



A Comprehensive Analysis on Image Encryption and Compression Techniques with the Assessment of Performance Evaluation Metrics

N. Mahendiran¹ · C. Deepa²

Received: 6 November 2020 / Accepted: 11 November 2020 / Published online: 11 January 2021
© Springer Nature Singapore Pte Ltd 2021

Abstract

The explosive generation of data in the digital era directs to the requirements of effective approaches to transmit and store the data. The necessities of security and limited resources have led to the development of image encryption and compression approaches, respectively. The digital contents are transmitted over the internet which may subject to security threats. To overcome these limitations, image encryption approaches are developed. The image compression approaches result in the efficient usage of available transmission bandwidth and storage area. Image encryption and compression approach play an important role in the multimedia application that authenticates and secures the digital information. This paper covers the various approaches of image encryption and compression. To validate the performance of the approaches, evaluation metrics are projected and its significance is also discussed.

Keywords Encryption · Cryptography · Compression · Differential analysis · Compressive sensing · Compression gain

Introduction

Recent progression in the area of information and communication technology has an outcome with the creation of a massive quantity of data. As a result, transmission and storage of data rates are increased and the lack of security and privacy concerns are also experienced. The requirements of security concerns have made the development of encryption approaches and the necessities of limited storage and transmission resources have led to the development of compression approaches. The multimedia data are transmitted over the internet which may subject to lack of bandwidth and security threats. To overcome the drawbacks, image

encryption approaches and image compression approaches are developed.

The recent advancement in technology has provided the world with a scenario where chunks of information are transmitted effectively through the public network. The public transmission channels are reliable to transmit the data that may susceptible to vulnerability. The transmitted information may be accessed and modified by ransom ware like unauthorized users [1]. Hence, the transmission of data is attained with a secured format using encryption approaches. The encryption approaches enrich the security of digital images and it shows significance in the transmission of military image, telemetric medical imaging, and video conferencing [2]. In image encryption, the actual image is converted into a meaningless form of data and the receiver will decrypt the image using a unique key that ensures the protection of the transmitted image.

The propagation of multimedia images over the network is growing day by day and the rate of data growth is higher than technology growth. The generation of huge data needs high storage and transmission capability. To address these issues, image compression approaches are introduced. It reduces the size in bytes of the multimedia file without reducing the quality of the multimedia file. Image compression reduces the cost of transmission and storage [3]. Image compression eliminates data irrelevancy and redundancy.

This article is part of the topical collection “Advances in Computational Approaches for Artificial Intelligence, Image Processing, IoT and Cloud Applications” guest edited by Bhanu Prakash K N and M. Shivakumar.

✉ N. Mahendiran
drnmahendiran@gmail.com
C. Deepa
deepa@srcas.ac.in

¹ Department of Computer Science, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India

² Department of Information Technology, Sri Ramakrishna College of Arts and Science, Coimbatore, Tamil Nadu, India

The classification and the overall schema of image encryption approaches are detailed in “Classification of Image Encryption Technique”, the assessment of performance evaluation metrics for image encryption approaches are described in “Assessment of Performance Evaluation Metrics based on Image Quality”, the classification of image encryption approaches are described in “Classification of Data Compression Techniques”, the assessment of performance evaluation metrics of image compression techniques are elucidated in “Assessment of Image Compression Evaluation Metrics” and “Conclusion” concludes with the scope of image encryption and compression approaches.

Classification of Image Encryption Technique

Image encryption converts the actual information into a meaningless structure before transmitting over the public network. Image encryption algorithms play a significant role in protecting the images [4]. The confidential information is inserted into the digital media such as images, audio files, and videos to conceal its existence and the process is carried by the steganography. Thus, information hiding is achieved by steganography in which the existence of data is recognized only by the appropriate receiver. Whereas, in the context of cryptography, the obscured form of data is displayed rather than hiding. In the digital watermarking scheme, digital information is implanted with a distinctive identifiable signal called a watermark [5]. To validate the digital information, a watermark in the digital information will be retrieved at the recipient end. The digital information can be an image, video, text, and audio files that are secured using the watermarking approach. Whenever the illegal usages of watermarked images are identified, the implanted watermark is retrieved to validate the ownership claims.

Framework of Image Encryption Approach

The general framework of the image encryption approach is illustrated in Fig. 1. The plain image act as an input image that is encrypted and it is termed as a ciphered image. The plain and cipher image is signified as PI and CI, respectively. The process of encryption is presented as:

$$CI = En_Fn_{En_K}(PI),$$

where $En_Fn()$ is an encryption function that is applied to the image PI using the encryption key (EK). Similarly, at the recipient side, the decryption function ($De_Fn()$) and decryption key (De_K) is applied in the encrypted image to retrieve the original image is denoted as:

$$PI = De_Fn_{De_K}(CI).$$

The image encryption approach is classified as symmetric and asymmetric approach. In the context of symmetric encryption, both the encryption and the decryption keys are similar i.e., $En_K = De_K$. In this approach, keys are kept confidential during the data transmission process. The dissimilarity identified in the keys i.e., $En_K \neq De_K$ is termed as asymmetric encryption. Whereas, De_K is maintained as private and the En_K is maintained as public.

Image Encryption Approach

The image encryption approaches are categorized into four major types which are compressive sensing, optical, transform, and spatial domain as illustrated in Fig. 2.

The increasing usage of multimedia contents and its applications has necessitated the security system to protect confidential information. Encryption of information is a prominent way of protecting the transmitted data and ensuring the security aspects. Thus, image encryption is projected to protect the images and the security requirement has facilitated the development of various encryption approaches. The normal image will be encrypted and transmitted. The encrypted images will be accessed only by the authorized parties which assure the security of the information. The encryption approaches and its categories are explained in Fig. 2 and its significance is elucidated in the subsequent table. The image encryption approaches are expressed in Table 1.

