Review of Image Compression and Encryption Techniques

Emy Setyaningsih
Doctoral Program Department of Computer Science and Electronics
Universitas Gadjah Mada, Yogyakarta, Indonesia
Department of Computer System, Institut Sains dan Teknologi AKPRIND Yogyakarta, Yogyakarta, Indonesia

Retantyo Wardoyo
Department of Computer Science and Electronics
Universitas Gadjah Mada
Yogyakarta,
Indonesia

***Abstract*—In line with a growing need for data and information transmission in a safe and quick manner, researches on image protection and security through a combination of cryptographic and compression techniques begin to take form. The combination of these two methods may include into three categories based on their process sequences. The first category, i.e. cryptographic technique followed by compression method, focuses more on image security than the reduction of a size of data. The second combination, compression technique followed by the cryptographic method, has an advantage where the compression technique can be lossy, lossless, or combination of both. The third category, i.e. compression and cryptographic technologies in a single process either partially or in the form of compressive sensing(CS) provides a good data safety assurance with such a low computational complexity that it is eligible for enhancing the efficiency and security of data/information transmission.**

Keywords—cryptography; compression; lossless; lossy; compressive sensing

I. Introduction

The development of informational technology has a broad impact on the human ways of communication from initially through 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 like 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 of 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 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].

In this paper, the author will mainly discuss a combination of compression and cryptography techniques to enhance efficiency in the transmission and safety of image data during the last decade.

II. The Procedure of Sorting Out Literature

In line with a growing need for data and information transmission in a safe and quick manner, researches on image protection through a combination of cryptographic and compression techniques begin to take form. Combination of these two methods may be classified into three categories based on their processual sequences: (1) a cryptographic technique followed by a compression technique [encryption-compresssion], (2) a compression technique followed by a cryptographic method [compression-encryption], and (3) both techniques employed in a single process [hybrid compression-encryption].

The procedure type of literary works is done by seeking out articles in journals and conference proceedings, published from 2004 up to 2016. This searching uses ontology of hybrid image compression encryption mapped and taken from several sources: IEEEXplore Digital Library(IEEEXplore), Science Direct(Direct), Springer, Scholar and other journals and proceedings outside IEEEXplore, Direct, Springer, Scholar, and others. This procedure results in 64 articles with the following details: IEEEXplore (10 articles), Direct (11 articles), Springer (17 articles), Scholar (20 articles), and others (6 articles). Step two: 64 articles is classified into 3 (three) based on their techniques: compression-encryption, encryption-compression, and hybrid compression encryption. Classification of those articles results in 47 (73.44%) relevant articles as shown in Fig 1.

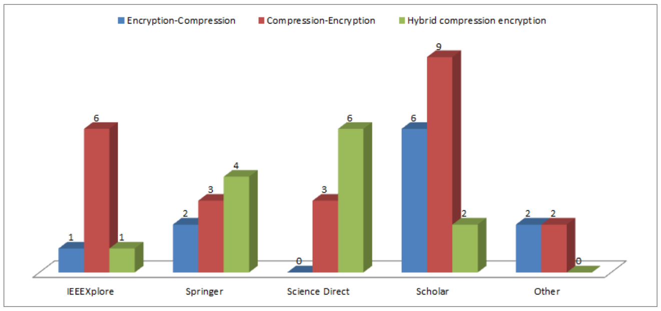

Fig. 1. Articles sorted by classification

Analytical result of 47 articles can be classified into three groups as shown in Fig 2. There are 11 articles (23.40%) in the First group discussing the development of cryptographic techniques followed by compression techniques. The second group of 23 articles (48.94%) discusses the development of compression techniques followed by cryptographic techniques. The third group of 13 articles (27.66%) presents the combination of both techniques.

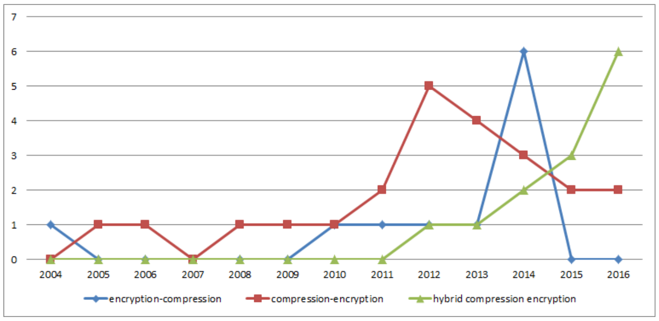

Fig. 2. Research developments according to yearly classification

III. Encryption-Compression Technique

A. *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 downsampled 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 grayscale 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 zig-zag, Run Length methods, and Huffman encoding. The proposed scheme provides two freeways of data encryption and compression. The test is applied to 3 grayscale 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.

B. *Symmetric and Asymmetric Cryptographic Method with Lossless Compression*

Shafinah and Ikram[8] have applied a concept of Pretty Good Privacy (PGP) developed by Phil R. Zimmermann to enhance digital file safety for textual data. PGP concept of merging technique is applied using IDEA symmetric cryptography and asymmetric RSA method, with lossless compression technique using ZIP. By contrast, Kale et al. [9] combine symmetric cryptographic techniques 3D-Advanced Encryption Standard (3D-AES) and asymmetric cryptography using the RSA method, with lossless compression technique using Shanon fano. The method of 3D-AES is used to generate symmetric keys by randomizing first key arrays three times which generates a better key in each randomization. As a result, the final key will be stronger than standard AES keys. This technique is capable of providing a high level of informational protection of message confidentiality, and originality exchanged between two parties as well as reducing the length of words. This application works on smartphones and does not require other encryption tools. In contrast, Arunkumar and Prabu[10] proposed the combination of an asymmetric cryptographic technique using RSA method and lossless compression technique using SPIHT method. This combination method allows a partial data access on the part of decoder so that it produces a better efficiency and less computational complexities than the existing approaches. Hence, it will likely be a prospective avenue for video compression in the future.

