Markov Random Field based Compression of Encrypted Medical Images

Vinoth Kumar C, Nirmala K

Sri Sivasubramaniya Nadar College of Engineering, Chennai, India

Corresponding author: Vinoth Kumar C, Email: vinothkumarc@ssn.edu.in

Medical images are extensively used to convey information for further diagnosis. A large number of such images need to be stored in medical databases with assured security. Secure transmission of medical images requires a robust encryption and compression algorithm. There have been a few researches on the binary and gray scale encrypted and compressed images, despite the fact that there have been many studies on the non-encrypted-compressed images. On the other hand, low computational complexity and high security are not able to achieve by existing encryption image compression algorithms simultaneously. As a result, a method for compressing an encrypted image demands additional investigation in order to make optimal use of storage space while maintaining confidentiality. In order to overcome this issue, this study proposes a novel image encryption-then-compression (ETC) system based on 2D Compressive Sensing (2DCS) and the Markov random field (MRF) model. The objective is to achieve both minimal computing complexity and high security. In addition, the reconstructed image should have a significantly higher Peak Signal-to-Noise Ratio (PSNR).

Keywords: Markov random field, Encryption, Compression, Compressive sensing, Wavelet Transform.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 309–317. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-32

1 Introduction

Images are extensively used to convey information in today's world. Since an image has a significant number of pixels, the sender normally compresses it first, and then encrypts it before sending it to the recipient over a communication channel. This ensures secrecy and saves bandwidth. When sending an image over an untrusted communication route with limited bandwidth, the standard approach is to first reduce redundancy by compressing the image and then to protect the privacy of the compressed image, encrypt it as shown in Fig. 1 [5]. Encryption-then-compression (ETC) is necessary in certain applications, even though compression-then-encryption (CTE) system satisfies the demands of some important applications, i.e., image compression must be performed after encryption as shown in Fig. 2 [5].

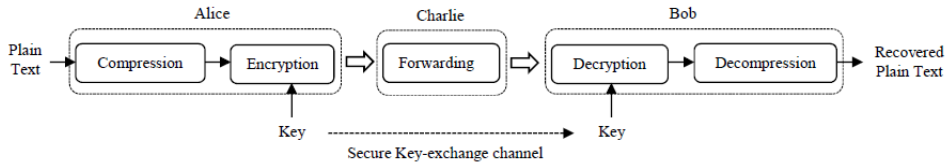


Fig 1. Traditional CTE system [5]

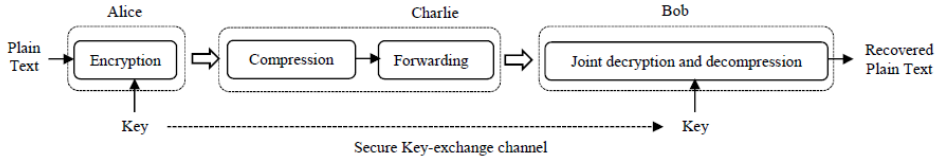


Fig 2. The ETC system [5]

To explain the CTE system using an illustration, consider through Charlie, Bob receives an image from Alice. She compresses as well as encrypts data. Charlie is required to simply forward this to Bob. But there may be circumstances where Charlie is needed to store images and forward it to the receiver, when asked. In the case of scenario such as cloud computing and distributed processing, the sender may lack computer resources, thus it may just encrypt the cover image without compressing it first. The encrypted image is compressed within the transmission channel without obtaining the encryption key in order to preserve communication traffic and storage space. To retrieve the original image on the receiver side, concurrent decompression and decryption must be performed. As a result, the ETC case is created. Let this be explained with an example. Alice wishes to send an image to Bob across a dubious channel set up by Charlie. She wishes to encrypt the image to safeguard the image's privacy. Despite this, she seems to have no desire to reduce the image and hence intends to delegate the compression computation to Charlie, the channel administrator, who usually has adequate processing resources. As a result, in the image ETC system, Alice just has to encrypt the image to disguise its content before sending it to Charlie. Charlie might receive many such images for transmission to other parties. Hence, this calls for a need for compressing those encrypted images in order to reduce storage space. As a result, Charlie will have to condense the secret image without knowing the original data or the key. This is the ETC system. For the encrypted binary pictures, the present system uses a lossy compression method. Using Stream Cipher method, the sender encrypts the binary image. Then in the cloud site, the encrypted binary image is down-sampled and creates the LDPC syndrome. The receiver restores

the original input binary image by creating joint element graph with the combination of LDPC decoding, decryption, and MRF. Finally, the sum-product algorithm (SPA) is performed on the constructed joint factor graph.

