*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 409–420
DOI : 10.47974/JDMSC-1897

# A scheme for encrypted image data compression

Nileshsingh V. Thakur *
*Department of Computer Technology*
*Yeshwantrao Chavan College of Engineering*
*Nagpur*
*Maharashtra*
*India*

Kalyani Deshmukh †
*Department of Computer Science and Engineering*
*Prof. Ram Meghe Institute of Technology and Research*
*Badnera*
*Maharashtra*
*India*

Saurabh A. Shah §
*Department of Computer Science and Engineering*
*Prof Ram Meghe College of Engineering and Management*
*Badnera*
*Maharashtra*
*India*

Vijay Bhaskar Semwal ‡
*Department of Computer Science and Engineering*
*Maulana Azad National Institute of Technology*
*Bhopal*
*Madhya Pradesh*
*India*

* *E-mail :* thakurnisvis@rediffmail.com (Corresponding Author)
† *E-mail :* Kalyani.deshmukh19@gmail.com
§ *E-mail :* shahsaurabh.15@gmail.com
‡ *E-mail :* vsemwal@manit.ac.in

**Abstract**

A hybrid approach of image encryption and compression can give highly secured and compressed image data which can be easily transmitted through unsecured and bandwidth constrained channels. This paper proposes a mechanism which handles image encryption prior to image compression. The work is basically divided into two parts. The first part focuses on image encryption approach in which Roman numeral logic and pixel scrambling logic is applied to image data. The second part focuses on compression of encrypted image data using Huffman's encoding. The proposed approach is lightweight, easy to understand and implement. Results are obtained using standard dataset and it is observed that 16%-18% compression is obtained after encryption.

***Subject Classification:*** *Primary 93A08, Secondary 68P25.*

***Keywords:*** *Image processing, Image encryption, Image compression, Roman numerals.*

## 1. Introduction

Image compression and encryption are, in general, the known techniques which are used in transmission of image data and to provide the security to the image. These two techniques can be used independently. Also, the hybrid approach is also possible where the image compression can be used prior to image encryption and the vice-versa. Main issue concerned with the encryption is that it increases the size of data and hence the issue of transmission. Also, the computational burden of such type of approaches is more. In literature, independent encryption approaches are related to S-box based [1, 9], block-based scrambling [11], embedding algorithm [14], key substitution [17], medical image encryption [22], lossless compression based [23], and chaotic map based [24]. Independent image compression approaches are sparse-representation based image compression [4], low-bit rate [5], lossy image compression [7, 10], progressive coding [12], 360° image compression [13], and remote sensing image compression [18]. Compression and then encryption involves scanning based [2], sparse representation and chaotic confusion [6], discrete cosine transform and hyperchaotic system based [8], compressive sensing related work [15, 21]. Encryption and then compression involves block based [3], encryption involves SHA-256 [16], lossy compression [19], and deep learning [20]. This paper presents an approach which involves the encryption as first part and compression as second part. This presented hybrid approach addresses the issue of computational burden, security and the image quality. Proposed approach

uses the Roman numerals logic and scrambling for encryption and lossless Huffman encoding for compression.

This paper is organized as follows. In section 2, we formulate the identified problem. Section 3 discusses proposed approach. Section 4 provides experimental setup and results. Finally, in section 5 we draw conclusions and consider future work.

## 2. Problem Formulation

It is observed that if, let $A(x,y)$ is original image and $A'(x,y)$ is an encrypted image obtained from $A(x,y)$, then the relationship between both the images related to data size is represented by $A(x,y) \leq A'(x,y)$. If we apply compression on encrypted image $A'(x,y)$ to get compressed image let $A_c(x,y)$ then relationship between both the images related to data size is represented by $A_c(x,y) \leq A'(x,y)$. But, it is not necessary that the compressed image data size is always less than the original image data size. It is possible to reduce the size of image encrypted data without compromising image quality which can increase the compression ratio of encrypted image. Consider an image say '$X_{org}$' which need to be transmitted through unsecured and bandwidth constrained channel. To achieve this, it is necessary to apply some encryption and compression methodology. Encryption is divided into two phases, say E1 and E2. In E1, Roman numeral mechanism is applied to get a new encrypted Roman image, say '$X_{roman}$'. Keep aside a matrix of image size containing length of all roman numerals of original image. Let '$M_{len}$' is the length matrix. Length matrix will act as a key at the time of retrieving original from encrypted image. In E2, apply scrambling mechanism to get new scrambled image, say '$X_{scr}$'. Here, length '$M_{len}$' and scrambled image '$X_{scr}$' are the encrypted data for compression. '$X_{scr}$' and '$M_{len}$' is compressed using Huffman's encoding (HE). Let '$X_{scr\_comp}$' is compressed image of '$X_{scr}$' and '$M_{len\_comp}$' is compressed matrix of '$M_{len}$'. Block schematic of logic of encryption and compression is given in Figure 1. At receiver's end, reverse processing can be applied to retrieve original image. '$X_{scr\_comp}$' and '$M_{len\_comp}$' can be uncompressed using