C. *Symmetric Cryptographic Method with Lossy Compression*

Some researchers have developed a conventional technique of symmetric key cryptographic method and lossy compression method [11]-[14]. Razzaque and Thakur [11] used an image compression method to minimize bit numbers in the post-encrypted images to protect them against unauthorized access. The encryption processes images without the secret key exchange process. You do this by dividing the test images into four blocks, then performing the image encryption using sender's K1 key on one of the essential image blocks and then delivered a receiver it. The receiver then encodes the image he/she received using his/her K2 key and sends it back to the sender. Subsequently, the sender decrypts it using a K1 key and then compresses it using Discrete Cosine Transform (DCT) and sends it back to the receiver. The testing result of 5 grayscale images of 512x512 size with ratio 8 indicates that average PSNR value is 26.35 dB. This size means a still relatively good quality of images after their network transmission.

Kang et al.[12] proposed the application of lossy scalable compression technique after cryptographic process using standard stream cipher method. The values of image pixels that have been encrypted with standard a stream cipher are then put into the compression process by sending subsamples and bit planes. This proposed scheme has an advantage on the part of the decoder as there are no intensive computational iterations and no other orthogonal matrices. It is also applicable to soft and rich-in-texture images. The testing result of 4 grayscale images gives average PSNR values of over 30 dB, indicating that the quality of image remains fairly good. This method is also resistant to statistical attacks as is randomly observed from the visual test.

Aujla and Sharma[13] proposed a combination method of the symmetric cryptographic technique using random permutation method and lossy compression technique using Haar and Daubechies wavelet transformation method to enhance the efficiency of compression process of already encrypted images. The application of this approach results in a positional change for the similar pixel values after their encryption. The resultant images are almost identical to the original as the correlative values among neighboring pixels are relatively high. The result of the encrypted image compression, using orthogonal wavelet transform, is that the majority of the pixels is converted into a series of coefficients. There will be a reduction of data if you remove redundant information contained in the coefficient. This application of compression approach to encrypted images proved to be more efficient according to a testing on CR, Mean Square Error (MSE), and PSNR.

Kamble and Manwade[14] proposed a symmetric cryptographic technique on colored images using Blowfish and block cipher methods followed by a lossless compression method using LBG (Linde-Buzo-Gray) vector quantization algorithm. A test on 6 data samples indicates that the application of a symmetric key algorithm using block cipher and Blowfish methods to encrypt individual colored images requires an average encryption speed of 10.167 byte/second. The quality of encoded images is relatively good, which is over 30 dB.

TABLE I presents a summary to encryption-compression technique reviewed in this section.

TABLE I. ENCRYPTION-COMPRESSION TECHNIQUE SUMMARY

No.	Author, Year	Compression		Cryptographic		Key Stream Generator	Compression Method	Cryptographic Method
		Lossy	Lossless	Symmetric	Asymmetric			
1	Johnson et al.[4], 2004		X	X		PRG	Slepian-Wolf Coding	Binary Stream Cipher
2.	Liu et al.[5], 2010		X	X		-	RPC (Slepian-Wolf Coding)	Stream Cipher
3.	Mariselvi and Kumar[6], 2014		X	X		-	RPC (Huffman or Arithmetic Coding)	DES
4.	Sharma et al.[7], 2014		X	X		-	Zig-zaq scan, Huffman, and RLE	MPDFRFT
5	Shafinah and Ikram[8], 2011		X	X	X	-	ZIP	RSA, IDEA
6	Kale et al. [9], 2014		X	X	X	-	Shanon Fano	RSA, 3D-AES
7	Arunkumar and Prabu[10], 2014		X		X	-	SPIHT	RSA
8	Razzaque and Thakur [11], 2012	X		X		-	DCT	Multiplicative Cipher
9	Kang et al.[12], 2013	X		X			Lossy Scalable Compression	Stream Cipher
10	Aujla and Sharma[13], 2014	X		X			DWT (Haar and Daubechies)	Random Permutation
11	Kamble and Manwade[14], 2014	X		X			LBG Vector Quantization	Block Cipher and Blowfish

IV. 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 ciphertext data to do the analysis. An intruder needs enough data to analyze a ciphertext. 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].

A. Lossy Compression Method with Symmetric Cryptography

Loussert et al.[3] proposed an integrative model of lossy compression technique using DCT transformation method with an asymmetric cryptographic technique using bit xor operation with fingerprint as the key. The testing result indicates that transmission time increases and systemic security can be increased using biometric characteristics. In this study, the method is applied to a sample of data, and the result shows that the data is capable of being encoded and re-decrypted.

Krikor et al.[16] proposed a selective encryption method to reduce a computational process on large images. Selective encryption aims at obtaining a quick method by encrypting a small piece of a bit stream. The proposed method is in the form of image decomposition into block 8x8. From its spatial domain, the block is later transformed into frequency domain using DCT. Subsequently, DCT coefficient of high-frequency image blocks is encrypted using Non-Linear Shift Back Register (stream cipher). The proposed algorithm for these encryption purposes uses a key of 6-byte long. The first 4 (four) bytes are used to generate a pseudorandom sequence to encrypt images using a stream cipher, and 2 (two) other bytes are two prime numbers used to create rows and columns to randomize images. Based on visual information of randomly perceived encryption result, this proposed method offers a higher security level than if it encrypts all image data.

Benabdellah et al.[17] recommended a compression technique using Faber-Schauder Multiscale Transform (FMT) method followed by quantization on dominant transformed coefficients. Next, the result is encrypted using DES or AES algorithm. The results show that, when using AES, encryption speed is approximately 1,022 times faster than DES method. Both proposed techniques still demonstrate a good performance. The testing result of a visual image looks random, while on FMT-AES the histograms is a Gaussian function, meaning that it is secure from statistical attacks. The quality of reconstructed images is also excellent which is visible from the average PSNR values of over 30 dB for either FMT-AES or FMT-DES methods.

