International Engineering Journal For Research & Development
Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

AN OVERVIEW AND APPROACH FOR HYBRID IMAGE ENCRYPTION AND COMPRESSION

Prof. Kalyani H. Deshmukh
Department of Computer Science and Engineering
Prof Ram Meghe Institute of Tech and Research
Badnera-Amravati, India
kalyani.deshmukh19@gmail.com

Prof. Pratik S. Deshmukh
Department of Computer Science and Engineering
Prof Ram Meghe Institute of Tech and Research
Badnera-Amravati, India
psdeshmukh150@gmail.com

Abstract-

In an image processing, for proving security to an image many encryption techniques are available. But most of the Encryption techniques mask some amount of data to the source image that always increases the size of image. Encryption makes it difficult to transmit an image through bandwidth constrained channel. To overcome this problem, Image Compression can be applied on the Encrypted image to reduce its size. This paper presents the analysis and overview of some prominent approaches which are relevant to the image encryption and compression. It also discusses an approach to perform joint encryption and compression on image. The scope of implementation for the derived idea exists. Some analytical analysis is also presented from the proposed approach implementation point of view.

Keywords—image compression; image encryption; auxiliary image data; Huffman encoding

INTRODUCTION

In image processing, use of Image Compression and Encryption leads in transmitting an image securely and in compressed form through unsecured and low bandwidth channel. In image processing, for proving security to an image many encryption techniques are available. But most of the Encryption techniques mask some amount of data to the source image that always increases the size of image. Encryption makes it difficult to transmit an image through bandwidth constrain channel. To overcome this problem Image Compression can be applied on the Encrypted image to reduce its size. But traditional compression algorithms underperform for many of the image encryption techniques. Applying the Hybrid approach increases the computational complexity. This paper discusses about some methodologies which are used for performing image Encryption, Image Compression and Joint Encryption Compression. This literature review is basically classified into four categories. There are some papers which focuses on image Compression techniques. Some have Image Encryption techniques. Some related works are carried out using joint approach in which Encryption that can be done prior to Compression or vice versa.

MOTIVATION

In Joint Image Encryption and Compression approach, it is observed that after applying Encryption the image data size increases because of some data masking. It makes it difficult to transmit the data though low bandwidth channel. For this a Compression can be applied on the image data. Or the techniques can be reversely applied i.e. compression first and the Encryption on image data,

Again after applying both the techniques it is not necessary that we always get same quality of image at the time of retrieving it. At receivers end, data can be lost while retrieving the original image. These aspects motivate us to study different Image Compression, Image Encryption and Hybrid Image Compression Encryption Techniques.

LITERATURE REVIEW

This literature review is basically classified into four categories. There are some papers which focuses on image Compression techniques. Some have Image Encryption techniques. Some related works are carried out using joint approach in which Encryption that can be done prior to Compression or vice versa.

Image Data Encryption prior to Compression

This section discuses some related work based on joint Image Encryption and Compression approach.

Zhang et al. (2014) [1] gives a method in which compression is applied on encrypted image using supportive information. It is used here for retrieving original image from encrypted image. Quantization of encrypted data is obtained by supportive data parameters. At receivers end it is necessary to transmit the encrypted image, quantized data, parameters and supportive data. Decryption can be done using compressed encrypted data and a secret key at receivers end. Here a ratio-distortion criterion for selecting the quantization parameter by channel provider is used. In this method unnecessary use of iterative reconstruction procedure is avoided. While comparing with other schemes, here compression performance ratio is considerable with respect to its computational complexity. Johnson et al. (2004) [2] described that, transmitting information over an insecure and narrow bandwidth channel leads leaking of data. An encryption and compression can applied on data by keeping encryption key hide from compressor. Compressing encrypted data approach is used for identification of the connection between the stated problem and distributed source coding. As the key will be available at decryption end, compression can be applied on encrypted data using distributed source coding principles. There is wide scope in the domain of cryptography for the system described here. A pseudo random key generation can be used here to increase its complexity.

