STUDY ON MACHINE LEARNING AND CRYPTOGRAPHIC METHODS FOR IMAGE COMPRESSION AND SECURED TRANSMISSION

V.Prabavathi, Research scholar, Department of Computer Science, Nallamuthu Gounder Mahalingam College,Pollachi. Mail id: prabavathi@ngmc.org
Dr.M.SAKTHI, Associate Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi. Mail id: sakthi.cs.phd1@gmail.com

ABSTRACT

Image processing converts the image into digital form and performed operations on image to attain the helpful information. With fast development of images, security and memory space consumption for transmission and storage is a critical issue. Compression and Encryption are employed to protect the input images from an unauthorized access. Image compression is carried out in graphic file to minimize their size without affecting the image quality. The input images are compressed before transmission because they occupy large storage space. Many image encryption and compression methods are discussed for performing efficient image transmission. But, the confidentiality rate was not improved and compression time was not minimized by existing techniques. Therefore, machine learning and deep neural learning based on compression and cryptographic techniques are discussed to enhance the performance of image encryption and compression system.

Keywords: Image Processing, Compression, Encryption, Unauthorized access, Machine learning, Deep learning

1. INTRODUCTION

Image processing is used to process the images with help of mathematical operations. An image is considered as an input and output is the group of characteristics related to the image. Image processing handled the images with two dimensional signals through signal processing techniques. Image processing increased raw image quality received from cameras placed on satellites for different applications. An image is sent from different sources through internet. The images comprised the confidential information protected from leakage during secure transmission. Different methods were introduced for protecting the images from leakage. The secured image transmission is carried out through performing image encryption and data hiding.

This paper is arranged as: Section 2 reviews the drawbacks on existing secured data transmission methods. Section 3 shows the study of secured transmission methods. Section 4 performs possible comparison between them. Section 5 explains the limitations of secured transmission techniques. The paper conclusion is given in the section 6.

2. LITERATURE REVIEW

Fully Connected Neural Network (FCNN) architecture was introduced in [1] to perform efficient prediction. A dynamical FCNN model comprised the learning process with image substances for adaptive learning. However, the computational complexity was not minimized by FCNN architecture.

A spectral-spatial transform termed extended Star-Tetrix transforms (XSTTs) was introduced in [2] for edge-aware XSTTs (EXSTTs) without extra bits and complexity. Star-Tetrix transform (STT) was new spectral-spatial transform based spectral-spatial transform. But, the computational cost was not minimized by XSTTs.

A new secret sharing scheme was introduced in [3] with Chinese remainder theorem for polynomial ring. The designed scheme employed the polynomials to divide the secret image. RESIS scheme attained the secret and cover image for lossless restoration. But, the compression ratio was not improved by designed scheme.

A Robust Reversible Watermarking scheme in Encrypted Image with Secure Multi-party (RRWEI-SM) was designed in [4] depending on lightweight cryptography. The robust reversible watermarking was carried out depending on Prediction Error Expansion (PEE) through Secure Multi-party Computation (SMC). But, computational complexity was not minimized by RRWEI-SM.

A region-based hybrid Medical Image Watermarking (MIW) scheme was introduced in [5] to improve image authenticity transmitted through public network. RoI was watermarked with adaptive Least Significant Bit (LSB) substitution for tamper detection and recovery. Though the confidentiality level was improved, the computational complexity was not minimized by MIW scheme.

A modular and composable compression framework termed SZ3 was introduced in [6] with four-folds. A SZ3 framework was introduced with the modular abstraction for prediction. A compression pipeline used SZ3 with GAMESS data for increasing the compression ratio. Though the compression ratio was improved, complexity level was not minimized by SZ3.

RDHEI scheme was introduced in [7] for performing the pixel prediction and bit-plane compression with correlation analysis. An original image was partitioned into equal size blocks. An additional data was inserted in the vacated room through multi-LSB substitution. But, compression time consumption was not minimized by RDHEI scheme.

A novel compression method was designed in [8] with bi-level region of interest (ROI) maps. The designed scheme attained high compression ratio through dividing image into smaller blocks. The optimization algorithm identified best combination of direction for non-zero blocks. However, the compression ratio was not improved by designed method.