Samson and Sastry[18] proposed a new approach towards image encryption supported by a lossy compression using multilevel wavelet transformation. First, a 2-D multilevel wavelet transformation is applied to input images and then followed by threshold testing on their decomposed structures to obtain compressed images. In this study, Samson tests the application of 5 wavelet filters, i.e., 'haar' 'bior6.8', 'coif5', 'sym8' to see the effect of wavelet filters on the proposed method. The testing result shows that compression ratio depends on types of image and transformation used. Samson and Sastry[19] also suggest a method of securing data that supports RGB images by combining a compression technique using lifting wavelet transform and predictive coding with an encryption scheme using Secure Advanced Hill Cipher (SAHC), involving a pair of involutory matrices, Mix function and an operation called XOR. The test results visually on two pieces of the color image looks random, so that the proposed method can be used to transmit image data efficiently and securely.

Gupta and Silakari [20] introduced a scheme of chaos-based compression and encryption using a cascading 3D cat map and standard map. As for the session to secure key exchange, the use of Elliptic Curve Cryptography is essential. Before its encryption, the image is first compressed using curvelet transformation to remove redundancy in the colored images for a faster transmission. The testing result shows that average PSNR values are over 30 dB, NPCR is over 99%, UACI is below 33%, and entropic values are 7.99 in average, which are close to 8. This shows that the proposed method provides excellent security and speed as well as a better transmission performance.

Li and Lo[21] suggested a combination of image compression and encryption by controlling encryption parameter. The advantage of this proposed compression and encryption combination lies in its applicability on distorted images and its reversibility even without the encryption key. This method uses a base on the JPEG method, by adding an encryption algorithm into its transformation stage. Image encryption and compression method may be employed simultaneously using DCT transformation and block of the 8x8 pixel. It develops a new orthogonal transformation by introducing sign-flip into butterflies method on the DCT flow-graph structure. One of the alternative ways to use during JPEG transformation is a different orthogonal transformation, which is produced by the sign-flipping strategy. By selecting butterflies method for sign-flip, it is expected to control the visual quality of encrypted images. The testing result of significant key space and encryption space, of security against replacement attack, and of security against statistical model-based attack has demonstrated that the proposed method is capable of securing image data.

B. Lossless Compression Method with Symmetric Cryptography

Chung and Kuo[22] suggested two approaches combine encryption with multimedia compression system, i.e., a modified selective encryption using entropy coder with some statistical models. The proposed method works by changing entropy coders into cipher encryption using some statistical models. The test results showed that compression without sacrificing performance and computation speed, security remains achievable.

Hermassi et al.[23] introduced a new scheme called Chaotic Human Tree (CHT) method using a modification of Huffman code implemented on textual data. This approach has succeeded in overcoming the downsides of Multiple Huffman Coding (MHT) by combining stream cipher algorithm and Huffman compression algorithm. By contrast, the cryptographic method used is a chaotic map to generate keystream by renewing Huffman coding tree. Keystream generated is based on the concept of chaos; the permutation is then performed on the base tree without changing their statistical models. As a result, a symbol can be encoded by more than one codeword for data with the same length. An analysis of compression performance results in an exactly same ratio between proposed method and standard Huffman scheme. This fact is, in fact, a consequence as there is no statistical change in the model during Huffman tree mutation. Each symbol encrypted using the proposed method will have the same code length of the code used in the classic Huffman scheme. The proposed method is relatively immune to brute force attacks. In comparison to arithmetic coding, the proposed method has a little higher compression efficiency. However, it has a slower encryption/decryption speed than that of Huffman+stream cipher algorithm. Chen et al.[24] also proposed a scheme of compression and encryption based on chaos. For encryption, they use a table dynamically modified in its searching process. As a result, the target symbol will finally connect to other partitions that result in fewer iterations to find it. Simulations show that the proposed modification offers a better compression performance, while execution efficiency is proportional to its security level.

Kishore et al.[25] proposed the application of Slepian-Wolf coding compression method, while the cryptography is done using bit-wise exclusive OR operation. The study focuses on the design and analysis of lossless compression, where image data is encrypted using stream cipher method after its compression. The proposed method is tested on two grayscale images to check the randomly perceived cipher image visually. The success of this approach lies in its provision of partial access to the source of data on the part of the decoder to increase security.

V. Nair et al.[26] proved that arithmetic coding is randomly not secure. Therefore, a lossless compression method is presented using arithmetic coding technique by dividing data into similar intervals and followed by symmetric encryption technique using bit-wise XOR with pseudorandom bit sequence. This system offers compression and security and is capable of blocking any attacks launched to obtain information about input or output permutation and information on how to divide intervals. The proposed method is proved to be secure and immune to chosen plaintext attack. Also, it is capable of reducing a delay during data transmission and of increasing data security.

Sudesh et al.[27] proposed the application of adaptive compression to obtain a high compression ratio. An adaptive compression works to reduce the size by analyzing frequencies repeatedly and then retaining them in a dictionary or tabular forms. By contrast, cryptography uses Milline transform approach based on the mathematical transformative operation which makes it perform faster and more efficient. The level of security is obtained through the method of implementation transformation Milline encoding, Whereas coding efficiency will be achieved when you apply adaptive dictionary. The testing result of 6 sample images indicates that the average PSNR values are 32.93 dB.

Xiang et al.[28] proposed a Joint compression and selective encryption based on SPIHT(JCSE-SPIHT), i.e., a compression algorithm and selective encryption based on set partitioning in hierarchical trees (SPIHT), by embedding encryption into SPIHT coding procedure. The basic idea of JCSE-SPIHT method is to perform a fast random insertion(FRI) on the list of insignificant pixels(LIP) and insignificant sets(LIS) on selected numbers of iteration coding of SPIHT. Therefore, selective node randomization of LIP and LIS by FRI is in the first round (r) of iteration, where parameter r is used to control the particular encryption strength. A proper selection of r will generate a good trade-off between security requirement and computational overhead. The testing result indicates that r = 6 is a suitable configuration as the plain image is well protected and requires 1-4% of data to be encrypted. The proposed method generates keystream plain text that is dependent on JCSE-SPIHT compression algorithm that makes it immune to chosen-plaintext attacks.