Farok et al. [1] conducted an investigation into image encryption technologies. An efficient cryptographic technique has a vast key space that resists brute force search time, low execution time complexity, and fast speed, as well as the capacity to provide high confusion and diffusion to provide good security. Several ciphers techniques such as both classic and modern for images are compared based on various parameters. An analysis of simulation results shows that chaotic encryption techniques, especially hyper-chaotic, are the most efficient among them all. The limitations of the existing system are that it can be applicable to the binary images, includes more error in the reconstructed images and high time complexity. Sirichotedumrong et al. [2] introduced a novel block scrambling encryption technique for JPEG images used to safely transmit images across an untrusted channel provider that increases the security of ETC systems. They suggested an encryption technique that is suitable for use with social networking sites (SNS).In comparison to traditional methods, the proposed method allows for a reduced block size of greater number. Images encrypted using this system contain less colour information, even when the original image has three colour channels, due to the usage of grayscale. These features improve security against brute-force assaults, jigsaw puzzle solver and other threats.

Suneetha et al. discussed an efficient lossless and lossy compression technique based image ETC system. This image encryption technique provides high level of security in the prediction error domain [3].Prediction error clustering and random permutation are used to perform image encryption in the suggested framework. Using a context-adaptive arithmetic coding method, highly efficient compression of encrypted data was achieved. Theoretical and experimental findings reveal that reasonable levels of security have been maintained. More significantly, the coding effectiveness of the recommended compression approach on encrypted photos is very close to that of state-of-the-art lossless / lossy image codecs that receive original, unencrypted images as input.

Miao Zhang et al. [4] achieved reconstruction resilience and high security by presenting a technique for image compression and encryption based on compressive sensing (CS) and Fourier transform. The authors have used the Two-dimensional fractional Fourier transforms (2D-FRT) to execute encryption in order to avoid disclosing the security of plaintext energy information from encrypted text and reusing the measurement matrix to increase security. According to the test findings, this approach has a high level of security, compression performance, and reconstruction robustness. Existing CS-based coding systems for encrypted images, on the other hand, have not been able to accomplish both low computational complexity and excellent security. Zhang et al. [5], Using the 2DCS approach, a novel compressed sensing (CS) method-based ETC system was suggested. On the encoder side, the original image is first encrypted with GRP and then the encrypted image is compressed with 2D CS. The 2D projected Land weber (2DPL) technique is proposed for image reconstruction on the decoder side and for image reconstruction on the decoder side, the 2D projected Landweber (2DPL) technique is proposed. Wang et al. [6] provided a method for compressing encrypted binary images efficiently. The stream cypher is used to encrypt the original binary image, which is subsequently compressed using sequential down-sampling and LDPC encoding. The reconstruction problem is described as an optimization problem in lossy reconstruction, and the joint factor graph is built to tackle this optimization problem. The original binary picture is then retrieved in a lossy manner by developing the SPA (sum-product method) tailored to the JFG-LR and then executing the adapted SPA on the JFG-LR iteratively. With the original, unencrypted binary images as input, experimental findings reveal that this suggested technique yields optimal compression efficiency and is comparable to, if not better than, JBIG2. Wang et al. [7] have proposed a method for characterizing the statistical relationships between neighboring bit planes of a grey image using MRF, representing it with a factor graph, and then

integrating the MRF factor graph into the binary image reconstruction factor graph, resulting in a joint factor graph for grey image reconstruction (JFGIR).The reconstruction of the original bit planes is aided by utilising the JFGIR at the receiver and theoretically deriving the sum-product algorithm (SPA) applied to the JFGIR, resulting in a novel MRF-based ETC system. The proposed technique, which uses the 2-D Markov source model at the receiver, outperforms the state-of-the-art and is comparable to or slightly inferior to the resolution-progressive approach in recovery.