Fig. 1 Outline of image encryption approach

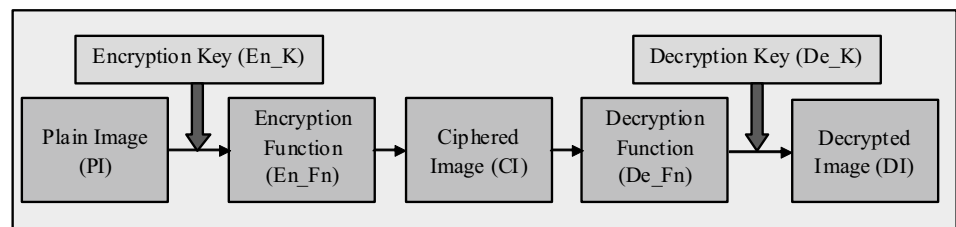
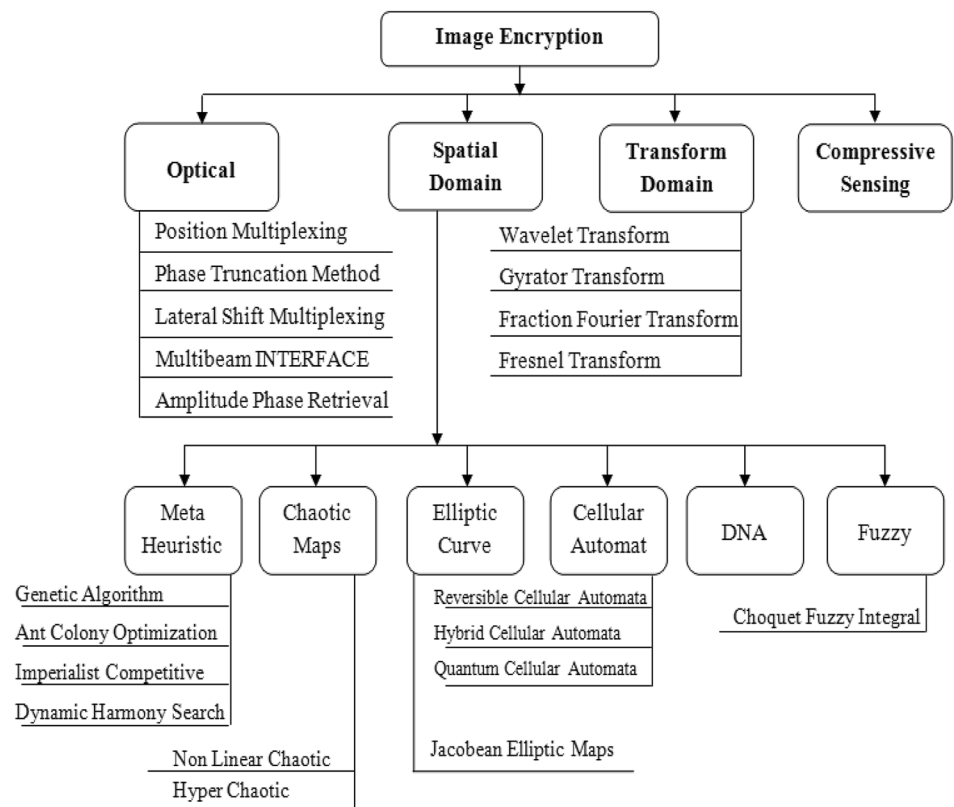


Fig. 2 Categorization of image encryption approach



Assessment of Performance Evaluation Metrics Based on Image Quality

The effectiveness of the image encryption approach is measure with the assistance of evaluation metrics. The varied characteristics of an image encryption approach are investigated using these parameters.

Differential Analysis

The differential attacks are analyzed using the parameters called unified averaging changing intensity (UACI) and number of pixel change rate (NPCR). The sensitivity of the algorithm towards these trivial alterations in the plain image is tested using the differential attack. The images are altered by the attackers and encrypt the images by applying the same secret key. The relationship among the original and modified images identified.

Unified Averaging Changing Intensity (UACI)

UACI estimates the average intensity of divergence among the encrypted and its relevant plain image that having a difference of one pixel [22, 23]. It is determined as,

$$UACI = \frac{\sum_{l,m} B(l, m) - B'(l, m)}{255 \times W_i \times H_i} \times 100,$$

where $B(l, m)$ represents encrypted image and $B'(l, m)$ represents an altered image.

Number of Pixel Change Rate (NPCR)

The value of NPCR is estimated as,

$$NPCR = \frac{\sum_{l,m} B(l, m)}{W_i \times H_i} \times 100.$$

Here,

$$B(l, m) = \begin{cases} 0 & \text{if } B(l, m) = B'(l, m) \\ 1 & \text{if } B(l, m) \neq B'(l, m) \end{cases},$$

where W_i and H_i represent the width and height of the images, respectively. $B(l, m)$ denotes the difference among the relevant pixels of the original and altered image. The range on NPCR belongs [0, 100]. The rate of NPCR in the encrypted file must be close to 100. Both the UACI and NPCR values have to be maximized in the process of encryption [24].