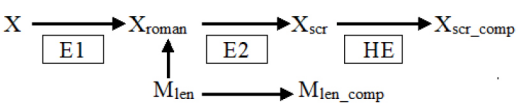


**Figure 1**

**Problem Formulation**

Huffman's decoding to get '$X_{scr}$' and '$M_{len}$', respectively. We can retrieve '$X_{roman}$' by applying unscrambling logic to '$X_{scr\_comp}$' image and using '$M_{len}$' original image can be retrieved easily.

## 3. Proposed Approach

Compressing an encrypted data is always beneficial in image data transmission through unsecured and bandwidth constrained channel because encryption always leads in increasing size of original image. Proposed approach deals with a system-based compression of encrypted data. Proposed approach is a novel encryption technique which is based on the use of Roman numeral with a pixel scrambling mechanism. Most of the encryption algorithm increases the size of image data, but use of Roman numeral leads in little bit reduction in size of image data. Use of pixel scrambling mechanism provides more security to our already encrypted image. For compression, Huffman encoding is used on encrypted data which is the lossless encryption technique. This approach is basically divided into four main parts, namely- image encryption using Roman numeral and pixel scrambling mechanism, image compression using Huffman encoding, image decompression using Huffman decoding. Block schematic for encryption and compression is given in Figure 2. Block schematic for decompression and decryption is given in Figure 3.

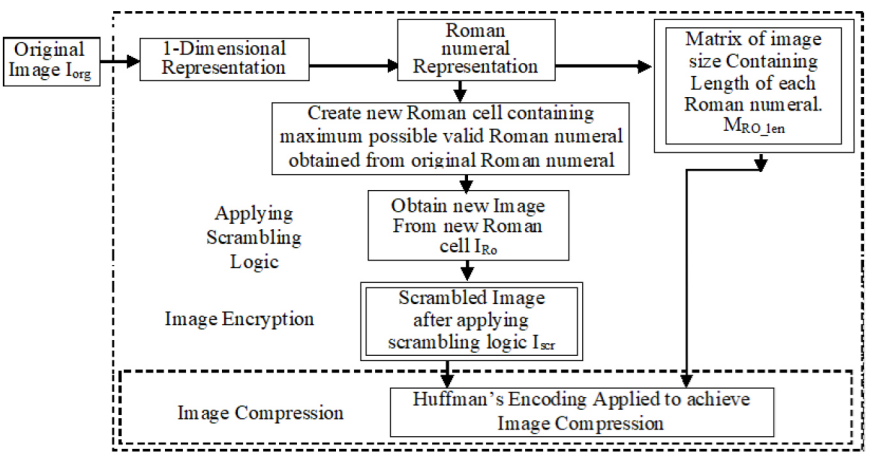


**Figure 2**

**Block Schematic for Encryption and Compression**

Complete procedure for image encryption and compression is as follows:

Step 1 : Start

Step 2 : Input an image say '*I*' and convert it into 1-Dimentional array.

Step 3 : Convert 1-Dimentional array into its equivalent Roman numeral representation and save length of each Roman numeral into image size matrix say $M_{RO\_len}$.

Step 4 : Create a single Roman numeral string. Trace it from left to right to get maximum possible valid Roman numeral and save it.

Step 5: Create new array obtained from new Roman numeral and convert it into new image say '$I_{RO}$'.

Step 6 : Apply pixel scrambling Logic on image '$I_{RO}$' to get new image say '$I_{scr}$'.