Medical images are extensively used to convey information for further diagnosis. A large number of such images need to be stored in medical databases with assured security. So cloud sites must perform compression on images and also, the images must be encrypted at the sender's end as cloud sites are third parties. Hence, a method to perform compression on an encrypted image deserves further exploration in order to efficiently use the storage space and ensure confidentiality. From the detailed literature survey, it was evident that, to perform compression on encrypted images a highly secure algorithm is needed. In response to that, a scheme using 2D Compressive Sensing (CS) and MRF has been proposed to achieve low computational complexity, high security and maximum PSNR.

2 Methodology

To provide strong security and minimal computing cost, a 2D Compressed Sensing (2DCS) image coding system is employed for encrypted images. To provide high secrecy, a global random permutation-based encryption approach is used. 2DCS is used to compress this encrypted image with minimal computational complexity. A 2D Projected Gradient (2DPG) with MRF algorithm is used for reconstruction, where, iteratively, the signal recovery is implemented. Every iteration involves two step. First is to increase image sparseness in the wavelet domain by bivariate shrinkage and the second is to project the iterative solution onto the cypher domain. After a certain number of iterations, the original image's accuracy is estimated. The suggested ETC system based on 2DCS has a number of advantages over current CS-based ETC approaches. The key benefit of this system is that it achieves low computing complexity while providing good security. The reconstructed image is then given a large boost in peak signal-to-noise ratio (PSNR). A novel MRF with 2DPL approach is proposed in this work, even if the encrypted image is no longer sparse, the original image is recovered. The overall procedure of the image ETC system is shown in Fig. 3.

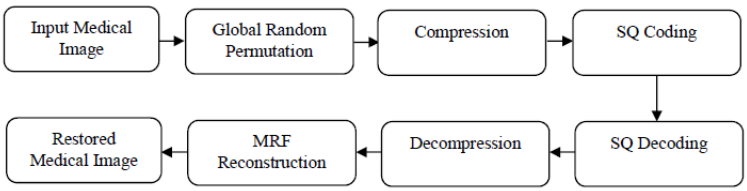


Fig 3. Schematic representation of the proposed method

The proposed method involves of three steps namely the global random permutation (GRP) based image encryption; 2DCS based encrypted-image compression and MRF joint decoding scheme with 2DPG algorithm. The image is encrypted using GRP method and the privacy of the image is protected before sending it to the network operator.

2.1.1 Image Encryption

In ETC systems that use JPEG compression to reliably transmit images over an unreliable channel provider, the grayscale-based block scrambling image encryption algorithm is presented to increase not only confidentiality but also compression efficiency. In comparison to the color-based image encryption system, this scheme allows for a larger number of blocks with block size. According to the block scrambling-based image encryption technique for ETC systems, an image of M X N pixels is divided into non-overlapping blocks, each having Bx X By pixels. The input medical image with M XN pixels is separated into sub images with Bx X By pixels, and the divided blocks are permuted randomly using a secret key to obtain a random integer [12-16]. Randomize the number, then using the randomized integer rotate and invert each block as a guide. Finally, using a randomly generated binary integer, to each block, the negative-positive transformation is performed.

2.1.2 Compression of the Encrypted Image

To preserve channel bandwidth and storage space, the encrypted image that is the input to the cloud site must be compressed without knowing either the secret key or the actual data. This problem is effectively solved using the 2D Compressive Sensing approach.

Algorithm for compression:

(i) Create a template matrix (with each pixel as 128) of dimensions M*N.

(ii) Subtract the template matrix from the received encrypted matrix.

(iii) Generate two M×N random matrices and multiply them along with the subtracted matrix in order to obtain the compressed matrix.