Table 1 Significance of image encryption approach

Technique	Inference
Optical domain [6]	It shows computational efficiency, information storage, and parallel processing in varied dimensions. It is suitable for real-time applications. The information stored in various forms such as spatial frequency, wavelength, phase, and polarization of light
Position multiplexing [7]	This scheme is the encryption of multiple images and utilizes minimum time. The reconstruction of plain text is attained by specially designed the encryption key
Phase truncation method [8]	The color image is enciphered into a single channel as an alternative of three channels. It preserves the non-linear characteristics during the process of encryption
Lateral shift multiplexing [9]	This method incorporated the multiple-image encryption process. It is very effective in addressing the silhouette issue
Amplitude phase retrieval [10]	It is mainly used in the optical-based encryption process. This approach displays a false image instead of a noisy image that ensures security
Meta-heuristics [11]	It offers high security and best quality decrypted image
Chaos-based cryptography [12]	The behavior of the approach is deterministic that is predetermined
Hyper chaotic [13]	This scheme uses the hash function for creating the secret key and estimates the preliminary values of a chaotic system
Elliptic curve-based cryptography [14]	The process of generation of a key is fast and necessitates a random generator. It provides an equal and higher degree of security with a minimal size of the key
Cellular automata [15]	It is easy to execute in both the software and hardware. It offers the highest security and it can run in a parallel way that ensures independency
DNA-based cryptography [16]	It requires minimum storage, effective in energy utilization, and high computational speed
Fuzzy-based cryptography [17]	It is appropriate for uncertain cases of ad reasoning scenarios. The fuzzy approach creates the preliminary constraints of a chaotic map. The differential attacks are resisted with the significant sensitivity of preliminary conditions
Wavelet transform [18]	The depiction of the location and the frequency of the image is provided. It is well suited for non-stationary and has an uneven shape. The information about the temporal data is retained in the process of transformation
Gyrator [19]	It provides non-reciprocal transformation and the data range is not altered. It is a linear, passive, and lossless approach
Fraction Fourier transform [20]	This approach is appropriate for spectral analysis and can detain the non-repetitive event. It can store waveforms of data
Compressive sensing [21]	The bandwidth and storage space of the transmission is reduced in this approach. The CS is a sampling method and it is a low cost that provides cryptosystem. This method is suitable for a restricted system with minimal complexity. This scheme offers great potential in terms of security

Statistical Analysis

The encryption approaches are decrypted using statistical analysis. The correlation analysis (CA) and the histogram analysis (HA) are applied to investigate the adjacent pixel of the image to ensure the robustness of the encryption approach against the statistical analysis.

Correlation Coefficient (CC)

The correlation coefficient is applied to spot the similarity among the relevant pixel of an encrypted and original image. The rate of the adjacent pixels of the original information is strongly interrelated with the direction, i.e., vertical, diagonal, and horizontal. The best image encryption approach minimizes the association in the ciphered image [15]. The value of correlation coefficient is estimated as [25]:

$$R_{(i,j)} = \frac{Ci(i,j)}{\sqrt{De(i) \cdot De(j)}}$$

Here,

$$Ci_{(i,j)} = \frac{\sum_{x=1}^{Ke} (i_x - B_{(i)}) (j_y - B_{(j)})}{Ke}$$

$$De(i) = \frac{1}{Ke} \sum_{x=1}^{Ke} (i_x - B_{(i)})^2,$$

$$De(j) = \frac{1}{Ke} \sum_{y=1}^{Ke} (j_y - B_{(j)})^2,$$

where $Ci(x, y)$ denotes the covariance among the sample i and j which is a coordinate value of the image. The pixel

pairs are represented as Ke of (x_i, y_i) . The standard deviation value of i and j are $De(i)$ and $De(j)$. $B(i)$ indicates the value of x_i pixel and the range of Ci belongs to $[-1, 1]$ and it should be near to 0.

Histogram Analysis (HA)

The value of pixels distributed across the image that is exposed with the assistance of the histogram analysis. The histogram value entirely varies for the original and encrypted images. The distribution of histograms in the original image is non-uniform and the encrypted image is uniform in nature [2]. That is the value of the pixel is equally distributed in space.

Information Entropy (IE)

IE is used to estimate the average information per bit in multimedia content. Every pixel in the multimedia content has varied values and possible information. Therefore, the entropy value of an image determines the equality of uniform distribution [26]. It is estimated as:

$$E(S) = - \sum_s (Po(s_i) \times \log_2 Po(s_i)),$$

where $E(S)$ denotes the entropy of the source image (S), $Po(s_i)$ represents the occurrence probability s_i . The range of IE belongs $[0, 8]$ and an 8-bit image is close to the value 8.

Key Analysis (KA)

The major part of the encryption algorithm is used in generating the security key and the effectiveness of the algorithm relies on the potency of the key that also develops resistance against a variety of security attacks. The considerable properties of security keys are high sensitivity and huge keyspace. If the key size is huge, then the process of decryption is tedious for the attacker and the sensitivity made it unrecoverable [14].

Noise Attack (NA)

The attackers may introduce noise values into the encrypted image that may destroy the needed information in the image. The receiver may not recover the image after the intrusion and the efficient approach can overcome this attack. The attacker may introduce Poisson noise, Gaussian, and additive into the encrypted multimedia content [2].

Execution Time (ET)

The time required to precede the encryption process is determined as execution time (ET). It is the combination of run and compile time [14]. The minimum ET determines the

effectiveness of the approach and measured in terms of minutes, milliseconds, or seconds.

Bit Correct Ratio (BCR)

The value of BCR is applied to measure the variation among the original and encrypted multimedia files. It determines the exactness of the altered decrypted image [27]. It is estimated as:

$$BCR = \left(1 - \frac{\sum_{i,j}^{X \times Y} O(i,j) \oplus De(i,j)}{X \times Y} \right),$$

where i and j values represent the coordinate points of a pixel in the image of dimension $X \times Y$ for the original image O and decrypted image D and the XOR operation is \oplus . The value of BCR belongs to the value of $[0, 1]$.

Mean Squared Error (MSE)

The value of MSE is used to evaluate the correctness of the pixel value and the difference is the error value [28]. It is estimated as:

$$MSE = \frac{1}{XY} \sum_{m=1}^{m=X} \sum_{n=1}^{n=Y} (O(m,n) - R(m,n))^2.$$

Peak Signal-to-Noise Ratio (PSNR)

The quality of the image is estimated by the PSNR value of the decrypted and original [29]. It is estimated as:

$$PSNR = 10 \log_{10} \frac{(2^n - 1)^2}{MSE},$$

where n denotes the count of the bits per pixel and PSNR is estimated in decibel (dB). The value of PSNR must be high and the range belongs to the value of $[0, \infty]$.