Step 7 : Apply Huffman encoding on both $M_{RO\_len}$ and $I_{scr}$.

Step 8 : Stop.

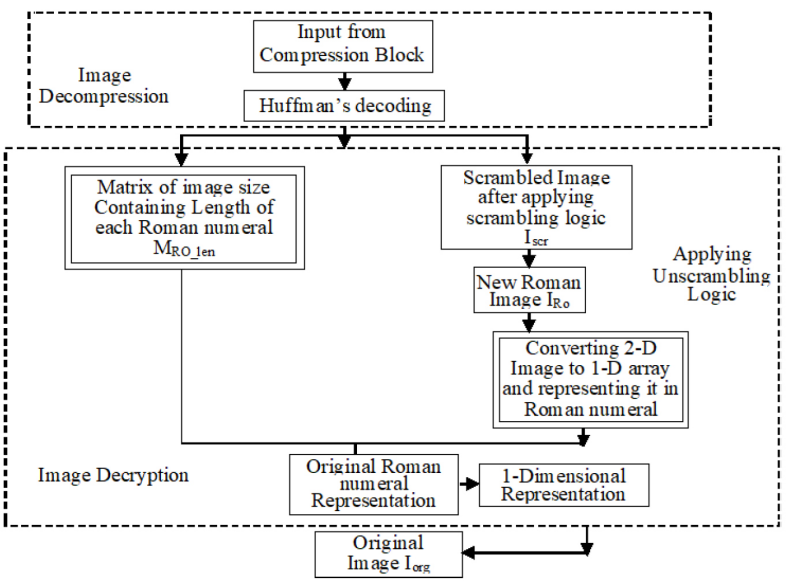


**Figure 3**

**Block Schematic for Decryption and Decompression**

Procedure for image decryption and decompression is as follows:

Step 1 : Start

Step 2 : Input Huffman encoded data and apply Huffman decoding to get '$M_{RO\_len}$' matrix and '$I_{scr}$' scrambled image.

Step 3 : Apply unscrambling mechanism on '$I_{scr}$' image to get new Roman converted image '$I_{RO}$'.

Step 4 : Converting 2-D image '$I_{RO}$' to 1-Dimenssional array and representing it in Roman numeral.

Step 5: Convert '$I_{RO}$' into a string and obtain original image Roman representation using length matrix '$M_{RO\_len}$'.

Step 6 : Convert Roman numeral into decimal number and obtain original image.

Step 7: Stop.

To transmit image data through an unsecured channel leads in stealing image data. Hence, encryption technique(s) should be applied on image data for its protection. Encryption part of proposed approach is divided into two sub-parts.

Use of Roman Numerals: Roman numerals are nothing but the collection of 7 characters i.e. 'I', 'V', 'X', 'L', 'C', 'D' and 'M' with decimal values 1, 5, 10, 50, 100, 500, and 1000, respectively. Pixel values of image are always represented in between 0-255. We can convert those pixel values into its equivalent roman numeral to get a roman string. Logic applied is shown in Figure 4 as follows.

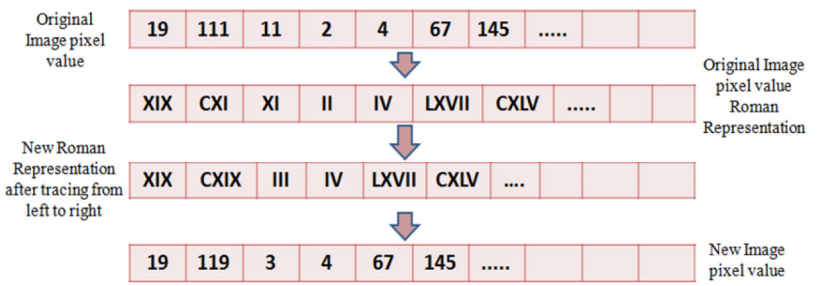


**Figure 4**

**Roman Logic of Encryption**

Firstly, convert an image into 1-Dimentional array. The array is then converted into its equivalent Roman numeral representation. Next, converting it into Roman string and tracing it from the starting point in forward direction to obtain the maximum possible valid combination,

accordingly, we can get new Roman numerals. Converting back new Roman numerals into its decimal equivalent gives new decimal array. According to Figure 4, the number of pixels in original image are more than that of obtained new image, hence, the obtained new image is padded with some dummy pixel having value 255, *i.e.*, using white color from further processing point of view. New obtained image is then forwarded to next encryption phase which is discussed in further section.