An autoencoder-based compression prototype was employed in [9] to diminish the floating point data. An implementation was carried out to achieve high compression ratio and sufficient error bounds. Though the compression ratio was improved, the space complexity was not minimized by designed prototype.

A self-tuning tensor compression framework called CSwap+ was introduced in [10] for enhancing the virtual memory management. The designed framework employed compression with minimum compression ratio at minimal runtime. But, the compression time was not minimized by designed framework.

3. SECURED IMAGE COMPRESSION AND TRANSMISSION

Security is the main issue concerned with protecting the digital images that are transmitted over network. The digital images on network are protected from different types of attacks. Cryptography is used to convert the original message into cipher message. Cryptographic methods are used for attaining high security goals like confidentiality and integrity. Image compression is an important concept in image processing. Image compression is used to reduce the storage size of an image without reducing the image. The file size minimization increased the storage capacity.

3.1 Dynamic Neural Network for Lossy-to-Lossless Image Coding

A 2D non-separable lifting scheme comprised prediction steps to learn the prediction filters using FCNN. The designed network was employed to perform the update stage. The update optimization problem was reformulated as a prediction problem. Fully Connected Neural Network (FCNN) architecture was introduced to perform the prediction and updating. FCNN-based Lifting Scheme (LS) was carried to perform encoding of an input image. A dynamical FCNN model was introduced for learning process with an input image contents. FCNN-based Lifting Scheme was resorted using an iterative algorithm where variable computation was carried out in an alternating way. The second learning method identified the model parameters directly through a reformulation of loss function. FCNN model was trained through minimizing the loss function. The learned weights were kept fixed after training and generate the wavelet representation of any image in the test set. The designed method was employed to design adaptive FCNN model depending on input image with acceptable complexity.

3.2 Edge-Aware Extended Star-Tetrix Transforms for CFA-Sampled Raw Camera Image Compression

The codec using spectral-spatial transform compressed the raw camera images gathered with color filter array through varying RGB color space into decorrelated color space. The spectral-spatial transform termed extended Star-Tetrix transforms (XSTTs) and edge-aware versions termed edge-aware XSTTs (EXSTTs) was introduced without extra bits and complexity. An extended StarTetrix transform (STT) was spectral-spatial transform with wavelet based spectral-spatial transform. The designed transform considered 2-D wavelet transform with two 1-D diagonal transforms. The designed transform employed weighting along edge directions in images. XSTTs/EXSTTs improved lossless and lossy compression without minimizing the compression efficiency for images.

3.3 A reversible extended secret image sharing scheme based on Chinese remainder theorem

The secret image was partitioned into 'n' shadow images in secret image sharing (SIS) scheme. The shadow images recovered the secret image. An extended SIS (ESIS) embedded shadow images into cover image. ESIS was secure as shadow images were noise-like images that arouse suspicion of attackers. The stego images were meaningful images. When secret image and cover image was recovered from stego images in ESIS scheme, the reversible ESIS (RESIS) was introduced. A new secret sharing scheme used Chinese remainder theorem for polynomial ring. RESIS employed polynomials to divide the secret image. Least significant bit substitution technology hides the shadow images and generated the stego images. RESIS scheme guaranteed the secret and cover image for lossless reconstruction. The shadow images obtained satisfactory quality results not affected by different cover images.

3.4 Robust Reversible Watermarking in Encrypted Image with Secure Multi-Party Based on Lightweight Cryptography

The reversible watermarking increased their robustness to avoid the attacks during digital media transmission. The reversible watermarking scheme functioned in encrypted form for privacy preserving of cover image. The robustness of watermarking and the privacy preserving of cover image was the essential factors of reversible watermarking. The robust reversible watermarking in encrypted area resists attacks like JPEG compression and noise addition simultaneously. An embedding capacity of robust watermark and efficiency of encryption method was taken. Multi-party watermarking was essential one for the network media to protect party rights. A Robust Reversible Watermarking scheme in Encrypted Image with Secure Multi-party (RRWEI-SM) was designed with lightweight cryptography. An additive secret sharing and block-level scrambling were used to generate the encrypted image. The robust reversible watermarking was performed with Prediction Error Expansion (PEE) through Secure Multi-party Computation (SMC). A Modified RRWEI-SM was introduced with two-stage architecture for increasing the robustness. RRWEI-SM scheme and Modified RRWEI-SM scheme was used for multiparty protection. RRWEI-SM and Modified RRWEI-SM were secure, robust and efficient.