In some multimedia contents there is a need of processing encrypted signals directly to get desired output which requires both signal processing and cryptography research. Erkin et al. (2007) [3] discussed a encrypted signal processing scheme which tells about cryptographic primitives used in existing solutions to processing of encrypted signals and its security needed. For both analyzing multimedia contents analysis and retrieving and security domains state-of-the-art algorithms are described. Authors also discussed about challenges and issues regarding secure signal processing. Jakimoski and Subbalakshmi (2007) [4] have described a scheme of image encryption and lossless image compression for gray scale and color images. As an alternative process of directly applying encryption on the images, here applies encryption algorithm on prediction errors and for cipher text compression distributed source coding is used. Here advancement on the compression gains of RGB color images are occurred by applying the correlation among the planes. Final conclusion for discussed system is that, it is always advantageous to use encryption on the prediction errors instead of using encryption directly on the image in terms of both lossless compression and computational cost. In lossless encrypted image compression, at decoder side for retrieving original image from an encrypted image at it is necessary to provide side information with the encrypted image. Lazzeretti and Barni (2008) [5] have applied encryption and compression mechanisms on grey-level and color images using decompression of images into bit-planes. In this work authors have given few techniques for compression of encrypted images. According to their theoretical results best result is obtained by transformation of color image into YCbCr format. Here as to spatial de-correlation, working on the prediction error gives good results, whereas the xor-based algorithm causes the system tends towards lossy compression. By keeping acceptable quality of reconstructed image there is a need of removing the lower encrypted bit-planes to decrease the bit rate. Even if to state-of-the-art compression in the plain domain is wide, obtained results are considerable. Kumar and Makur (2008) [6] described a scheme of image encryption and lossless image compression for gray scale and color images. As an alternative process of directly applying encryption on the images, here applies encryption algorithm on prediction errors and for cipher text compression distributed source coding is used. By analyzing proposed system compression ratio varies from 1.5 to 2.5 even though encryption is applied on the images. The compression gains of RGB color images are occurred by applying the correlation among the planes are considerable. Final conclusion is that, it is always advantageous to use encryption on the prediction errors instead of using encryption directly on the image in terms of both lossless compression and computational cost. According Liu et al. (2010) [7], a distributed source coding technique can used for compressing encrypted image without using data to be compression before to encryption to reduce the size. In this system, both security and compression efficiency is considered for getting desired output. Here stream-cipher based encryption is applied on an image before compression. Resolution-progressive compression (RPC) technique is used for an efficient compression of encrypted image. The technique is used for both inter-frame and intra-frame correlation. Slepian-Wolf Coding is used for achieving lossless compression of encrypted sources. MPEG-4 technology is used for compressing audio and visual data transmission.

In the mentioned work, Schonberg et al. (2008) [8] described a skeleton for compressing encrypted media like image and video. Considering distributed source coding, it is possible to compress encrypted data. But for compression there are two main challenges i.e. first is model development that accepts primary skeleton and compatible with proposed framework and second is that because of encoding, the compressors doesn't recognize what rate to focus on. For overcoming both challenges before handling video, authors have developed statistical models for images and compared their results with -of-the-art motion-compensated lossless video encoder which requires unencrypted video as input. In the work authors have

developed a protocol for general compression. They have demonstrated total implementation for encrypted video. Klinc et al. (2009) [9] gives a system that deals with compression of encrypted data using block-cipher, like Advanced Encryption Standard. The data can be feasibly compressed by applying Slepian–Wolf coding without knowing secret key. Here a concept of chaining modes is used with block cipher establishes a simple symbol-wise connection between consecutive blocks of information. The proposed compression technique is used for protection of encryption scheme. Authors have also shown the limitations of block cipher when no chaining mode is applied. The results for proposed work are still away from theoretical limits. For the future extension of work an improved performance is expected with further enhancement in block size. Kumar and Makur (2009) [11] discussed about difficulties occurred in lossy compression technique for encrypted image data. The approach is based on compressive sensing methodology. A joint decoding/decryption with some enhanced pursuit decoding approach for encryption is described here. The basic pursuit algorithm is modified for enabling joint decompression and decryption. Here the compression results are demonstrated using simulation results. In this paper, basic pursuit as decoding algorithm and DCT basics are considered at the time of simulation. The obtained result can be enhanced using some time efficient greedy algorithms along with some basics of compressive sensing.