C. Combination of Lossy and Lossless Compression Method with Symmetric Cryptography

Ou et al.[29] developed an ICES (Image Compression Encryption Scheme) model by integrating compression technique using Discrete Wavelet Transform(DWT) transformation method, orthogonal wavelet family type Haar without quantizer and Significance-Linked Connected Component Analysis(SLCCA) encoder proposed by Chai et al.[30]. The cryptographic technique used is AES method. The proposed method allows compressed images to generate a high compression ratio while maintaining security during transmission so that simultaneously can solve the problem of bandwidth and safety. The test results on six image grayscale with different image sizes shows that the reconstructed image is of high quality, and efficient.

Alfalou et al.[31] proposed simultaneous fusion, compression, and encryption of multiple images (SFCE) methods to obtain image compression and encryption simultaneously. The proposed techniques adapt the DCT method, by combining spectral fusion according to DCT properties, particular spectral filtering, and quantization of encoded frequency using select bit number. The study finds that this size of adaptation provides a good trade-off between bandwidth spectral plane and output number of reconstructed images. Improved encryption capabilities are achieved by using biometric locks and by randomly changing the angle of rotation of each block before fusion spectral. The use of the image as the key of real-valued has succeeded in increasing compression level into 50% better than that of the original SFCE method.

The following study uses a modification of chaotic key generator on encryption process. Tong et al.[32] proposed an image compression and encryption scheme based on nearest-neighboring coupled-map lattices(NCML) and Non-uniform Discrete Cosine Transform(NDCT). A new chaotic map is recommended based on Devaney theory, which works as a local map of NCML called system spatiotemporal cross chaotic. This algorithm adopts Huffman coding and NDCT for transforming image data and compressing it. It consists of two steps of the encryption process. Compressed data is divided into blocks and is subsequently permutated and diffused amongst blocks simultaneously. The parameter obtained through system spatiotemporal cross chaotic is used to control NDCT non-uniformity, which plays a significant role in the encryption process. The result of security test indicates that the proposed method offers high speed and safety as well as a good compression effect. This is observable from the average

PSNR values of 6 tested images of over 30 dB, average entropy values of over 7.99 which is close to 8, average NPCR values of over 99%, and average UACI values of over 33%. Besides, the degradation result of the performance of the proposed method is 3.26-9.02% better than that of a typical technique of DCT and Huffman coding followed by AES. Tong et al.[33] also conducted a study to combine lossy compression technique using lifting wavelet transform(LWT) and lossless compression technique using SPIHT coder, followed by cryptosystem symmetric using Chaotic sequence generation. Testing of the proposed method is done using five grayscale image data with a size of 512 x 512 pixels. The measurement result of the change rate of cipher text is about 50% (the change rate is the ratio of the position of the original cipher text and cipher text in which the plaintext is modified). The testing result of changing one bit of bitmap image, on the modification level of cipher stream, ranges between 40-44%, indicating a high sensitivity to plain text. Based on the testing of the key sensitivity of five images, an average value of key sensitivity is more than 49.9%, indicating that algorithm has an excellent key sensitivity. Its compression ratio is about 50% of the original file size. The test results histogram also looks flat; it shows that the frequency of appearance of color in the cipher image looks evenly, so is secure against statistical attack. The entropy value is relatively high as well, i.e., 7.99 in average which is close to 8, meaning that this method is secure from cryptanalytic entropy attack.

Zhiqianga et al.[34] combined JPEG image compression algorithm with a chaotic encryption algorithm. This process can save storage space for images and tight transmission security of pictorial information more efficiently. In contrast, Goel, N et al.[35] combined a lossy compression technique using DCT method with a lossless compression technique using Huffman coding, followed by symmetric cryptosystem technique using Logistic Map method. This paper highlights anything to do with Huffman coding in the view of the proposed image encryption method. Besides, it also presents a snapshot of one logistic map dimension, having been used as pseudorandom numbers. The proposed method is shown to overcome many limitations of dictionary-scrambling-based encryption technique. The testing of the proposed method is excellent when implemented on the low-contrast image, as seen from the high PSNR value. Also, the method has high sensitivity key, and use of the compressibility of the encoder does not result in adverse effects.

Kumar and Vaish [36] proposed a compression-encryption image method to transmit image quickly and securely through the network. The core idea of the proposed method is to select significant and non-significant coefficient in the wavelet domain. These two coefficients will be encrypted using pseudo-random number sequence and permutation on their each coefficient. The proposed method is first to perform a DWT transformation process. Furthermore, do the pseudo random encryption process (PRNG) and then the compression process using the quantization and entropy coding, whereas wavelet sub-bands detail (LH, HL, HH) substitution process is carried out using the k2 key and is subsequently encrypted using coefficients permutation. The next process of image encryption result is compressed using Singular Value Decomposition(SVD) and Huffman code. Seeing that performance of image compression is mostly based on the selected wavelet transformation filter, then the use of different filters like biorthogonal wavelet, Haar, Symlets, Daubechies, Coiflets, etc., is also tested. The test results demonstrate that the use of biorthogonal wavelet filter produces better compression performance. For example, when image Lena is compressed using wavelet biorthogonal on singular values (SVs)=256 and η = 1, the CR value is 0.2883 and PSNR value is 45.66 dB. By contrast, CR values for other wavelets like Symlets, Daubechies, Coiflets, Haar and Discrete Meyer wavelet are 0.2970, 0.2967, 0.2979, 0.3014 and 0.3092 each respectively, while appropriate PSNR values are 45.75 dB, 45.95 dB, 45.04 dB, 42.64 dB, 47.89 dB. Also, the proposed method has an advantage of making use of SVD to obtain a better compression performance while maintaining the desired features of the reconstructed image. The proposed scheme is immune to brute force attacks and proved to be more efficient than that of Zhang and to be better than that of JPEG standard.

D. Joint Method of Lossy or Lossless Compression with Asymmetric Cryptography

Rahmawati et al.[37] combined lossy and lossless compression techniques using DCT, quantization, Huffman coding to obtain a high energy compaction, followed by asymmetric cryptosystem technique using Secure Hash Algorithm-1 (SHA 1) method as its encryption algorithm. Errors in one of the keys will generate an impaired, reconstructed image. The value of compression ratio and PSNR obtained through this algorithm is influenced by the employed quantization matrix. Luminance quantization matrix produces a lower compression ratio than that of chrominance quantization matrix, only that it produces higher PSNR values. The proposed algorithm has a high sensitivity to the use of each of the key. The key sensitivity marks a good encryption performance.