3.5 SZ3: A Modular Framework for Composing Prediction-Based Error-Bounded Lossy Compressors

A modular, composable compression framework termed SZ3 was introduced with four-folds. SZ3 employed features with an innovative modular abstraction for prediction-based compression framework. The compression module was employed to design compressors depending on data features and user needs. A new compression pipeline was carried out for GAMESS data to increase the compression ratio. An adaptive compression pipeline was carried out for APS data with lesser efforts. SZ3 resulted in best rate distortion among error-bound lossy compressors for any bit-rate. The pipelines combined several compression pipelines from multiple disciplines. SZ3 obtained limited overhead in compressor integration and customized compression pipelines resulted improvement in compression ratios under data distortion.

3.6 Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT

A region-based hybrid Medical Image Watermarking (MIW) scheme was designed to guarantee the authenticity of medical images in IoMT. The medical images were divided into Region of Interest (RoI) and Region of Non-Interest (RoNI). Tamper detection and recovery bits were inserted in medical image to improve the integrity of RoI. RoI was watermarked by adaptive Least Significant Bit (LSB) substitution with hiding capacity map for higher RoI accuracy in tamper detection and recovery. Electronic Patient Record (EPR) was compressed through Huffman coding and encrypted with pseudo random key to attain higher confidentiality. Encrypted EPR and RoI recovery bits were interrupted in RoNI through Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD). The designed scheme was tested under geometric and non-geometric attacks like filtering, compression, rotation, salt and pepper noise and shearing. The designed scheme attained high imperceptibility, robustness, security, payload, tamper detection and recovery accuracy under image processing attacks. The designed scheme was employed used in transmission of medical images in IoMT.

4. PERFORMANCE COMPARISON OF IMAGE COMPRESSION AND SECURED TRANSMISSION TECHNIQUES

Experimental evaluation of existing image compression and secured data transmission techniques are implemented in MATLAB Software. During experimental consideration, the number of images is considered as an input. Result analysis are carried out with existing methods using three different parameters are,

- Data Confidentiality Rate,
- Compression Ratio and
- Compression Time

4.1 Analysis on Confidentiality Rate

Confidentiality rate is described as the ratio of number of images that are protected to the entire number of images sent. It is computed in terms of percentage (%). It is determined as,

$$CR = \frac{Number\ of\ images\ protected}{Number\ of\ images\ sent} * 100 \qquad (1)$$

From (1), 'CR' represent the confidentiality rate. When the confidentiality rate is higher, the method is said to be more efficient. Table 1 describes the confidentiality rate comparison for six different conventional techniques.

Table 1 Tabulation for Confidentiality Rate

Number of Images (Number)	Confidentiality Rate (%)					
	FCNN architecture	Spectral-spatial transform	SIS scheme	RRWEI-SM	SZ3 framework	Region-based hybrid MIW scheme
10	89	78	85	71	68	85
20	91	80	88	73	70	87
30	93	82	90	75	73	89
40	95	85	92	77	76	91
50	92	83	91	74	73	89
60	90	81	88	72	71	87
70	88	78	85	70	69	85
80	91	82	87	73	72	88
90	93	84	89	75	74	90
100	95	86	91	78	76	92

Table 1 explains the confidentiality rate with respect to number of images ranging from 10 to 100. Confidentiality rate comparison takes place on the existing FCNN architecture, Spectral-spatial transform , SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme. Let us consider that number of images as 60, the confidentiality rate of FCNN architecture , Spectral-spatial transform , SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme is 90%, 81%, 88%, 72%, 71% and 87% respectively. The graphical representation of confidentiality rate is illustrated in the figure 1.