X. Zhang (2011) [12] discussed a methodology for compressing an encrypted image using lossy compression and iterative reconstruction. First step for practical scheme is encryption of original image using pseudo random permutation. Next step is compression by discarding rough and important data of coefficient in transformed domain. After having compressed and permuted data, an iterative updating procedure is used for retrieving the coefficient values by using spatial correlation in original image. It reconstructs original image. With different values of compression parameters, compression ratio and the quality of reconstructed image differ. In the system only pixel positions are shuffled not masked with other values. Here security is weaker than that of standard stream cipher. There is wide area of improvement as security is concerned. Zhang et al. (2012) [13] discussed about a scheme of scalable coding for encrypted images. In encryption pixel values of original image are masked by modulo-256 addition with pseudorandom numbers which are generated from a secret key. The encrypted data is then decomposed into down sampled sub-image and several data sets with a multiple-resolution construction. To reduce data amount, an encoder quantizes sub-image coefficients of each data set. The data of quantized sub-image and coefficients are considered as a set of bit streams. At receivers end, quantized coefficients are used to reconstruct the original image. Zhou et al. (2014) [15] suggested a highly efficient image encryption and then compression mechanism applicable for both lossless and lossy compression. The mechanism operates on the basis of the prediction error domain which is responsible for providing high level security while transmitting the image via unsecure channel. There is also demonstration of an arithmetic coding based approach which can be used for efficient compression of encrypted images. The compression scheme is a little worse in terms of compression efficiently as compare with the state-of-the-art lossless/lossy image coder because it takes unencrypted images as input. Slepian-Wolf coding is generally used for achieving Lossless compression of encrypted sources. For images, to improve compression efficiency we have to consider source dependency. According to Liu et al. (2010) [17] Slepian-Wolf decoder's Markov properties does not work for grayscale images. In the proposed approach, authors have applied stream-cipher based encryption algorithm prior to compression. According to their experiments, the result of coding efficiency and less computational complexity are considerable. This can be calculated using resolution progressive compression (RPC). The work can implement on encrypted videos, in which RCP can be applied on inter-frame and intra-frame correlation at decoder side.

A stream cipher encryption algorithm in standard format is applied on image prior to compression. According to Zhou et al. (2014) [18], the base layer bit stream is produced when they code a series of non overlapping patches of uniformly down-sampled version of the encrypted image. A learning approach which is off-line in nature can be used to model the error that occurs from original images patch pixel sample. It is based on local complexity and the length of the compressed bit stream relationship. The model leads to adaptively selecting pixels greedy strategy which is coded in enhancement layer. At decoder end, a multi scale and iterative technique is for reconstruction of image using all pixel samples. According to authors the system performs well for state-of the- arts for both performance and visual quality of output image at both low and medium region rate. Here Kang et al. (2013) [19] discussed a scheme of lossy compression using pixel-value encrypted images which can be either smooth or texture-rich images. At the receivers end, bit plane information is used as auxiliary information for image reconstruction. Total bit planes transmitted is directly proportional to the quality of reconstructed image. The system performs is considerable while comparing with some existing system based on lossy compression method on pixel value encrypted image. It also achieves same performance as that of state-of-the-art lossy compression applies on pixel permutation-based encrypted images. The system have some advantages like, there is no need of having computationally intensive iteration and additional l public orthogonal matrix. The Xinpeng Zhang (2011) [20] discussed an approach of the lossy compression on encrypted image with variable compression ratio. For encrypting an image pseudorandom permutation technique is used. At