Signals to Distortion Ratio (SDR)

The SDR value estimates the distortion value [30]. It is estimated as:

$$SDR = 10 \log_{10} \frac{\sum_{m,n} O(m,n)^2}{\sum_{m,n} (O(m,n) - De(m,n))^2},$$

where $De(m, n)$ and $O(m, n)$ denotes the decrypted and the original image, respectively which is with the dimension of $X \times Y$. It is estimated in decibel and range belongs to the value of $[0, \infty]$. The value of SDR must be minimum for effective the algorithm.

Structural SIMilarity Index (SSIM)

The SSIM exposes the similarity of the decrypted and original image. This value is the quality assessment and estimated by numerous windows of the image having similar size [31]. It is estimated as:

$$SSIM = \frac{(2\mu_I\mu_{De} + CI_1)(2\sigma_{IDe} + CI_2)}{(\mu_I^2 + \mu_{De}^2 + CI_1)(\sigma_I^2 + \sigma_{De}^2 + CI_2)},$$

where μ_I denotes the average of an input (I) and μ_{De} represent the decrypted (De) images. The variance of the I and De are σ_I^2 and σ_{De}^2 , respectively. σ_{IDe} signifies the covariance of the values I and De. CI_1 and CI_2 represent the regularization with the value $(0.01P)^2$ and $(0.01P)^2$, respectively. The value of P is the dynamic range and the SSIM value belongs to the range of $[-1, 1]$.

Root Mean Squared Error (RMSE)

The RMSE value estimates the MSE value that gives accurate and precise data [32]. It is estimated as:

$$RMSE = \sqrt{\frac{\sum_{l=1}^X \sum_{m=1}^Y [O(l, m) - De(l, m)]^2}{XY}},$$

where the coordinate values are represented by l and m with the size of $X \times Y$. The original and decrypted images are denoted as O and De, respectively. The range of RMSE lies between $[0, \infty]$.

Mean Absolute Error (MAE)

The variation among the original and the decrypted image is estimated by the MAE value [33]. It is estimated as:

$$MAE = \frac{1}{XY} \sum_{l=1}^X \sum_{m=1}^Y |O(l, m) - De(l, m)|,$$

where the original image is denoted as $O(l, m)$ and the decrypted image is denoted as $De(l, m)$ with the pixel coordinate and dimension l, m , and $X \times Y$, respectively. The range of MAE is $[0, 2^{num} - 1]$ where num is the count of bits per pixel and the value must be maximum.

Signal to Noise Ratio (SNR)

The efficiency of the algorithm is estimated quantitatively by the SNR value [34]. It is estimated as:

$$SNR = \frac{\sum_{x,y} [O(x, y)]^2}{\sum_{x,y} [O(x, y) - De(x, y)]^2},$$

where $O(x, y)$ denotes the original image and $De(x, y)$ denotes the decrypted image with the pixel coordinates x and y . The SNR range lies between $[0, \infty]$ and the SNR value must be maximum.

Classification of Data Compression Techniques

The transmission of multimedia content over the network is growing and the rate of data growth is higher than the expansion of technology [35, 36]. The huge amount of data generation necessitates the high storage and transmission capability with higher bandwidth. To address these shortcomings in the transmission technology, image compression approaches are introduced. Based on the requirement and the transmission condition, the image compression approaches are developed [37]. The categories of image compression approach are illustrated in Fig. 3.

Image compression approaches minimize the size in bytes of the multimedia content without minimizing the quality of the multimedia file. Image compression decreases the cost of transmission rate and storage capacity. Generally, data irrelevancy and redundancy are eliminated by the image compression approach. The process of image compression is segregated into two categories namely, modeling and coding. At the initial stage, the multimedia content is analyzed for the occurrence of any redundant content in the file and it is retrieved to establish an effective model.

In the subsequent stages, the variation among the newly created model and the original data are considered as a residual data.

The value estimated from the difference acts as coding and it is coded by the encoding approach. There are numerous methods to characterize data and diversified descriptions made the establishment of various compression schemes. The significance of the compression approach is depicted in Table 2.

Assessment of Image Compression Evaluation Metrics

The information theory offers an outline for the plan of a loss-less compression scheme. In the system of information theory, the random variables entropy value is estimated by a term called self-retrieved information [74]. The random experiment results in an event called L that is having the probability $P(L)$ and the relation of self-information is denoted in the below equation,

$$i(L) = -\log_b P(L).$$

For two occurrences of X and Y , the self-retrieved information is associated to L and M is represented as:

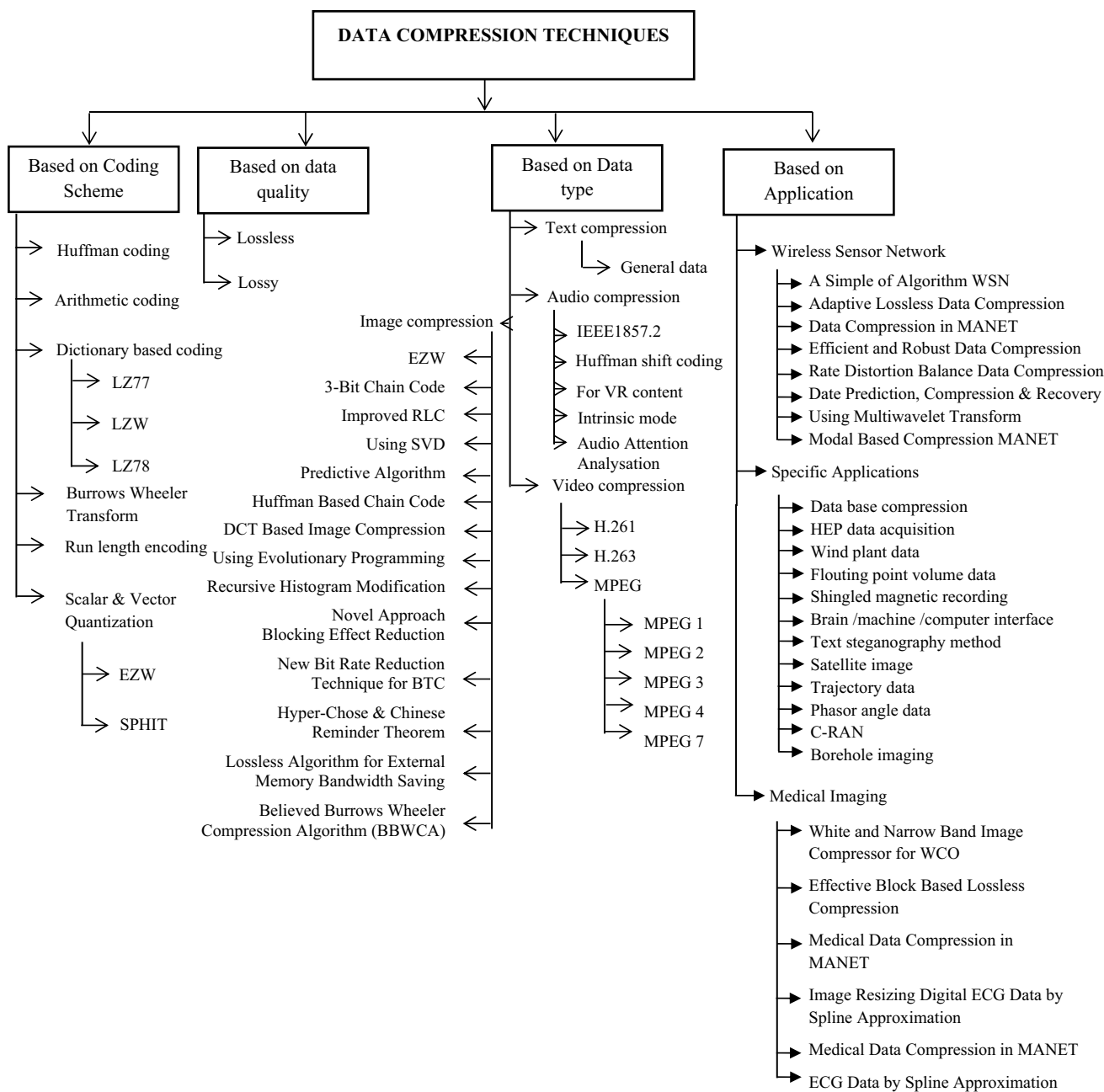


Fig. 3 Categorization of image compression approach

$$i(L) = \log_b \frac{1}{P(LM)}$$

When the values L and M are autonomous nature, $P(LM) = P(L)P(M)$, then the self-retrieved information correlated with L and M is determined by,

$$i(L) = \log_b \frac{1}{P(L)P(Y)} = \log_b \frac{1}{P(L)} + \log_b \frac{1}{P(Y)} = i(L) + i(M).$$

The performance of the compression algorithm is investigated in various aspects. The computational complexity, speed, memory, quality of the restructured data, and compression amount are the diversified aspects of the performance of the algorithm. The general measure to estimate the effectiveness of the algorithm is the compression ratio (C). It is determined as the ratio of the total count of bits needs to store the uncompressed data and compressed data.

Table 2 Image compression approaches and its significant insights

Compression approach	Compression scheme	Inference	Compression type	Applications	Performance metrics	Comparison approach
Coding approach						
	Huffman coding [38]	Entropy based	Lossless	ARG, ZIP, JPEG, PKZIP, MPEG	-	-
	Arithmetic [39]	Entropy based	Lossy and lossless	JPEG, applications having multimedia data	-	-
	LZ coding [40]	Dictionary based	Lossless	GIF, TIFF, PDF, Deflate, Gzip, V.42, ZIP, and PNG	-	-
	Fractal compression [41]	Block-based coding	Lossy	Live video streaming	-	-
	BWT [42]	Block sorting compression	Lossless	Bzip	-	-
	RLE [43]	Incorporated with high redundant data	Lossless	Fax, TIFF, PDF and BMP	-	-
	Scalar and vector quantization [44]	Denotes huge set of value a minimal value	Lossy and lossless	-	-	-
Data type	General data [45]	Logical truth table	Lossless	Wired and wireless networks	CR, CF	-
	Textual data [46]	BWT and Boolean minimization	Lossless	-	CR	LZW, Huffman, BZIP, gzip2
	Textual data [47]	b64 pack	Lossless	-	CR, CT	Compress, gzip, bzip2
	Textual data [48]	Greedy approach	Lossless	Distributed systems	CR	Suffix and prefix closed with dictionary entity
	Textual data [49]	Sent comp	Lossless	Sentimental analysis	-	-
	Textual data [50]	FPHuffman	Lossless	-	CR	Huffman
	Textual data [51]	FPH2 method	Lossless	-	CT, CR	LZ77, LZW, FPH1 and LZSS
	Image [52]	One-bit adaptive quantizer Linear quantization	Lossless	Low bit rate applications	MSE abd bit rate	MBTC, BTC, HVB and HVO
	Image [53]	Decoding process is established by post processing approach	Lossless	-	Quality of the visual and PSNR	CLS, POGS and Crouse method
	Image [54]	3-Bit chain code	Lossless	Bi-level images	CR	Freeman code, ZIP and JBIG
	Image [55]	BWT, reversible color transform (RCT)	Lossless	Color images, EEG data, raster images	HEYC, LZ4X	HEYC, LZ4X
	Image [56]	SVD Huffman coding	Lossless	Secured image Transmission	JPEG	JPEG
	Audio [57]	IEEE1857.2	Lossless	Music audio and speech files	Mp4, wav, ogg, flac	Mp4, wav, ogg, flac
	Audio [58]	Audio attention analysis	Lossless	-	-	-
	Audio [59]	Huffman shift coding	Lossy	Multimedia	-	-
	Audio [60]	LZ compression	Lossy	Audio-video conferencing, VoIF, VoWLAN	DCT, DWT	DCT, DWT