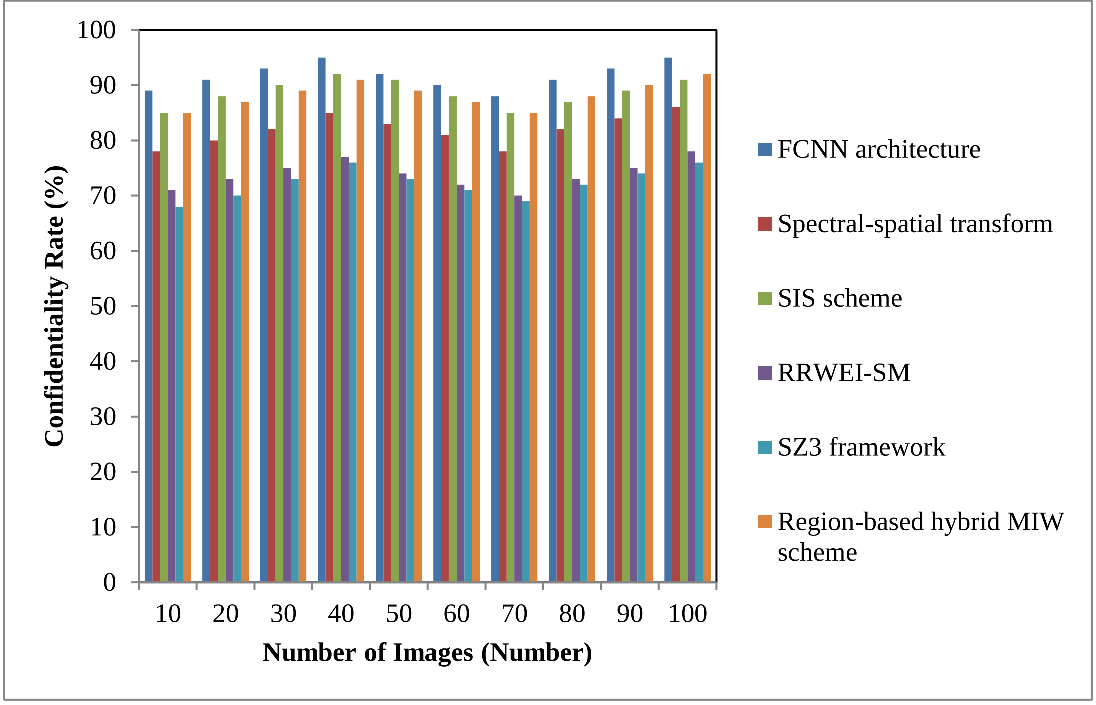

Figure 1 Measurement of Confidentiality Rate

Figure 1 explains the confidentiality rate for different number of images. Confidentiality rate using FCNN architecture is higher than conventional methods. Let us consider that number of images as 60, the confidentiality rate of FCNN architecture is comparatively higher than Spectral-spatial transform, SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme. This is because of using FCNN-based Lifting Scheme with an iterative algorithm. The second learning method identified the model parameters directly through reformulation of loss function. As a result, confidentiality rate of FCNN architecture is increased by12%, 4%, 24%, 27% and 4% when compared to Spectral-spatial transform, SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme respectively.

4.2 Analysis on Compression Ratio

Compression Ratio is the ratio of uncompressed data size to the compressed data size. The compression ratio is computed as,

$$Compression\ ratio = \frac{Uncompressed\ data\ size}{Compressed\ data\ size} \qquad (2)$$

From (2), compression ratio of different data size is obtained. When the compression ratio is higher, the technique is said to be more efficient.

Table 2 Tabulation for Compression Ratio

Image Size (KB)	Compression Ratio					
	FCNN architecture	Spectral-spatial transform	SIS scheme	RRWEI-SM	SZ3 framework	Region-based hybrid MIW scheme
10	11	18	6	9	15	13
20	13	20	8	12	17	16

30	15	23	11	14	19	18
40	17	25	13	16	21	20
50	20	28	15	18	24	22
60	23	30	18	21	27	25
70	26	32	20	24	29	27
80	29	34	23	26	32	28
90	32	37	25	28	34	30
100	35	40	28	31	37	33

Table 2 explains the compression ratio with respect to number of images ranging from 10 to 100. Compression ratio comparison takes place on existing FCNN architecture, Spectral-spatial transform , SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme. Let us consider that image size 20 KB, the compression ratio of FCNN architecture, Spectral-spatial transform, SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme is 13, 20, 8, 12, 17 and 16 correspondingly. The graphical representation of compression ratio is shown in the figure 2.