encryption phase a mechanism of pixel position shuffling is applied on image without using any masking values. Using elastic pixel values, compressed data can be produced with the help of generated coefficients. The approach lags in security because of weaker encryption technique. The flexible pixel values can be used to retrieve original data. An approach described by Yuen and Wong (2011) [21] used discrete cosine transformation (DCT) and Secure Hash Algorithm-1 (SHA-1) for Chaos-based joint image compression and encryption algorithm. SHA-1 Algorithm is used for enhancing diffusion effect on image pixels. There are two DCT coefficients one is the sequence of low-frequency coefficients with secret keys that generates a message to take in other sequence composed of high-frequency coefficients. Here Huffman coding is used for compressing encrypted chains of pixel data. The approach is an efficient and high sensitive algorithm for both key stream and the plain-image. Jridi and Alfalou (2010) [22] discussed about fully pipelined single chip architecture suitable for concurrent image compression and encryption methodologies real-time application. Here uses DCT properties for both compression and encryption on image. For compression, 8-point DCT is applied on images and then some applied multiplex on some special points of DCT outputs. For encryption, a random number is added to DCT coefficients. In the approach, attention is given on DCT Algorithm. The simulation result gives high compression ratio. Bourbakis (1997) [23] discussed a fractals efficient image compression-encryption method. The method is based on principle of family of fractal based languages (Scan) used for compressing and encrypting images. It is a context free language that processes nxn 2 dimensional array data sequentially by shot set of simple algorithms from wide range of algorithms. For compression Scan method accesses 2 dimension images using arithmetic operation. Region searching coding criterion is used for compression of both color and gray-level image. Both lossy and lossless compression can be achieved using Scan method. Encryption of image is directly obtained from the Scan method. The work can be extended by performing scanning at grayscale level of pixels rather than that of bit plane level.

Image Compression prior to Encryption

For Compression prior to Encryption maximum work is done on the basis of quardtree decomposition compression [24, 26, 27] mechanism and Slepian-Wolf distributed compression mechanism [14].

Grant et al. (2011) [14] derived a rate region for a secure distributed source coding problem. For lossless approach it is always best to design encryption and compression separately. In the scheme Slepian-Wolf distributed compression and one- time pad for encryption is used for transmitting image data securely with minimal transmission rate. With differs many multiuser settings, the use of the separation of compression and encryption is best for this particular case. After having constructively demonstrated that switching the order of compression and encryption does not gain any performance loss. Xiaobo et al. (1997) [24] discussed a scheme of image coding in mobile wireless environment. Here authors have used two image compression methodologies quardtree decomposition method for image in the spatial domain and MSPIHT approach used for wavelet transform of image decompose in transmission domain which is the modified version if SPIHT algorithm. Here lattice quantization is used. A partial encryption technique is used here that takes benefit of tree structure. Cheng and Xiaobo (2000) [26] discussed a methodology based on partial encryption mechanism for image and video. Here two compression mechanisms are discussed. One is quardtree compression algorithm for which 13 to 27 % image is encrypted and set partitioning in hierarchical trees (SPIHT) algorithm for which only 2% image is encrypted. Use of partial encryption reduces encryption and decryption time and does not affect the compression performance. Reaz et al. (2005) [27] discusses experimentation based on Altera FLEX10K FPGA device for partial encryption of compressed image. Here according to for image compression, lossless linear quardtree compression algorithm and for Encryption RSA Encryption algorithm is used. Encryption is applied on critical areas of image so that processing speed of the system is get increased.