(iv) Find the maximum and minimum values of the compressed matrix and assign a value for quantized bit-depth (say 6).

(v) Calculate the quantization step-size by dividing the difference between maximum and minimum value with 2^qbit-depth, where q is the quantized bits.

(vi) Further quantize the compressed image (scalar) to obtain an encoded image. Each pixel corresponds to a rounded-off value depending on the step size obtained.

2.1.3 Image Reconstruction

The recovery of image signal is performed iteratively. Two steps are involved in each iteration. To begin, bivariate shrinking is used to stimulate the scarcity of images in the wavelet domain. The solution space is then inserted in the cypher domain to project the iterative solution [17-21]. An estimation of the original image is obtained accurately after a given number of iterations.

Algorithm for Image Reconstruction:

(i) Multiply template matrix with the randomly generated matrices (during compression) and add it to the encoded matrix to obtain decoded matrix.

(ii) Pseudo-inverse the random matrices and multiply them with the decoded matrix.

(iii) For each iteration, perform Dual-tree discrete wavelet transform (DT- DWT) on the gradient values, and then apply bivariate shrinkage by calculating approximation coefficient value and shrinkage image.

(iv) Inverse DT-DWT is applied in between the process to obtain the iterative solution space.

(v) In the wavelet domain, update the image in the solution space followed by the projection in the cipher domain.

(vi) Unscramble the data of the image in the decryption process and update the index value of the image.

(vii) Perform negative to positive inverse transformation.

(viii) Carry out MRF based pixel reconstruction in optimization by choosing an initial configuration for the variables.

(ix) Iterate through each node, calculating the energy-minimizing value given the current values for all variables in the region. (New value of variables becomes current value for next iteration)

3 Simulation Results

The original medical image is encrypted using GRP and scrambling at the sender's site. The encrypted image undergoes compression by 2D CS algorithm. Further it is subjected to scalar quantization - encoding and decoding. Finally, the image is reconstructed using 2D PG and MRF algorithms, at the receiver's site. Various medical images (CT and X-Ray Images, shown in Fig. 4) of different anatomy are considered to illustrate our proposed algorithm.

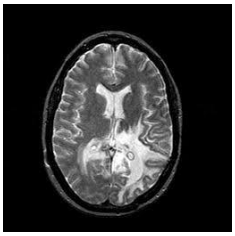
(a) Eye

(b) Thorax-T.S

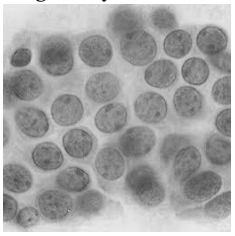
(c) ShoulderJoint

(d) Lung-X-Ray

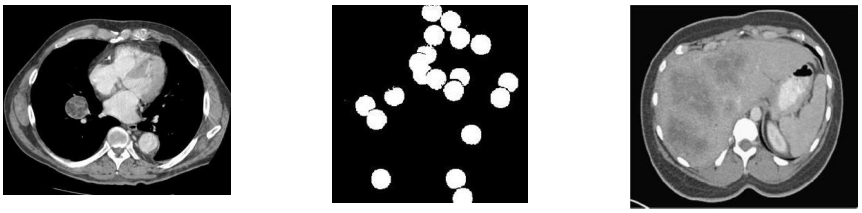
(e) Heart



(f) Brain



(g) Blood cells



(h) Lung Tumor (i) Cancer cells (j) Liver Lesions

Fig 4. Input Medical Images

The simulation results of the medical image - Lungs X-ray is illustrated Fig. 5. The medical image is scrambled and encrypted by GRP method. The encrypted image is sent to the cloud site for compression. As the cloud site is owned by a third party, encryption is required in order to preserve the patients' privacy. The encrypted medical image undergoes 2D compressive sensing based compression and then is encoded using scalar quantization before leaving the cloud. This final encoded image is sent to the receivers' end. The reconstruction part of the algorithm includes Scalar quantization - decoding, decompression, and unscrambling using 2DPG and MRF concepts. Later reconstruction of the restored image comparable to the original image is carried out. For the reconstructed image, the values of PSNR and MSE are calculated as measures to judge the efficiency of the system.