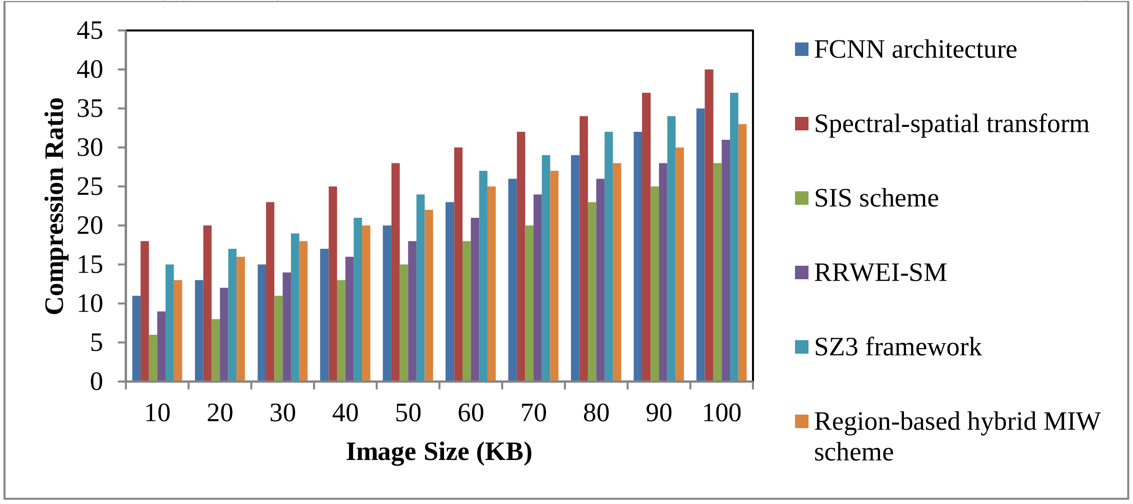

Figure 2 Measurement of Compression Ratio

Figure 2 depicts the compression ratio for different image size. In the above figure, the comparative analysis of compression ratio is shown in different colors. Compression ratio using Spectral-spatial transform is higher than other existing methods. This is due to the application of 2-D wavelet transform with two 1-D diagonal or horizontal-vertical transforms. The designed transform used transform weighting along edge directions in input images. As a result, compression ratio of Spectral-spatial transform is increased by36%, 90%, 51%, 14% and 25% when compared to FCNN architecture, SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme respectively.

4.3 Analysis on Compression Time

Compression Time is defined as the product of number of image and amount of time consumed to compress one image. The compression time is formulated as,

$$Compression\ time = N * time\ consumed\ to\ compress\ one\ image \qquad (3)$$

From (3), compression time of different number of images is obtained. When the compression time is higher, the method is said to be more efficient.

Table 2 Tabulation for Compression Time

Number of Images (Number)	**Compression Time (ms)**					
	FCNN architecture	**Spectral-spatial transform**	**SIS scheme**	**RRWEI-SM**	**SZ3 framework**	**Region-based hybrid MIW scheme**
10	25	18	15	10	22	29

20	27	20	17	12	24	31
30	29	23	19	15	27	33
40	32	25	22	18	30	35
50	34	27	24	20	32	38
60	36	29	26	22	34	40
70	39	31	28	25	37	42
80	42	33	30	28	40	45
90	45	35	32	30	42	47
100	48	38	34	33	44	49

Table 3 describes the compression time with respect to number of images varying from 10 to 100. Compression time comparison takes place on existing FCNN architecture, Spectral-spatial transform , SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme. Let us consider that number of images is 80, the compression time of FCNN architecture, Spectral-spatial transform, SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme is 42ms, 33ms, 30ms, 28ms, 40ms and 45ms correspondingly. The graphical representation of compression time is shown in the figure 3.