Pixel scrambling of image: Pixels are scrambled by creating a random generated index matrix having index values of same as that of image size. Each of the matrix rows contains unique number from *1* to *n*, where *n* is size of image. To form index matrix, pixel positions of first element of each of rows are recorded. Size of index matrix is always equal to size of new Roman numeral image. Using index matrix pixel of Roman numeral image are shuffled.

Huffman encoding is applied on a matrix containing length of Roman numeral of original image and a scrambled image obtained from encryption block. At receiver's end, Huffman decoding is applied to retrieve compressed data. Huffman encoding is a lossless compression technique, so, transmitted Matrix '$M_{RO\_len}$' and scrambled image '$I_{scr}$' is retrieved perfectly.

After decompression, matrix '$M_{RO\_len}$' and scrambled image '$I_{scr}$' are used to retrieve original image. Again, decryption is divided into two sub-parts. Apply unscrambling logic on '$I_{scr}$' to get Roman image and then obtaining original roman numeral values with the help of Matrix '$M_{RO\_len}$'. Original pixel intensity values are retrieved after getting original Roman numeral series.

## 4. Experimental Setup and Results

Cameraman, Baboon, Lena, Pirate, Aeroplane and Splash images are used in experiments. A small block of size 16×16 is selected from Cameraman image to show actual 2-Dimentional representation. After converting it into 2-Dimentional matrix, Roman numeral conversion logic is applied to get series of equivalent Roman numerals. Roman numeral representation of a small block from Cameraman image is shown in Figure 5. All the Roman numeral values are shown in the Figure 5 are stored into a cell array and then concatenated to get a series of Roman symbols only. This string is then used as input to Roman tracing logic. After getting Roman representation, next step is to trace all Roman numeral from left to right to get maximum possible Roman numeral value. New Roman

numeral resultant image obtained is shown in the Figure 6. As discussed previously, number of pixels in original image is more than that of encrypted image, hence for further processing extra pixels are added to the image with intensity value 255. A white patch seen in Figure 6 is of padded pixels with intensity value 255. Next step is to apply scrambling to an encrypted image in first phase of encryption. Scrambling is applied on the Roman numeral image and resultant scrambled image is shown in Figure 6.