Chal.la et al.[38] proposed a Learning with Errors (LWE) and public-key based compression which is implemented using CNA to reduce a key size. CNA is a new lossless compression algorithm which is practical and has a higher adaptive capability.

TABLE II presents a summary to compression- encryption technique reviewed in this section.

TABLE II. COMPRESSION- ENCRYPTION TECHNIQUE SUMMARY

No.	Author, Year	Compression		Cryptographic		Key Stream Generator	Compression Method	Cryptographic Method
		Lossy	Lossless	Symmetric	Asymmetric			
1	Loussert et al.[3], 2008	X		X		fingerprint	DCT	Bit XOR Operation
2.	Krikor et al.[16], 2009	X		X		Pseudorandom	DCT	Selective Encryption, Bit Stream Cipher
3.	Benabdellah et al.[17], 2011	X		X			FMT	DES or AES
4.	Samson and Sastry[18], 2012	X		X			2-D Multilevel Wavelet Transformation	Permutation
5	Samson and Sastry[19], 2012	X		X			Lifting Wavelet Transform	SAHC
6	Gupta and Silakari [20], 2012	X		X		Cascading 3D Cat Map,Standard Map	Curvelet Transformation	Elliptic Curve
7	Li and Lo[21], 2015	X		X		Random 128-bit Key	JPEG	RC4
8	Chung and Kuo[22], 2005		X	X		Segment Key	Multiple Huffman Tables (MHT) or QM Coder	Stream Cipher
9	Hermassi et al.[23], 2010		X	X		Piecewise Linear Chaotic Map	Renewing Huffman Coding Tree	Stream Cipher
10	Chen et al.[24], 2011		X	X		Chaotic Map	Entropy Coding	Lookup Table
11	Kishore et al.[25], 2012		X	X			Slepian-Wolf Coding	Bit-wise XOR Operation
12	V. Nair et al.[26], 2012		X	X		Pseudorandom Bit	Arithmetic Coding Technique by Dividing Data into Similar Intervals	Bit-wise XOR Operation
13	Sudesh et al.[27], 2014		X	X			Adaptive Compression	Transformation Milline
14	Xiang et al.[28], 2014		X	X			SPIHT	Selective Encryption
15	Ou et al.[29], 2006	X	X	X			DWT, SLCCA	AES
16	Alfalou et al.[31], 2013	X	X	X		Biometric	Combining Spectral Fusion According to DCT Properties	XOR Operation
17	Tong et al.[32], 2013	X	X	X		Spatiotemporal Cross Chaotic System	Huffman Coding and NDCT	Packed into blocks, Permutation Between Blocks and Diffusion in Block
18	Tong et al.[33], 2016	X	X	X		Lorenz map, Henon map, Logistic Map	LWT, SPIHT	Stream Cipher
19	Zhiqianga et al.[34], 2013	X	X	X		Logistic Sequence	JPEG	Chaotic Encryption
20	Goel, N et al.[35], 2014	X	X	X		Logistic Map	DCT, Huffman	Dictionary Scrambling
21	Kumar and Vaish [36], 2017	X	X	X		PRNG	DWT, SVD, Huffman	Stream Cipher
22	Rahmawati et al.[37], 2013	X	X		X		DCT, quantization, Huffman	SHA 1
23	Chal.la et al.[38], 2015		X		X		CNA	LWE and Public Key

V. 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.[39] 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 increases. 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.[39] 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.

Wang et al. [40] proposed a similar technique to that of Al-Maadeed et al.[39], the difference on the Schema Lifting(LS) DCT that is performed on the input image before processing the transformation DWT. Having finished performing the separation of subband approximation (LL) and subband details (LH, HL, HH) through DWT transformation process, encryption and compression are done using a different method. After getting subband LL proceed with the encryption method process using a stream cipher, other subbands are encrypted using a permutation method. By contrast, compression is performed by a third party. Regarding subband LL, the result of encryption is then compressed using lossless compression process (encoding is carried out on each coefficient bit). With subbands LH, HL, and HH, encryption results are then compressed using rate-distortion optimized quantization and is followed by a coding process using an arithmetic coding method. The test results of the proposed method are equivalent to the value of the smallest compression ratio (CR = 4.461) when using filters Bior2.2. By contrast, the best-suited subband level for the proposed scheme is on level 3. Also, the proposed scheme provides a small computation time.

Hassan and Younis[41] offered a combination of lossless compression technique using Quadtree and Huffman coding method and symmetric cryptosystem technique using the partial method where the encrypted data will become a part of compressed data using AES method. The testing result indicates that only 10-25% of the output of Quadtree compression algorithm is encryptable. The testing of the proposed method is performed on a grayscale image of size 256x256. The visual testing of a cipher image looks random. The test results histogram also looks flat; it shows that the method is safe from statistical attack. However, the PSNR is low, i.e., below 30 dB, meaning the quality of the reconstructed image is not reasonably safe.

Xiaoyong et al.[42] combined a compression technique using an algorithm of generalized knight's tour, DCT, Quantization and zigzag scan coder and symmetric cryptosystem technique using non-linear chaotic maps method. In contrast, the encoding procedure uses a nested generalized knight's tour (NGKT) matrix generated scramblingly by Semi Ham algorithm on the bright image. Furthermore, this is to produce a high image compression ratios by utilizing DCT and quantization coding. The diffusion process is subsequently done using encryption parts of DCT coefficient obtained from Chen chaotic map. The evaluation of the proposed scheme is carried out by a series of tests using five grayscale images, and the results show that the proposed scheme has a compression performance and good security. Evaluation is also done using compression Degree (CD) used to reflect the compression performance. After the testing result of 5 data, it turns out that the compression performance of the proposed method is better than that of Zang, Yuen, and Zhou, to which this paper refers. However, it is closer to JPEG algorithm. Analysis of key space shows that computational accuracy of 64-bit double precision numbers is about 10-14. The key space of each chaotic map is 1014, and chaotic key space is 1014 × 1014 × 1014 = 1042 which are bigger than 2100[43] that the proposed scheme is relatively resistant to brute force attacks. The testing of key sensitivity provides a value of > 99%, meaning that the key sensitivity is excellent. The testing of differential attacks shows that NPCR value is over 99% and UACI value is over 33%. It means that the proposed scheme is sensitive to plain image and is capable of blocking differential attacks due to its high NPCR and UACI values. The Robustness analysis shows that an image obtained from a decryption process is still recognizable even though it is not as good as the original. The last test is a Structural Similarity Index Measurement (SSIM) comparing images regarding lighting, contrast, and structure, replacing the application of PSNR method in evaluating the similarity among pictures. The testing result of SSIM of 5 data shows a result that is closer to 0, meaning that the proposed scheme is secured.