The quality of the compressed image is measured using MSE and PSNR. Lower the value of MSE indicates the reduced error. The elapsed time, the actual time to execute the program, is a measure to analyze the time complexity. The MSE, PSNR and elapsed time values obtained for all the input medical images have been tabulated in Table 1.From the table, it can be inferred that the presented algorithm resulted in lower MSE and elapsed time for all the test medical images.

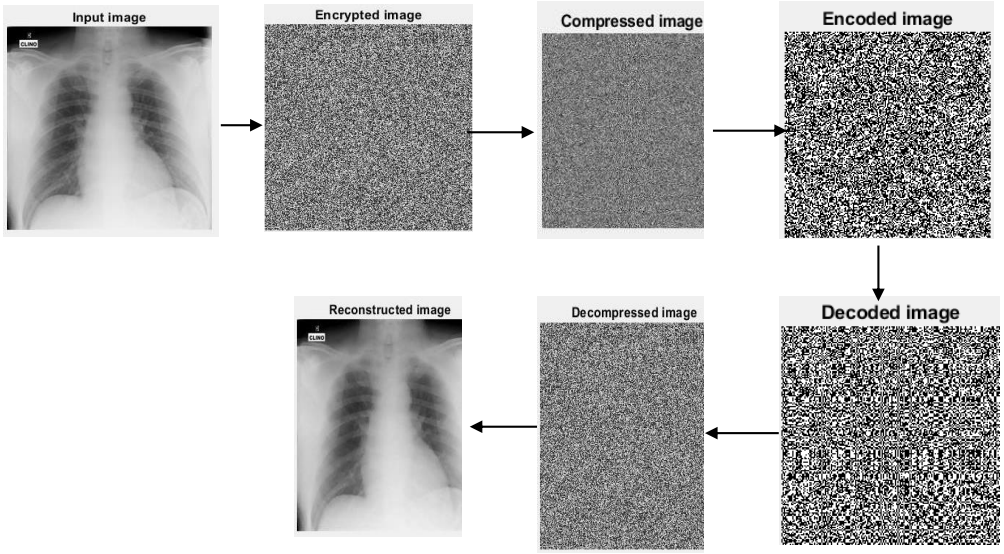


Fig 5. Simulated result of Ling X ray Image using the proposed algorithm

Table 1. Performance analysis of the presented scheme for various medical images

Image Name	Proposed Method		Method 1 [4]		Method 2 [22]	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Eyes	0.6995	49.68	0.7794	49.21	0.8534	48.82
Thorax	1.0211	48.04	1.1322	47.59	1.2542	47.15
ShoulderJoint	0.5983	50.36	0.6641	49.91	0.7305	49.49
Lung	0.3607	52.56	0.3914	52.20	0.4354	51.74
Heart	0.4803	51.32	0.5842	50.47	0.5311	50.88
Brain	1.6126	46.06	1.9131	45.31	1.7391	45.73
Bloodcells	1.3793	46.73	1.7398	45.73	1.5817	46.14
LungTumor	1.5954	46.10	1.7572	45.68	1.9329	45.27
CancerCells	0.3646	52.51	0.4457	51.64	0.4902	51.23
LiverLesions	1.8674	45.42	2.0213	45.07	2.2234	44.66

4 Conclusion

With the growing importance of images in the medical field, we need a secure system for storing and retrieving those images. The CS-based ETC using MRF and 2DPGis proposed in this work. On the encoding side, the original image is encrypted using global random permutation, and the encrypted image is compressed using 2DCS. For image reconstruction on the decoder side, 2DPG mixed with MRF method is proposed. This system is useful since it provides minimal computational complexity, good security, and a large gain in PSNR of the reconstructed-images at the same time. As a result, it illustrates the scheme's viability and effectiveness. This work uses the concept of 2D Compressive Sensing, bivariate shrinkage and MRF for efficiently compressing encrypted images as well as reconstruction. The main focus is to achieve a secure system with maximum PSNR and minimum MSE values of the reconstructed image. However, different methods of encryption, compression and reconstruction may yield different results, in certain cases, better results. Hence the future work would be to study and work on different methods to make the algorithm more efficient and error-free.