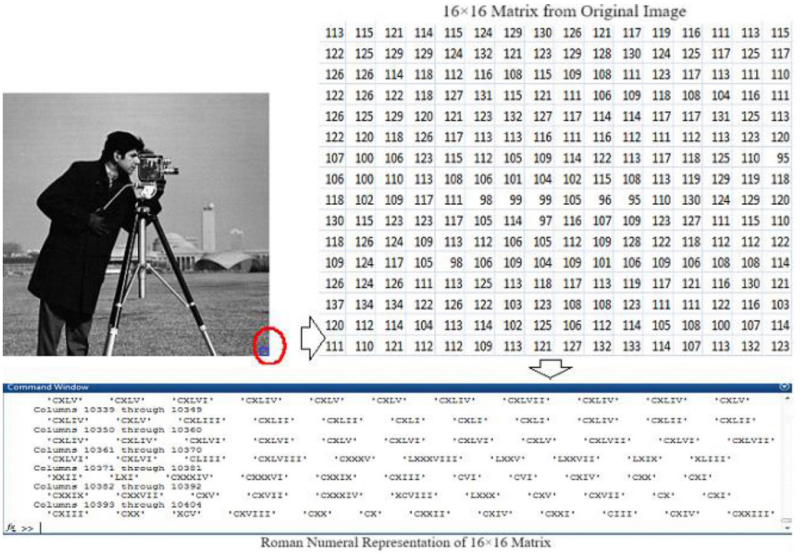


**Figure 5**

**Roman Numeral Representation of cameraman.tif Image**

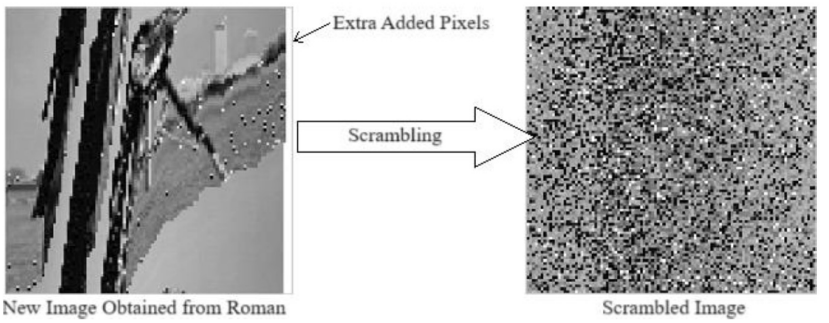


**Figure 6**

**New Image Obtained from Roman and Its Scrambling**

Figure 7 shows the obtained results for standard images where the columns 'a' and 'd' represents the original images, columns 'b' and 'e' shows the results of encryption in first phase of encryption, and columns 'c' and 'f' shows the results of encryption in second phase. Huffman encoding compression technique is applied on obtained scrambled image and Roman length matrices. Compression ratio (CR) is evaluated to analyze the compression evaluation. Table 1 summarizes the obtained results for encryption and compression for Encrypted Data Size (EDS) in bits, Compressed Data Size (CDS) in bits,

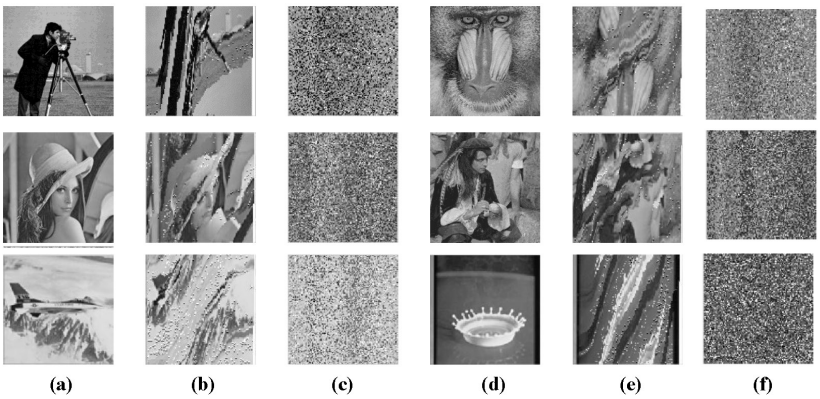


**Figure 7**

**Results of Encryption on Cameraman, Baboon, Lena, Pirate, Aeroplane and Splash**

**Table 1**

**Performance Evaluation Parameter of different images**

| Image Name | Resolution | EDS | CDS | CR |
|---|---|---|---|---|
| Cameraman | 102×102 | 124848 | 102612 | 0.8219 |
| Baboon | 102×102 | 124848 | 102357 | 0.8198 |
| Lena | 102×102 | 124848 | 104632 | 0.8380 |
| Pirate | 102×102 | 124848 | 103758 | 0.8310 |
| Aeroplane | 102×102 | 124848 | 97376 | 0.7800 |
| Splash | 102×102 | 124848 | 104115 | 0.8339 |

## 5. Conclusion and Future Scope

After rigorous experimentation on standard dataset images, the results obtained are motivating and are towards positive direction. From experimentations, it is seen that compression ratio from all the images lies between 16-18 percent except Aeroplane. Mean Squared Error (MSE) values for original images and recovered images are zero. It proves that there is no image data loss occurred during processing. The methodology described in this paper is easy to understand and less complex. Time required for image decryption and decompression is less than that of time required for image encryption and compression. There is always a scope for improvement in any kind of experimentation. There is a scope for reduction in encryption time. The approach can be iteratively applied on color images by separating their RGB planes. There is a tremendous scope in encryption logic as ultimately processing is applied on Roman string. Pseudo Roman representations can be used to increase encryption efficiency.

## References

[1] Z. A. Abduljabbar et al., "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," *IEEE Access*, vol. 10, pp. 26257-26270, (2022).

[2] P. Chaudhary, R. Gupta, A. Singh, P. Majumder, A. Pandey, Joint image compression and encryption using a novel column-wise scanning and optimization algorithm, *Procedia Computer Science*, Volume 167, 2020, Pages 244-253, (2020).