Hamdi et al.[44] proposed a method using a more efficient compression technique to generate a high-quality image and little computational complexities. The cryptographic method is confusion and diffusion technique which is integrated and connected to compression chains. The first step is to generate three keys for encryption process using Chirikov Standard Map algorithm. The next step is to perform DWT transformation and is followed by a bit encryption on wavelet coefficient (LL Subband) using the first key, whereas other subbands are undergoing encryption process using the list of LIP and second key. The third step is permutation after SPIHT coding. This stage is to increase the diffusion of the encrypted image. It is to ensure an efficient informational diffusion according to bitwise permutation process. The testing result of the image of a house using level-3 decomposition shows that PSNR value is 39.674, while the image of an airplane using level-2 decomposition shows that PSNR value is 38.013. The average key sensitivity of MAD value for ten tested data images with three different keys is 85.13, which is closer to its ideal value, 85.33 (256/3). By contrast, the average number of pixels change rate (NPCR) of 10 tested images for all stages is 99.55% bigger than the required value of 99%, and the value of Unified average changing intensity (UACI) of 33.59% is larger than the required value of 33%. Thus, the result of differential analysis indicates that the proposed encryption algorithm is very sensitive to small changes in the original images and very resistant to differential attacks.

The following several studies use a concept of compressive sensing(CS) to perform compression and encryption process simultaneously[45]-[52]. Zhou et al.[45] proposed an image encryption-compression hybrid algorithm based on CS and random pixel exchanging, where compression and encryption are done simultaneously. The first divides the image into four blocks for the purpose of compression and encryption. Then an exchange of the pixels that have been randomized to be compressed and encrypted. This method makes use of circulant matrices to develop measurement matrices on CS and to control first line vectors of the circulant matrices using the chaotic system. The proposed algorithm is proved to be secure. The simulation shows that the proposed method provides good security and excellent performance of the compression. It is perceived from the histogram of three original images which is clearly different from each other, whereas the encrypted image has a similar histogram. Huang et al.[46] also proposed a CS-based encryption method combining sampling, compression, and encryption simultaneously. The testing result indicates that the proposed encryption method does not achieve an outstanding randomness, even the diffusion and sensitivity outperform image encryption method performed in parallel. The measurement result shows that the average PSNR values of 5 tested data are over 30 dB, indicating a good reconstruction quality. This method uses the key of 128 bits, meaning that it occupies the main space up to 2128≈3.4028 × 1038. In fact, it provides an adequate security against brute force attacks. It is also indicated by its average entropy values of 7.99, which is close to 8. The histogram looks visually flat, meaning that this method is immune to statistical attack. The average coefficient correlative value of adjacent pixels of 5 images is 0.0024, which is close to 0. Apart from that, the mean value of NPCR and UACI is close to 99.61% and 33.46% respectively, meaning that this method is very sensitive to small change in the key.

Fira[47] proposed a method designed to achieve an efficient compression to save memory space, to reduce transmission time, and to reduce energy consumption. CS algorithm is applied to compress and encrypt ECG signals. This study analyzes the compression obtained through standard wavelet-dictionary, while encryption is used to analyze the effect of its projection matrices.

Zhang et al.[48] designed a simple scheme to simultaneously compress and encrypt an image using random convolution and random subsampling methods based on CS encoding to offset the downsides of double random phase encoding which has no compression capability. Utilization of random methods with an underlying convolution CS inspires this method. In this method a CS using convolution with a random pulse followed by random subsampling. The testing shows that the proposed scheme is relatively immune and is capable of blocking the cropping attacks.

Ahmad et al.[49] proposed a new image encryption scheme based on chaotic maps and orthogonal matrices. In addition to performing encryption for higher security, this method also supports partial encryption for a faster process and a better result. The proposed scheme uses a primary method of new properties of the orthogonal matrices to get a random orthogonal matrix using Gram-Schmidt algorithm, and nonlinear chaotic map to randomize the pixel values of a plain image. The proposed scheme is capable of reconstructing an image, even if it is distorted by AWGN/noise due to its transmission through the network. The experiment and security analysis show that the proposed scheme is relatively secure and robust from channel noise and JPEG compression. The output quality of a decrypted image is fairly good. The highest PSRN value is 40 dB, whereas the average PSNR values of 4 tested images are 31.38 dB. The analysis of average differential attack of 4 tested images gives partial NPCR value=99.1% and UACL=15.38%. This fact indicates that the proposed algorithm is very sensitive to input change, but its security is still lacking, i.e., below 33%. The result of histogram analysis of encryption is close to Gaussian distribution, meaning that encrypted histogram is capable of concealing frequency distribution of plain text images.

Chen et al.[50] proposed an encryption and compression scheme based randomly on Elementary Cellular Automata (ECA) and Kronecker Compressed Sensing (KCS). The first stage: encryption is done using ECA to generate an image uniformity at its sparsity level. Second stage: KCS encryption is performed to encrypt and compress randomized images by measuring matrices with a reduced size conforming to the original image size. The proposed Kronecker Compressed Sensing (KCS) is used to solve high computational complexity and a bigger storage demand due to big matrix size. The experiment indicates that the proposed method based on ECA offers excellent performance in randomizing and enhancing uniformity at its sparsity level. Image encryption and compression based on the application of the method gives a higher level of confidentiality and a good performance of compression and flexibility.