References

[1] Mohammad, O. F. et al. (2017). A Survey and Analysis of the Image Encryption Methods. *International Journal of Applied Engineering Research*, 12(23): 13265-13280.

[2] Sirichotedumrong, W. et al. (2018). Gray scale based block scrambling image encryption for social networking services. *IEEE International Conference on Multimedia and Expo*, 1-6.

[3] Suneetha, B. (2015). Designing an efficient image encryption-then- compression system. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, 3(3): 1-12.

[4] Zhang, M. et al. (2020). Image Compression and Encryption Scheme Based on Compressive Sensing and Fourier Transform. *IEEE Access*, 19419062, 1-9.

[5] Zhang, B. et al. (2019). Compressing encrypted images by using 2D compressed sensing. *IEEE 5th International Conf. on Data Science and Systems*, 19029666: 1-9.

[6] Wang, C. et al. (2018). A New Encryption-Then-Compression Scheme on Gray Images Using the Markov Random Field. *Computer, Material and Continua*, 56(1): 107-121.

[7] Wang, C. N., Zhang, J. X. and Huang, Q. (2019). A New MRF-Based Lossy Compression for Encrypted Binary Image. *IEEE Access*, 8: 11328 – 11341.

[8] Endur, L. S. and Selesnick, I. W. (2002). Bivariate shrinkage functions for wavelet- based denoising exploiting interscale dependency. *IEEE Transactions on Signal Processing*, 50: 2744-2756.

[9] Hu, R., Li, X. and Yang, B. (2014). A new lossy compression scheme for encrypted gray-scale images, In *IEEE International Conference Acoust Speech and Signal Processing (ICASSP)*, 1-8.

[10] Yang, J. et al. (2008). Image coding using dual-tree discrete wavelet transform. *IEEE Transactions on Image Processing*, 17: 1555-1569.

[11] Johnson, M. et al. (2004). On compressing encrypted data. *IEEE Transactions on Signal Process*ing, 52(10):2992-3006.

[12] Kumar, A. and Makur, A. (2008). Distributed source coding based encryption and lossless compression of gray scale and color images. In *Proceeding of IEEE 10th Workshop Multimedia Signal Process*, 760-764.

[13] Kumar, A. and Makur, A. (2009). Lossy compression of encrypted image by compressing sensing technique In *IEEE Region 10 Conference (TENCON)*, 1-6.

[14] Liu, W. et al. (2010). Efficient compression of encrypted grayscale images. *IEEE Transactions on Image Process*ing, 19(4): 1097-1102.

[15] Schonberg, D., Draper, S. and Ramchandran, K. (2006). On compression of encrypted images. In *Proc. Int. Conf. Image Process*, 269-272.

[16] Schonberg, D. et al. (2008). Toward compression of encrypted images and video sequences. *IEEE Trans. Inf. Forensics Security*, 3(4):749-762.

[17] Wang, A. et al. (2018). Efficient compression of encrypted binary images using the Markov random field. *IEEE Trans. Inf. Forensics Security*, 13(5): 1271–1285.

[18] Woods, J. W. (1972). Two-dimensional discrete Markov random field. *IEEE Trans. Inf. Theory*, 18(2):232–240.

[19] Zhang, X. et al. (2011). Compressing encrypted image using compressive sensing. In *IEEE Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, 222-225.

[20] Zhang, B., Yang, L. and Wang, K. (2018). Block compressed sensing using two-dimension random permutation for image Encryption-then- Compression applications. In *IEEE Conference on Signal Processing (ICSP)*, 312-316.

[21] Zhou, J. et al. (2014). Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE Trans. Inf. Forensics Security*, 9(1):39-50.

[22] Wang, A. et al. (2015). A new encryption-then-compression algorithm using the rate–distortion optimization. *Signal Processing and Image Communication*, 39: 141–150.