Table 2 (continued)

Application domain	Compression scheme	Inference	Compression type	Applications	Performance metrics	Comparison approach
WSN [61]	WSN [61]	Huffman coding	Lossless	Gathers signals from numerous TPC, calorimeter and detectors	Error and significant factors of compression	Bzip2, S-LZW and gzip
WSN [62]	WSN [62]	Neural networks	Lossy	WSN	CR, RMSE, R ²	PCA, DCT, FFT, CS
Wireless networks [63]	Wireless networks [63]	Magnitude set coding RLE	Lossy	Forensic and remote sensing images	PSNR, visual quality and bpp	AIC, JPEG, and JPEG 2000
WANET [64]	WANET [64]	-	Lossless	GPS	-	-
Medical imaging [65]	Medical imaging [65]	Lossless JPEG based predictor Golomb-rice coding	Lossless	Endoscopic images of NBI and WBI, sequencing videos	PSNR, CR, VIF, VSNR and SSIM	-
Medical imaging [66]	Medical imaging [66]	Hadamard transform and Huffman coding	Lossless	Telemedicine	CR	JPEG2000
Medical imaging [67]	Medical imaging [67]	Modified EZW coding	Lossless	Compression of bio medical signal	CR	-
Medical imaging [68]	Medical imaging [68]	DCT, DWT AND FFT	Lossless	Compression of bio medical signal	PRD, ME, MSE, PSNR, CR	-
Medical imaging [69]	Medical imaging [69]	Subject-adaptive dictionary	Lossless	Compression of bio medical signal	CR, RMSE	-
Application oriented [70]	Application oriented [70]	Association rule mining	Lossless	Database compression	CR	Apriori and TDC
Application oriented [71]	Application oriented [71]	Shannon entropy	Lossless	Compression of wind plant	CR	BZIP2, Deflate, LMZA
Application oriented [72]	Application oriented [72]	APE, ACE	Lossless	Floating-point data of medical and scientific	CR, PSNR	JPEG
Application oriented [73]	Application oriented [73]	LZSS	Lossless	Reduce ITI read latency	CR, SNR, read latency and average read latency	-

$$CR = \frac{\text{count of bits in uncompressed information}}{\text{count of bits in compressed information}}$$

The CR is termed as bpb (bit per bit) and it determines the average counts of the bits need to be store the compressed information. Likewise, bpb is denoted as bits per pixel (bpp), whereas the advanced compression approaches incorporate the bits per character (bpc) that symbolizes the count of bits is necessary to reduce the character. Another estimation approach namely space saving is also incorporated that determine the minimization in the size of a file correlated to the size of the uncompressed and is estimated as follows:

$$\text{Space saving} = 1 - \frac{\text{count of bits in compressed information}}{\text{count of bits in uncompressed information}}$$

By considering the instance having a file size of 21 MB and the compressed file with the size of 3 MB and the space-saving is 0.9 (1–21/3). The value 90% denotes the saved storage space that is saved due to the compression approach. The gain in compression is estimated as,

$$\text{Compression gain} = 100 \log_e \frac{\text{original information}}{\text{compressed information}}$$

The speed of compression is estimated by the cycles per byte (CPB) and the count of the byte requires in compressing the data to one byte. CF and CR values estimate the performance of the lossless compression approach. The evaluation measure to estimate the level of fidelity, distortion, and quality is needed for the reconstructed data when having lossy compression. The difference in the reconstructed and original multimedia content is lossless that is defined as distortion. The general metric used for evaluating the distortion is PSNR and it is a dimensionless number that is expressed by decibel (dB). The original (L_i) and the reconstructed (M_i) are estimated as,

$$PSNR = 20 \log_{10} \frac{\max |L_i|}{RMSE},$$

where RMSE (root mean square error) represents the square root of mean square error (MSE) and it is estimated by:

$$MSE = \frac{1}{no} \sum_{i=1}^{no} (L_i - M_i)^2.$$

When the values of original and the reconstructed images are similar then the value of RMSE is zero and PSNR is infinity. The image with better similarity holds high PSNR value and low RMSE value. The SNR value is used to estimate the error rate in the signal.

$$SNR = 20 \log_{10} \frac{\sqrt{\frac{1}{no} \sum_{i=1}^{no} L_i^2}}{RMSE}.$$

In addition to this, the distortion is determined by the square value of the variation among the input and output signal that is the mean square error. The compression quality metrics cannot assess every kind of signal. To evaluate image compression approaches, the metrics used are PSNR, CR, MS-SSIM, MSE, SSIM, RMSE, MS-SSIM, etc.

Conclusion

Image encryption and compression approaches play a prominent role to handle security concerns and a huge amount of information generated in the digital world. Several compression and encryption approaches are established to process the numerous forms of data such as videos, audios, images, texts, and so on. This paper outlines the various approaches and assessment metrics of image encryption and compression methods. This paper also elaborates significance and various reviews of image encryption and compression algorithms. The developed algorithm's performance is evaluated by the assessment metrics. Based on the variation in the data and the algorithm, evaluation metrics may vary and various metrics have been described.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Tayal N, Bansal R, Gupta S, Dhall S. Analysis of various cryptography techniques: a survey. *Int J Secur Appl.* 2016;10(8):59–92.
2. Ghebleh M, Kanso A, Noura H. An image encryption scheme based on irregularly decimated chaotic maps. *Signal Process Image Commun.* 2014;29(5):618–27.
3. Kumar P, Parmar A. Versatile approaches for medical image compression: a review. *Proc Comput Sci.* 2020;167:1380–9.
4. Pankajavalli PB, Vignesh V, Karthick GS. Implementation of haar cascade classifier for vehicle security system based on face authentication using wireless networks. In: Smys S, Bestak R, Chen JZ, Kotuliak I (editors) *International conference on computer networks and communication technologies. Lecture Notes on Data Engineering and Communications Technologies*, vol 15. Singapore: Springer; 2019. https://doi.org/10.1007/978-981-10-8681-6_58.
5. Li XW, Kim ST. Optical 3D watermark based digital image watermarking for telemedicine. *Opt Lasers Eng.* 2013;51(12):1310–20.
6. Zhang Y, Zhang LY, Zhou J, Liu L, Chen F, He X. A review of compressive sensing in information security field. *IEEE Access.* 2016;4:2507–19.
7. Zhao H, Liu J, Jia J, Zhu N, Xie J, Wang Y. Multiple-image encryption based on position multiplexing of Fresnel phase. *Optics Commun.* 2013;286:85–90.