Deng et al.[51] proposed a joint algorithm between 2D CS and Discrete Fractional Random Transform (DFrRT), where compression and encryption can be performed simultaneously with a simple operation and high security. Plain text is expressed in the 2D cosine discrete domain and measured from two orthogonal directions. Furthermore, after encrypting using DFrRT do repeated measurements. This scheme shows a good performance by combining CS capability with simple operation of DFrRT. The testing result indicates that histogram of the reconstructed image takes the form of Gaussian function, meaning that the proposed scheme has a high capability to impede statistical analysis attack. Besides, the simulation shows that the proposed scheme is capable of blocking pixel cropping attack, brute-force attack and is sensitive to key change.

Zhou et al.[52] proposed a method of compression-encryption image scheme based on hyper-chaos system and 2D sensing. The parameters of 2D CS used are: x01 = 0.13, x02 = 0.25, μ = 3.99. The original value of hyper-chaos system is stated as: x0 = 0.3, y0 = 0.4, z0 = 0.5 and h0 = 0.6. The result of simulation shows that the proposed compression-encryption image scheme is effective, robust and secured with a good compression performance. This method is capable of blocking statistical analysis, brute force and noise attacks as the key space used is much bigger. Therefore, this proposed algorithm is useful for reducing the storage size of adequate security.

TABLE III presents a summary to hybrid compression-encryption technique reviewed in this section.

TABLE III. HYBRID COMPRESSION- ENCRYPTION TECHNIQUE SUMMARY

No.	Author, Year	Compression			Cryptographic		Key Stream Generator	Compression Method	Cryptographic Method
		Lossy	Lossless	Compressive Sensing	Symmetric	Asymmetric			
1	Al-Maadeed et al.[39], 2012	X			X		Chaotic Maps	DWT	Selective Encryption
2.	Wang et al. [40], 2015	X	X		X			LS DCT, DWT, Quantization and Adaptive Arithmetic Coding	Selective Encryption (Stream and Permutation Ciphers)
3.	Hassan and Younis[41], 2013		X		X			Quadtree and Huffman Coding	Partial Encryption, AES
4.	Xiaoyong et al.[42], 2016	X	X		X		Non-linear Chaotic Maps	DCT, Quantization, Ziqzaq Scan, Entropy Coding	Selective Encryption , NGKT
5	Hamdi et al.[44], 2017	X	X		X		Chirikov Standard Map	DWT, SPIHT	Confusion and Diffusion Technique Which is Integrated and Connected to Compression Chains
6	Zhou et al.[45], 2014			X	X		Logistic Map	CS	Random Pixel Scrambling
7	Huang et al.[46], 2014			X	X		Spatio temporal Chaos	CS	Including Arnold Scrambling, Mixing, S-box, Block-wise XOR Operation
8	Fira[47], 2015			X	X			CS	Substitutions
9	Zhang et al.[48], 2015			X	X			Random Convolution, Random Subsampling Methods Based on CS Encoding	A Linear Transform Encryption Mode and There Are Two Masks
10	Ahmad et al.[49], 2016			X	X		Nonlinear Chaotic dan Logistic Map	DCT, Matrix Orthogonal (via Gram-Schmidt Process)	Partial Encryption (Block- wise Random Permutation, Diffusion Process)
11	Chen et al.[50], 2016			X	X			KCS	ECA
12	Deng et al.[51], 2016			X	X		Logistic Map	2D CS	DFrRT
13	Zhou et al.[52], 2016			X	X		Hiper-Chaos	2D CS	Cycle Shift Operation

VI. CONCLUSIONS

The most combination of 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 measurement of the quality of 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 enhancing 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, still good quality of data during reconstruction and security assurance.

REFERENCES

[1] M. Merdiyan and W. Indarto, “Implementasi Algoritma Run Length, Half Byte, dan Huffman untuk Kompresi File,” in *Seminar Nasional Aplikasi Teknologi Informasi 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, pp. 10–28, 2011.

[9] N. A. Kale and S. B. Natikar, "Secured Mobile Messaging for Android Application," *International Journal of Advance Research in 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 Mobile Computing (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] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image Encryption Using DCT and Stream Cipher," *European Journal of Scientific Research*, vol. 32, no. 1, pp. 47–57, 2009.

[17] M. Benabdellah, F. Regragui, and E. H. Bouyakhf, "Hybrid Methods of Image Compression-Encryption," *J. of Commun. & Comput. Eng.*, vol. 1, no. 1, pp. 1–11, 2011.

[18] C. Samson and V. U. K. Sastry, "A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 3, no. 9, pp. 178–183, 2012.

[19] C. Samson and V. U. . Sastry, "An RGB Image Encryption Supported by Wavelet- based Lossless Compression," *International Journal of Advanced Computer and Aplications (IJACSA)*, vol. 3, no. 9, pp. 36–41, 2012.

[20] K. Gupta and S. Silakari, "Novel Approach for Fast Compressed Hybrid Color Image Cryptosystem," *Advances in Engineering Software*, vol. 49, no. 1, pp. 29–42, Jul. 2012..

[21] P. Li and K. Lo, "Joint Image Compressio n and Encryption Based on Alternating Transforms with Quality Control," in *2015 Visual Communications and Image Processing (VCIP)*, 2015, pp. 1–4.

[22] Chung-Ping Wu and C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828–839, Oct. 2005.

[23] H. Hermassi, R. Rhouma, and S. Belghith, "Joint compression and encryption using chaotically mutated Huffman trees," *Communications in Nonlinear Science and Numerical Simulation (ELSEVIER)*, vol. 15, no. 10, pp. 2987–2999, 2010.

[24] J. Chen, J. Zhou, and K.-W. Wong, "A Modified Chaos-Based Joint Compression and Encryption Scheme," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, no. 2, pp. 110–114, Feb. 2011.

[25] P. S. Kishore, N. A. Nagendra, K. P. Reddy, and V. V. S. Murthy, "Smoothing and Optimal Compression of Encrypted Gray Scale Images," *International Journal of Engineering Research and Applications (IJERA)*, vol. 2, no. 3, pp. 23–28, 2012.