[3] Sandeep Kumar Sharma, Anil Kumar, and Uday Pratap Singh. Enhanced Edges Detection from Different Color Space. In Proceedings of the 4th International Conference on Information Management & Machine Intelligence (ICIMMI '22). Association for Computing Machinery, New York, NY, USA, Article 16, 1–6 (2023). https://doi.org/10.1145/3590837.3590853.

[4] L. Dai, L. Zhang and H. Li, "Image Compression Using Stochastic-AFD Based Multisignal Sparse Representation," *IEEE Transactions on Image Processing*, vol. 31, pp. 5317-5331, (2022).

[5] F. Gao, X. Deng, J. Jing, X. Zou and M. Xu, "Extremely Low Bit-rate Image Compression via Invertible Image Generation," *IEEE Transactions on Circuits and Systems for Video Technology*, (2023).

[6] Ghaffari, A. Image compression-encryption method based on two-dimensional sparse recovery and chaotic system. *Sci Rep* 11, 369, (2021).

[7] Y. Hu, W. Yang, Z. Ma and J. Liu, "Learning End-to-End Lossy Image Compression: A Benchmark," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 8, pp. 4194-4211, (2022).

[8] Huang, H., Cheng, D. A secure image compression-encryption algorithm using DCT and hyperchaotic system. *Multimed Tools Appl* 81, 31329–31347 (2022).

[9] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," *IEEE Access*, vol. 9, pp. 120596-120612, (2021).

[10] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography,* 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[11] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," *IEEE Access*, vol. 9, pp. 37855-37865, (2021).

[12] S. Li, H. Li, W. Dai, C. Li, J. Zou and H. Xiong, "Learned Progressive Image Compression With Dead-Zone Quantizers," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 6, pp. 2962-2978, (2023).

[13] M. Li, J. Li, S. Gu, F. Wu and D. Zhang, "End-to-End Optimized 360° Image Compression," *IEEE Transactions on Image Processing*, vol. 31, pp. 6267-6281, (2022).

[14] P. Liu, X. Wang and Y. Su, "Image Encryption via Complementary Embedding Algorithm and New Spatiotemporal Chaotic System," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 5, pp. 2506-2519, (2023).

[15] Sharma, S.K., Kumar, A. Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.

[16] K. N. Singh, O. P. Singh, A. K. Singh, ECiS: Encryption prior to compression for digital image security with reduced memory, *Computer Communications*, Volume 193, Pages 410-417, (2022).

[17] Y. Song, Z. Zhu, W. Zhang, H. Yu and Y. Zhao, "Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture," *IEEE Access*, vol. 7, pp. 84386-84400, (2019).

[18] G. Sumbul, J. Xiang and B. Demir, "Towards Simultaneous Image Compression and Indexing for Scalable Content-Based Retrieval in Remote Sensing," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 60, pp. 1-12, Art no. 5630912, (2022).

[19] C. Wang, T. Zhang, H. Chen, Q. Huang, J. Ni and X. Zhang, "A Novel Encryption-Then-Lossy-Compression Scheme of Color Images Using Customized Residual Dense Spatial Network," *IEEE Transactions on Multimedia*, vol. 25, pp. 4026-4040, (2023).

[20] C. Wang, J. Hu, S. Bian, J. Ni and X. Zhang, "A Customized Deep Network Based Encryption-Then-Lossy-Compression Scheme of Color Images Achieving Arbitrary Compression Ratios," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 8, pp. 4322-4336, (2023).

[21] Wei, J.; Zhang, M.; Tong, X. Multi-Image Compression–Encryption Algorithm Based on Compressed Sensing and Optical Encryption. *Entropy*, *24*, 784, (2022).

[22] Y. Wu, L. Zhang, S. Berretti and S. Wan, "Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 2089-2098, (2023).

[23] Y. Yang, M. Cheng, Y. Ding and W. Zhang, "A Visually Meaningful Image Encryption Scheme Based on Lossless Compression SPIHT Coding," *IEEE Transactions on Services Computing*, vol. 16, no. 4, pp. 2387-2401, (2023).

[24] Zhang, Y.; Dong, W.; Zhang, J.; Ding, Q. An Image Encryption Transmission Scheme Based on a Polynomial Chaotic Map. *Entropy*, *25*, 1005, (2023).