–7, 2012.
[16] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A New Chaos-Based Image-Encryption and Compression Algorithm," Journal of Electrical and Computer Engineering, vol. 2012, pp. 1–11, 2012.
[17] SimYing Ong, KokSheik Wong, Xiaojun Qi, Kiyoshi Tanaka, " Beyond format-compliant encryption for JPEG image", Signal Processing: Image Communication, Volume 31, February 2015, Pages 47–60.
[18] Hang Cheng, Xinpeng Zhang, Jiang Yu, Yuan Zhang, " Encrypted JPEG image retrieval using block-wise feature comparison", Journal of Visual Communication and Image Representation, Volume 40, Part A, October 2016, Pages 111-117.
[19] Bian Yang, Chong-Qing Zhou, Christoph Busch, Xia-Mu Niu, " Transparent& Perceptually enhanced JPEG Image Encryption", IEEE DSP 2009.
[20] AthanassiosSkodras, CharilaosChristopoulos, and TouradjEbrahimi, "The JPEG 2000 Still ImageCompression Standard "..