Image Compression

Candes and Wakin (2008) [10] gives a novel scheme for compressive sampling is discussed which is known as compressed sampling or CS. In data acquisition compressed sampling goes against conventional approaches to sampling signals or images. In compressed sampling authors claim that recovery of certain signals and images can be done from very less samples or measurements is possible than that of traditional methodology used for sampling. For making this possible, compressed sampling basically relies on two principles. First is sparsity which relates signals of concern and second is incoherence which relates to sensing modality. Reichel et al. (2001) [16] discussed a work based on lossy to lossless image compression with the difference between the integer (IWT) and infinite precision (DWT). Here a degradation of quality caused by the use of IWT model is presented, which is based on the theory that says nonlinear rounding operation can be substituted by an additive white noise. In this method an equivalent transfer functions were computed to find the impact of various noise sources on the reconstructed pixel. The model uses white noise for verifying the proposed theory and uses compression system and natural images to check validity of the theory in real time application domain. Use of MES gives significant differences in both IWT and DWT approaches. IWT shows larger degradation result than that of DWT in small quantization steps. It concludes that for both a MSE and a visual quality point of view two

transforms are equivalent for large compression ratios. Wang and Zheng (2013) [28] introduces a new approach of Fractal image compression (FIC), in which local similar blocks are used for compression. The resemblance between two blocks of image is equal to total Pearson's correlation coefficient (APCC) value of the blocks. In this method, first all the blocks are classified to increase probability of its correspondence using APCC-based block classification method. Then sorting APCCs method is applied on all the domain blocks and predefined block in each class, and then searching mechanism is applied for searching matching block in each domain with preset block by APCC. Authors claim that the proposed system not only reduces encryption time but also maintains quality of image.

Chan et al. (2008) [29] discussed about new lossless image compression using pixel-wise palette reordering. It is used for reshaping index map of a color-indexed image's properties. In this approach index map of an image is converted into a new index map which contain record of pixel dependency palette. New index map shows incredibly less zero-order entropy and energy. Here authors have used matching coding mechanism for encoding the resultant index map. Author claims that, in teams of compression the proposed method shows more efficient results than that of other state-of-art lossless compression algorithms for color-indexed image. Thakur and Kakde (2007) [30] discusses an architecture which is based on Pseudo Spiral Architecture applied on one-plane image. For encoding purpose modified Fractal grey level image coding algorithm (MFCSA) is used on the architecture. This approach optimizes domain block using local search. Modified Fractal grey level image coding compression technique is based on block-based processing technique. Authors claim that there is reduction in number of plane of color image from three to one. It is always beneficial to use Pseudo Spiral Architecture instead of traditional Architecture for processing of image as one dimensional structure data.

Image Encryption

Xie et al. (2008) [25] discussed a Cryptosystems is based on NLM nonlinear mixing model with a strong noise for encryption and NMF (Nonnegative matrix factorization) for decryption. Cryptosystem security is based on some factors such as non invertible multivariable nonlinear function and NMF unilateral process. In this Cryptosystem authors have used multi time padding. There is no limitation for processing signals because of no limit on statistical characters of text. Authors have given considerable simulation results for security in their Cryptosystem. Li et al. (2008) [31] described a scheme based on Cryptanalysis of an Image Scrambling without Bandwidth Expansion using two-dimensional discrete prolate spheroidal sequences. The applied image scrambling is affected by attacks like ciphertext- only attack, known plaintext attack, chosen-plaintext attack, or chosen-cipher text attack. Based on the cryptanalytic results of the system, it is concluded that this image scrambling scheme is only used for (lossless or lossy) typical encryption, in place of providing a full protection of all (or most) visual information in the plain-image.

PROPOSED APPROACH AND FUTURE SCOPE

Proposed approach is divided into two parts namely, encryption and encoding, and decoding and decryption.

Image Encryption and Encoding

Image encryption and encoding approach is summarized below:

Step-1: Read color image i.e. (m).
Step-2: Convert color image into grey image i.e. (mm).
Step-3: Add 2 to the intensity values of grey image i.e. (mmm).
Step-4: Find the prime numbers count for every intensity value i.e. (mp).
Step-5: Find the last prime number in the list i.e. (ml).
Step-6: Subtract the last prime number from the result of Step-3 i.e. (mr).
Step-7: Find the quotient image using results of Step-4 and Step-6 i.e. (mq=mp/mr).
Step-8: Find the remainder image using results of Step-4 and Step-6 i.e. (mz=modulo(mp,mr)).
Step-9: Perform encoding on the results of Step-6, Step-7, and Step-8 using Huffman coding or Run-length coding

Image Decoding and Decryption

Image decoding and decryption approach is summarized below:

Step-1: Decode the received three files using relevant decoding technique to get three different decoded images i.e. Dmr, Dmq, Dmz
Step-2: Use above obtained three planes of images to construct the prime count matrix of image size i.e. Dmp=(Dmr*Dmq)+Dmz.
Step-3: Based on the results obtained in Step-2, find the list of prime numbers for every value of prime count matrix.