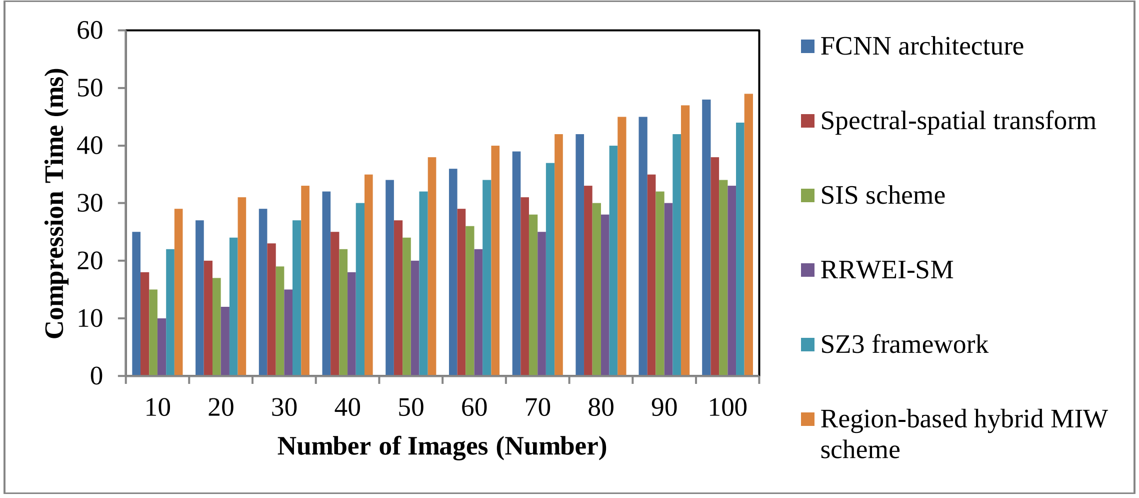

Figure 3 Measurement of Compression Time

Figure 3 shows the compression time for different number of images. In figure 3, the compression time for different methods is illustrated in six different colors. Compression time using RRWEI-SM is lesser than other conventional techniques. This is because of secret sharing and block-level scrambling for generating the encrypted image. The robust reversible watermarking was carried out with significant bit Prediction Error Expansion (PEE). A Modified RRWEI-SM with two-stage architecture improved the robustness. As a result, compression time of RRWEI-SM is reduced by42%, 26%, 16%, 38% and 47% when compared to FCNN architecture, Spectral-spatial transform SIS scheme, RRWEI-SM, SZ3 framework and Region-based hybrid MIW scheme respectively.

5. DISCUSSION AND LIMITATIONS OF IMAGE COMPRESSION AND SECURED TRANSMISSION TECHNIQUES

A novel secret sharing scheme used Chinese remainder theorem for polynomial ring to divide the secret image. Least significant bit substitution technologies hide the shadow images. RESIS scheme guaranteed secret and cover image for lossless reconstruction. However, the compression ratio was not increased by designed scheme. FCNN architecture was used to perform prediction. FCNN model used an iterative algorithm with variable computation. But, the computational complexity was not decreased by FCNN architecture.

Codecs using spectral-spatial transform compressed the images captured with color filter array through varying the RGB color space into decorrelated color space. The spectral-spatial transform used 2-D prediction step and weight the transforms along edge directions. However, the computational cost was not minimized by designed transform. RRWEI-SM was designed depending on lightweight cryptography. Though RRWEI-SM attained higher robustness, computational complexity was not minimized by RRWEI-SM.

SZ3 framework was employed with the features and compression modules were plugged to form compressors depending on data characteristics and user requirements. Though the compression ratio was improved, complexity level was not minimized by SZ3. The region-based hybrid Medical Image Watermarking (MIW) scheme was used to guarantee the authenticity, integrity, and confidentiality of medical images sent through network in IoMT. The medical images were divided into Region of Interest (RoI) and Region of Non-Interest (RoNI). Tamper detection and recovery bits were embedded in RoI for increasing the integrity of RoI. But, the computational complexity was not minimized by MIW scheme.

5.1 Future Direction

The future direction of the work is to perform efficient image compression and secured transmission with higher confidentiality rate and lesser compression time by machine learning and deep learning techniques.