8. Yu SS, Zhou NR, Gong LH, Nie Z. Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. *Opt Lasers Eng.* 2020;124:105816.
9. Qin Y, Gong Q. Multiple-image encryption in an interference-based scheme by lateral shift multiplexing. *Optics Commun.* 2014;315:220–5.
10. Wang X, Dai C, Chen J. Optical image encryption via reverse engineering of a modified amplitude-phase retrieval-based attack. *Optics Commun.* 2014;328:67–72.
11. Enayatifar R, Abdullah AH, Isnin IF. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt Lasers Eng.* 2014;56:83–93.
12. Wang Q, Guo Q, Lei L, Zhou J. Linear exchanging operation and random phase encoding in gyrator transform domain for double image encryption. *Optik.* 2013;124(24):6707–12.
13. Kadir A, Hamdulla A, Guo WQ. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik.* 2014;125(5):1671–5.
14. Abd El-Latif AA, Niu X. A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU Int J Electron Commun.* 2013;67(2):136–43.
15. Chai X, Gan Z, Yang K, Chen Y, Liu X. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process Image Commun.* 2017;52:6–19.
16. Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *AEU Int J Electron Commun.* 2014;68(3):186–92.
17. Liu H, Wang X, Kadir A. Color image encryption using Choquet fuzzy integral and hyper chaotic system. *Opt Int J Light Electron Opt.* 2013;124(18):3527–33.
18. Khan MA, Ahmad J, Javaid Q, Saqib NA. An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box. *J Mod Opt.* 2017;64(5):531–40.
19. Singh N, Sinha A. Gyrator transform-based optical image encryption, using chaos. *Opt Lasers Eng.* 2009;47(5):539–46.
20. Ozaktas HM, Kutay MA. The fractional Fourier transform. In: 2001 European control conference (ECC), IEEE; 2001. pp. 1477–1483.
21. Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt Lasers Eng.* 2017;88:197–213.
22. Zhao G, Chen G, Fang J, Xu G. Block cipher design: generalized single-use-algorithm based on chaos. *Tsinghua Sci Technol.* 2011;16(2):194–206.
23. Belazi A, El-Latif AAA, Belghith S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* 2016;128:155–70.
24. Abd El-Samie FE, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie ESM, Alshebeili SA. *Image encryption: a communication perspective.* Boca Raton: CRC Press; 2013.
25. Karthick GS, Pankajavalli PB. A review on human healthcare Internet of Things: a technical perspective. *SN Comput. Sci.* 2020;1:198. <https://doi.org/10.1007/s42979-020-00205-z>.
26. Zhang W, Wong KW, Yu H, Zhu ZL. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Commun Nonlinear Sci Numer Simul.* 2013;18(8):2066–80.
27. Li XW, Cho SJ, Kim ST. A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. *Optik.* 2014;125(13):2983–90.
28. Mehra I, Nishchal NK. Optical asymmetric image encryption using gyrator wavelet transform. *Opt Commun.* 2015;354:344–52.
29. Rawat N, Kim B, Kumar R. Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique. *Optik.* 2016;127(4):2282–6.
30. Abbas NA. Image encryption based on independent component analysis and arnold's cat map. *Egypt Inform J.* 2016;17(1):139–46.
31. Cao X, Wei X, Guo R, Wang C. No embedding: a novel image cryptosystem for meaningful encryption. *J Vis Commun Image Represent.* 2017;44:236–49.
32. Zhang Y, Xu B, Zhou N. A novel image compression–encryption hybrid algorithm based on the analysis sparse representation. *Opt Commun.* 2017;392:223–33.
33. Khan M, Shah T. A novel statistical analysis of chaotic S-box in image encryption. *3D Res.* 2014;5(3):16.
34. Ahmad J, Ahmed F. Efficiency analysis and security evaluation of image encryption schemes. *Computing.* 2010;23:25.
35. Smith CA. A survey of various data compression techniques. *Int J pf Recent Technol Eng.* 2010;2(1):1–20.
36. Hosseini M. A survey of data compression algorithms and their applications. *Network Systems Laboratory, School of Computing Science, Simon Fraser University, BC, Canada;* 2012.
37. Reddy MP, Reddy BVR, Bindu CS. Lossy image compression using exponential growth equation and encryption by natural exponential function. *J Image Process Pattern Recognit Prog.* 2018;4(3):46–55.
38. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH. Image steganography in spatial domain: a survey. *Signal Process Image Commun.* 2018;65:46–66.
39. Huffman DA. A method for the construction of minimum-redundancy codes. *Proc IRE.* 1952;40(9):1098–101.
40. Langdon GG. An introduction to arithmetic coding. *IBM J Res Dev.* 1984;28(2):135–49.
41. Ziv J, Lempel A. A universal algorithm for sequential data compression. *IEEE Trans Inf Theory.* 1977;23(3):337–43.
42. Saupe D, Hamzaoui R. A review of the fractal image compression literature. *ACM SIGGRAPH Comput Graph.* 1994;28(4):268–76.
43. Arnavat Z, Magliveras SS. Block sorting and compression. In: *Proceedings DCC '97, Data Compression Conference, Snowbird, UT, USA.* 1997. p. 181–90. <https://doi.org/10.1109/DCC.1997.582009>.
44. Capon J. A probabilistic model for run-length coding of pictures. *IRE Trans Inf Theory.* 1959;5(4):157–63.
45. Schmid M, Steinlein C, Bogart JP, Feichtinger W, Haaf T, Nanda I, et al. The hemiphractid frogs. *Phylogeny, embryology, life history, and cytogenetics.* *Cytogenet Genome Res.* 2012;138(2–4):69–83.
46. Mahmud S. An improved data compression method for general data. *Int J Sci Eng Res.* 2012;3(3):2.
47. Platoš J, Snášel V, El-Qawasmeh E. Compression of small text files. *Adv Eng Inform.* 2008;22(3):410–7.
48. Kalajdzic K, Ali SH, Patel A. Rapid lossless compression of short text messages. *Comput Stand Interfaces.* 2015;37:53–9.
49. De Agostino S. The greedy approach to dictionary-based static text compression on a distributed system. *J Discrete Algorithms.* 2015;34:54–61.
50. Che W, Zhao Y, Guo H, Su Z, Liu T. Sentence compression for aspect-based sentiment analysis. *IEEE ACM Trans Audio Speech Lang Process.* 2015;23(12):2111–24.
51. Oswald C, Ghosh AI, Sivaselvan B. Knowledge engineering perspective of text compression. In: *2015 Annual IEEE India conference (INDICON), IEEE;* 2015. pp. 1–6.
52. Oswald C, Sivaselvan B. An optimal text compression algorithm based on frequent pattern mining. *J Ambient Intell Humaniz Comput.* 2018;9(3):803–22.
53. Rao YR, Eswaran C. New bit rate reduction techniques for block truncation coding. *IEEE Trans Commun.* 1996;44(10):1247–50.