Step-4: Find the last prime number from the each list obtained in Step-3 to get last prime number matrix i.e. Dml.

Step-5: Add the last prime number matrix, that is the result of Step-4 to Dmr plane and then subtract 2 from the resultant plane to get the reconstructed image i.e. (Dml+Dmr)-2.

Preliminary Results

Preliminary obtained results are summarized in the Figure 1 through Figure 7.

Figure 1: Original Image

Figure 2: Gray-scale Image

Figure 3: Primary Count Image

Figure 4: Last Primary number Image

Figure 5: Difference Image i.e.mr= (mmm-ml)

Figure 6: Quotient matrix Image

Future Scope

Prime count matrix can be used for the pixel scrambling, as it plays a very important role in encryption mechanism. Prime count matrix can be used as the index matrix, as the maximum number existing in the matrix is 55. Based on this, the block of size 8X7 index matrix can be used repeatedly for the relocation of pixel values of the original image, which can give the better scrambled image. Possible combinations of the index matrix are shown in Figure 4.

Figure 7: Remainder matrix image

37	38	39	40	41	42	43
36	17	18	19	20	21	44
35	16	5	6	7	22	45
34	15	4	1	8	23	46
33	14	3	2	9	24	47
32	13	12	11	10	25	48
31	30	29	28	27	26	49
X	55	54	53	52	51	50

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	32	33	34	35
36	37	38	39	40	41	42
43	44	45	46	47	48	49
50	51	52	53	54	55	X

Figure 4: Possible combinations for Index Matrix

CONCLUSION

This paper provides detailed review of different existing Image Compression and Encryption Techniques along with some Hybrid approaches. By considering all aspects regarding the approaches there is no such technique that provides high security to image data and retrieves it without any loss simultaneously. We have to compromise on lack in one of the aspect. This motivates in development of technique that not only provides security without any data loss but also have less computational complexity.

References

Xinpeng Zhang; Yanli Ren; Liquan Shen; Zhenxing Qian; Guorui Feng, "Compressing Encrypted Images With Auxiliary Information," *Multimedia, IEEE Transactions on* , vol.16, no.5, pp.1327,1336, Aug. 2014

M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," *EURASIP J. Inf. Security*, pp. 1–20, 2007.

G. Jakimoski and K. P. Subbalakshmi, "Security of compressing encrypted sources," in *Proc. 41st Asilomar Conf. Signals, Systems and Computers (ACSSC 2007)*, 2007, pp. 901–903.

R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in *Proc. 16th Eur. Signal Processing Conf. (EUSIPCO 2008)*, Lausanne, Switzerland, Aug. 2008.

A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in *Proc. IEEE 10th Workshop Multimedia Signal Processing*, 2008, pp. 760–764.

W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Signal Process*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 749–762, 2008.

D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, "On compression of data encrypted with block ciphers," in *Proc. IEEE Data Compression Conf. (DCC '09)*, 2009, pp. 213–222.

E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar.2008.

A. Kumar and A. Makur, "Lossy compression of encrypted image by compressing sensing technique," in *Proc. TENCON 2009 IEEE Region 10 Conf.*, 2009, pp. 1–6.

X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 53–58, 2011.

X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 3108 3114, Jun. 2012.

S.W. Ho, L. Lai, and A. Grant, "On the separation of encryption and compression in secure distributed source coding," in *Proc. IEEE Information Theory Workshop*, 2011, pp. 653–657.