6. CONCLUSION

A comparison of different image compression and secured transmission techniques are studied. From the study, it is observed that the confidentiality rate was not improved. Though the compression ratio was improved, complexity level was not reduced by SZ3. In addition, the compression ratio was not enhanced by designed scheme. The wide range of experiment on existing methods determines the performance of image compression and secured transmission methods with its limitations. Finally, the research work can be carried out using machine learning and cryptographic techniques for improving the image compression and secured transmission performance with higher confidentiality rate and lesser compression time.

ACKNOWLEGDMENT

I convey my sincere thanks to the management of Nallamuthu Gounder Mahalingam College, Pollachi, for allowing me to carry out this research work by funding the SEED MONEY. I extend my sincere thanks to the Principal, Deans, HOD and Manager of Nallamuthu Gounder Mahalingam College, Pollachi for providing the necessary facilities to carry out the presence work.

REFERENCES

[1] Tassnim Dardouri, Mounir Kaaniche, Amel Benazza-Benyahia, and Jean-Christophe Pesquet, “Dynamic Neural Network for Lossy-to-Lossless Image Coding”, IEEE Transactions on Image Processing, Volume 31, September 2022, Pages 569 – 584

[2] Taizo Suzuki and Liping Huang, “Edge-Aware Extended Star-Tetrix Transforms for CFA-Sampled Raw Camera Image Compression”, IEEE Transactions on Image Processing, Volume 31, September 2022, Pages 6072 - 6082

[3] Keju Meng, Fuyou Miao, Yan Xiong and Chin-Chen Chang, “A reversible extended secret image sharing scheme based on Chinese remainder theorem”, Signal Processing: Image Communication, Elsevier, Volume 95, July 2021, Pages 1-15

[4] Lizhi Xiong, Xiao Han, Ching-Nung Yang and Yun-Qing Shi, “Robust Reversible Watermarking in Encrypted Image with Secure Multi-party based on Lightweight Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology, Volume 32, Issue 1, January 2022, Pages 75 – 91

[5] Priyanka Singh, K. Jyothsna Devi, Hiren Kumar Thakkar, and Ketan Kotecha "Region-Based Hybrid Medical Image Watermarking Scheme for Robust and Secured Transmission in IoMT", IEEE Access, Volume 10, January 2022, Pages 8974 – 8993

[6] Xin Liang; Kai Zhao; Sheng Di; Sihuan Li; Robert Underwood; Ali M. Gok, Jiannan Tian, Junjing Deng, Jon C. Calhoun, Dingwen Tao, Zizhong Chen and Franck Cappello, "SZ3: A Modular Framework for Composing Prediction-Based Error-Bounded Lossy Compressors", IEEE Transactions on Big Data, Volume 9, Issue 2, 01 April 2023, Pages 485 – 498

[7] Zhaoxia Yin, Yinyin Peng and Youzhi Xiang, "Reversible Data Hiding in Encrypted Images Based on Pixel Prediction and Bit-Plane Compression", IEEE Transactions on Dependable and Secure Computing, Volume 19, Issue 2, 01 March-April 2022, Pages 992 – 1002

[8] Reetu Hooda and W. David Pan, "Lossless Compression of Bilevel ROI Maps of Hyperspectral Images using Optimization Algorithms", IEEE Geoscience and Remote Sensing Letters, Volume 19, January 2021, Pages 1-15

[9] Tong Liu, Jinzhen Wang, Qing Liu, Shakeel Alibhai, Tao Lu and Xubin He, "High-Ratio Lossy Compression: Exploring the Autoencoder to Compress Scientific Data", IEEE Transactions on Big Data, Volume 9, Issue 1, 01 February 2023, Pages 22 - 36

[10] Ping Chen, Shuibing He, Xuechen Zhang, Shuaiben Chen, Peiyi Hong, Yanlong Yin and Xian-He Sun, "Accelerating Tensor Swapping in GPUs With Self-Tuning Compression", IEEE Transactions on Parallel and Distributed Systems, Volume 33, Issue 12, 01 December 2022, Pages 4484 – 4498