54. Sanchez-Cruz H, Rodriguez-Dagnino RM. Compressing bilevel images by means of a three-bit chain code. *Opt Eng.* 2005;44(9):097004.
55. Khan A, Khan A, Khan M, Uzair M. Lossless image compression: application of Bi-level Burrows Wheeler Compression Algorithm (BBWCA) to 2-D data. *Multimed Tools Appl.* 2017;76(10):12391–416.
56. Kumar M, Vaish A. An efficient encryption-then-compression technique for encrypted images using SVD. *Digit Signal Process.* 2017;60:81–9.
57. Huang H, Shu H, Yu R. Lossless audio compression in the new IEEE Standard for Advanced Audio Coding. In: 2014 IEEE international conference on acoustics, speech and signal processing (ICASSP), Florence. 2014. p. 6934–8. <https://doi.org/10.1109/ICASSP.2014.6854944>.
58. Hang B, Wang Y, Kang C. A scalable variable bit rate audio codec based on audio attention analysis. *Revista Técnica de la Facultad de Ingeniería.* 2016;39(6):114–20.
59. Brettel J, Skoglund J. Open-source spatial audio compression for vr content. In: SMPTE 2016 annual technical conference and exhibition, SMPTE; 2016. pp. 1–9.
60. Kosmidou VE, Hadjileontiadis LJ. Sign language recognition using intrinsic-mode sample entropy on sEMG and accelerometer data. *IEEE Trans Biomed Eng.* 2009;56(12):2879–90.
61. Marcelloni F, Vecchio M. A simple algorithm for data compression in wireless sensor networks. *IEEE Commun Lett.* 2008;12(6):411–3.
62. Alsheikh MA, Lin S, Niyato D, Tan HP. Rate-distortion balanced data compression for wireless sensor networks. *IEEE Sens J.* 2016;16(12):5072–83.
63. Rajakumar K, Arivoli T. Lossy image compression using multi-wavelet transform for wireless transmission. *Wirel Pers Commun.* 2016;87(2):315–33.
64. Drinic M, Kirovski D, Potkonjak M. Model-based compression in wireless ad hoc networks. In: Proceedings of the 1st international conference on embedded networked sensor systems; 2003. pp. 231–242.
65. Khan TH, Wahid KA. White and narrow band image compressor based on a new color space for capsule endoscopy. *Signal Process Image Commun.* 2014;29(3):345–60.
66. Venugopal D, Mohan S, Raja S. An efficient block based lossless compression of medical images. *Optik.* 2016;127(2):754–8.
67. Nielsen M, Kamavuako EN, Andersen MM, Lucas MF, Farina D. Optimal wavelets for biomedical signal compression. *Med Biol Eng Comput.* 2006;44(7):561–8.
68. Unnikrishnan S, Surve S, Bhoir D. Advances in computing, communication and control. In: Conference proceedings ICAC3; 2011. p. 109.
69. Vadori V, Grisan E, Rossi M. Biomedical signal compression with time-and subject-adaptive dictionary for wearable devices. In: 2016 IEEE 26th international workshop on machine learning for signal processing (MLSP), IEEE; 2016. pp. 1–6.
70. Lee CF, Changchien SW, Wang WT, Shen JJ. A data mining approach to database compression. *Inf Syst Front.* 2006;8(3):147–61.
71. Louie H, Miguel A. Lossless compression of wind plant data. *IEEE Trans Sustain Energy.* 2012;3(3):598–606.
72. Fout N, Ma KL. An adaptive prediction-based approach to lossless compression of floating-point volume data. *IEEE Trans Vis Comput Graph.* 2012;18(12):2295–304.
73. Venkataraman KS, Dong G, Xie N, Zhang T. Reducing read latency of shingled magnetic recording with severe intertrack interference using transparent lossless data compression. *IEEE Trans Magn.* 2013;49(8):4761–7.
74. Shannon CE. A symbolic analysis of relay and switching circuits. *Electr Eng.* 1938;57(12):713–23.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.