Jiantao Zhou; Xianming Liu; Au, O.C.; Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation," *Information Forensics and Security, IEEE Transactions on* , vol.9, no.1, pp.39,50, Jan. 2014

Reichel, J.; Menegaz, G.; Nadenau, M.J.; Kunt, M., "Integer wavelet transform for embedded lossy to lossless image compression," *Image Processing, IEEE Transactions on* , vol.10, no.3, pp.383,392, Mar 2001

Wei Liu; Zeng, Wenjun; Lina Dong; Qiuming Yao, "Efficient Compression of Encrypted Grayscale Images," *Image Processing, IEEE Transactions on* , vol.19, no.4, pp.1097,1102, April 2010

Jiantao Zhou; Au, O.C.; Guangtao Zhai; Yuan Yan Tang; Xianming Liu, "Scalable Compression of Stream Cipher Encrypted Images Through Context-Adaptive Sampling," *Information Forensics and Security, IEEE Transactions on* , vol.9, no.11, pp.1857,1868, Nov. 2014

Kang, Xiangui and Peng, Anjie and Xu, Xianyu and Cao, Xiaochun, "Performing scalable lossy compression on pixel encrypted images", *EURASIP Journal on Image and Video Processing ,Springer International Publishing* , vol.2013, no.1,May-2013

Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image," *Information Forensics and Security, IEEE Transactions on* , vol.6, no.1, pp.53,58, March 2011

Ching-Hung Yuen, Kwok-Wo Wong, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1," *Applied Soft Computing*, Vol 11, Issue 8, Pp 5092-5098, Dec 2011.

Jridi, M.; Alfalou, A., "A VLSI implementation of a new simultaneous images compression and encryption method," *Imaging Systems and Techniques (IST), 2010 IEEE International Conference on* , vol., no., pp.75,79, 1-2 July 2010

Bourbakis, N.G., "Image data compression-encryption using G-scan patterns," *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on* , vol.2, no., pp.1117,1120 vol.2, 12-15 Oct 1997

Xiaobo Li;Jason Knipe;Howard Cheng, "Image compression and encryption using tree structures1", *Pattern Recognition Letters,Elsevier*, Vol 18, Issues 11–13, Pp 1253-1259, ISSN 0167-8655, November 1997

Shengli Xie; Zuyuan Yang; Yuli Fu, "Nonnegative Matrix Factorization Applied to Nonlinear Speech and Image Cryptosystems," *Circuits and Systems I: Regular Papers, IEEE Transactions on* , vol.55, no.8, pp.2356,2367, Sept. 2008

Cheng, H.; Xiaobo Li, "Partial encryption of compressed images and videos," *Signal Processing, IEEE Transactions on* , vol.48, no.8, pp.2439,2451, Aug 2000

Reaz, M.B.I.; Mohd-Yasin, F.; Tan, S.L.; Tan, H.Y.; Ibrahimy, M.I., "Partial encryption of compressed images employing FPGA," *Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on* , vol., no., pp.2385,2388 Vol. 3, 23-26 May 2005

Jianji Wang; Nanning Zheng, "A Novel Fractal Image Compression Scheme With Block Classification and Sorting Based on Pearson's Correlation Coefficient," *Image Processing, IEEE Transactions on* , vol.22, no.9, pp.3690,3702, Sept. 2013

Chan, Yuk-Hee; Lui, Ka-Chun; Lun, P.K., "Compressing color-indexed images by dynamically reordering their palettes," *Signal Processing Conference, 2008 16th European* , vol., no., pp.1,5, 25-29 Aug.2008

Kakde O.G.; Thakur N.V. , "Color image compression with modified fractal coding on spiral architecture," *International journal of Multimedia*, vol:2, No:55-66, Aug 2007

Shujun Li; Chengqing Li; Kwok-Tung Lo; Guanrong Chen, "Cryptanalysis of an Image Scrambling Scheme Without Bandwidth Expansion," *Circuits and Systems for Video Technology, IEEE Transactions on* , vol.18, no.3, pp.338,349, March 2008