[26] A. V. Nair. S, G. K. Sundararaj, and T. S. R. Perumal, "Simultaneous Compression and Encryption using Arithmetic Coding with Randomized Bits," *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, vol. 2, no. 2, pp. 38–42, 2012.

[27] Sudesh, A. Kaushik, and S. Kaushik, "A Two Stage Hybrid Model for Image Encryption and Compression to Enhance Security and Efficiency," in *2014 International Conference on Advances in Engineering & Technology Research(ICAETR - 2014)*, 2014, pp. 1–5.

[28] T. Xiang, J. Qu, and D. Xiao, "Joint SPIHT Compression and Selective Encryption," *Applied Soft Computing*, vol. 21, pp. 159–170, Aug. 2014.

[29] S.-C. Ou, H.-Y. Chung, and W.-T. Sung, "Improving the compression and encryption of images using FPGA-based cryptosystems," *Multimedia Tools and Applications*, vol. 28, no. 1, pp. 5–22, Jan. 2006.

[30] B. Chai, J. Vass, X. Zhuang, and C. Science, "Significance-Linked Connected Component Analysis for Low Bit Rate Image Coding," vol. 8, no. 6, pp. 774–784, 1999.

[31] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing The Performance of a Method of Simultaneous Compression and Encryption of Multiple Images and Its Resistance Against Various Attacks," *Optics Express*, vol. 21, no. 7, pp. 10253–10265, 2013.

[32] X.-J. Tong, Z. Wang, M. Zhang, and Y. Liu, "A New Algorithm of The Combination of Image Compression and Encryption Technology Based on Cross Chaotic Map," *Nonlinear Dynamics*, vol. 72, no. 1–2, pp. 229–241, Apr. 2013.

[33] X.-J. Tong, P. Chen, and M. Zhang, "A Joint Image Lossless Compression and Encryption Method Based on Chaotic Map," *Multimedia Tools and Applications*, Jul. 2016. A

[34] L. Zhiqianga, S. Xiaoxin, D. Changbin, and D. Qun, "JPEG Algorithm Analysis and Application in Image Compression Encryption of Digital Chaos," in *2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control*. IEEE, 2013, pp. 185–189.

[35] N. Goel, B. Raman, and I. Gupta, "Chaos Based Joint Compression and Encryption Framework for End-to-End Communication Systems," *Advances in Multimedia.*, vol. 2014, pp. 1–10, 2014.

[36] M. Kumar and A. Vaish, "An Efficient Encryption-Then-Compression Technique for Encrypted Images using SVD," *Digital Signal Processing*, vol. 60, pp. 81–89, Jan. 2017.

[37] W. M. Rahmawati, A. Saikhu, and A. E. Kompresi, "Implementasi Algoritma Penggabungan Kompresi dan Enkripsi Citra dengan DCT dan SHA-1," *Jurnal Teknik POMITS*, vol. 2, no. 1, pp. 1–4, 2013.

[38] R. Challa, G. Vijaya Kumari, and P. S. Sruthi, "Proficient LWE-Based Encryption using CAN Compression Algorithm," in *2015 Conference on Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG)*. IEEE, 2015, pp. 304–307.

[39] 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.

[40] C. Wang, J. Ni, and Q. Huang, "A New Encryption Then Compression Algorithm using The Rate Distortion Optimization," *Signal Processing: Image Communication*, vol. 39, pp. 141–150, Nov. 2015.

[41] N. S. Hassan and H. A. Younis, "Approach For Partial Encryption Of Compressed Images," *Journal of Babylon University/Pure and Applied Sciences*, vol. 21, no. 3, pp. 1–10, 2013.

[42] J. Xiaoyong, B. Sen, Z. Guibin, and Y. Bing, "Image encryption and compression based on the generalized knight's tour, discrete cosine transform and chaotic maps," *Multimedia Tools and Applications*, Jul. 2016.

[43] G. Alvarez and S. Li, "Some Basic Cryptographic Requirements for

Chaos Based Cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[44] M. Hamdi, R. Rhouma, and S. Belghith, "A Selective Compression-Encryption of Images Based on SPIHT Coding and Chirikov Standard Map," *Signal Processing*, vol. 131, pp. 514–526, Feb. 2017.

[45] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel Image Compression–Encryption Hybrid Algorithm Based on Key-Controlled Measurement Matrix in Compressive Sensing," *Optics & Laser Technology*, vol. 62, pp. 152–160, Oct. 2014.

[46] R. . Huang, K. H. . H. Rhee, and S. . Uchida, "A Parallel Image Encryption Method Based on Compressive Sensing," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 71–93, Sep. 2014.

[47] M. Fira, "Applications of Compressed Sensing: Compression and Encryption," in *2015 E-Health and Bioengineering Conference (EHB)*. IEEE, 2015, pp. 1–4.

[48] Y. Zhang, K.-W. Wong, L. Y. Zhang, W. Wen, J. Zhou, and X. He, "Exploiting Random Convolution and Random Subsampling for Image Encryption and Compression," *Signal Processing: Image Communication*, vol. 39, no. 20, pp. 202–211, Nov. 2015.

[49] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A Compression Sensing and Noise-Tolerant Image Encryption Scheme Based on Chaotic Maps and Orthogonal Matrices," *Neural Computing and Applications*, Jun. 2016.

[50] T. Chen, M. Zhang, J. Wu, C. Yuen, and Y. Tong, "Image Encryption and Compression Based on Kronecker Compressed Sensing and Elementary Cellular Automata Scrambling," *Optics & Laser Technology*, vol. 84, pp. 118–133, Oct. 2016.

[51] J. Deng, S. Zhao, Y. Wang, L. Wang, H. Wang, and H. Sha, "Image Compression-Encryption Scheme Combining 2D Compressive Sensing with Discrete Fractional Random Transform," *M Multimedia Tools and Applications*, May 2016.

[52] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image Compression–Encryption Scheme Based on Hyper-Chaotic System and 2D Compressive Sensing," Optics & Laser Technology., vol. 82, pp. 121–133, Aug. 2016.