Advance in Technology, Engineering and Compuring – A Multinational Colloquium – 2017
Editor(s) Vinod P., Sunil Jacob, Sheeja Janaradhanan and Ratish Menon
doi:10.3850/978-981-11-0744-3_17-71-cd

Secure Analog Joint Source Channel Coding for Image Transmission

Glinet A. D. Silva[a], Pearlsy P. V.[b] and Ambili A. R.[c]

Department of Electronics and Communication Engineering Federal Institute of Science and Technology, Angamaly, Kochi, Kerala 683577, India.
[a] *glinet.antonydsilva9@gmail.com,* [b] *pearlsypv@fisat.ac.in,*
[c] *ambili ar@ f isat.ac.in.*

Secure Analog joint source channel coding (AJSCC) is a novel Shannon-Kotelnikovs mapping based confidential data protection scheme, whose security and integrity of the encrypted image sharing resist fraudulent scenario. Nowadays these problems affect most of the secure communication systems. Here this paper deals with AJSCC for which we make a literate choice of a good mapping structure such that the distortion between the transmitted and the reconstructed data is minimized. Initially investigation of transmission of independent and identically distributed (iid) Gaussian source over AWGN channel is performed. Then the case of 2:1 bandwidth reduction which can be easily applied for higher reduction factors is achieved which is further studied for image application. Furthermore, a data encryption based on position shuffling is introduced. The algorithm shuffles and reshuffles position of the image element in a retraceable manner with a large and different set of sensitive keys, which is sufficient to resist brute force attack. The proposed encryption scheme gives a significant resistance to other statistical attack with reduced delay and bandwidth efficiency.

1 Introduction

The increasing security attack of data transmission over the internet is an important issue to be addressed. A secure Communication requires a well-defined encryption technique. The term encryption can be defined as the practice of obscuring a piece of information by encoding it so that it can only be decoded, read and understood by the people for whom the information is intended. This paper, initially consider an analog joint source channel coding

(AJSCC) scheme for the analog transmission of discrete-time continuous amplitude source over an AWGN channel based on Shannon Kotel nikov mapping. The analog joint source channel coding scheme used here offers both bandwidth reduction and robustness to noise. The performance of the AJSCC is studied using Optimum value theoretically attainable (OPTA)[2]. From the theoretical perspective, separate source channel coding was proven to be optimal by Shannon [1], even though it provides an improved performance whenever the channel is fixed. The large block length unfortunately increases the delay and complexity of the system. When traditional communication system is considered the continuous source is first source encoded followed by channel encoding using capacity approaching channel codes such as LDPC codes [16] and turbo codes [27]. Such systems were uniquely designed for desired rate/distortion. Therefore, redesigning of system was necessary as each time the channel condition changes i.e. the source become under protected with increasing channel noise and vice versa. Analog Joint Source Channel Coding scheme is another possible choice to conventional digital system for drawing near optimum performance for high data rate with very low complexity and delay [4]-[6]. Interestingly with a known fact that analog communication is optimal in some circumstances, we prefer the direct transmission of Gaussian sample over AWGN channel [2], constrain to the fact that the Gaussian source are perfectly matched to Gaussian channel [3]. Over the past years, AJSCC is performed based on analog mapping scheme known as Shannon-Kotel Nikov mapping [7] based on parameterized continuous space filling curve also known as signal curves. The suitable geometric structure for this can be chosen through an educational guess or by looking up in a codebook structure of channel optimized vector quantizer [9], [10]. Recently we have performed some 2:1 bandwidth reduction scheme which makes use of an Archimedes parametric spiral curve to perform dimension compression. The early proposed technique was based on MMSE estimator which is similar to the idea discussed by [11] and [12] but with high complexity. Hence later they followed MMSE followed by ML detection scheme which was found to be much more delaying free and fewer complexes.

Several literatures on analog coding scheme have appeared in practice, which are based on uniform source and nonlinear mapping [1], [5], [11] and [16]. The ideas discuss that the discrete-time analog joint source channel coding achieve nearly optimal performance with much lower complexity and delay. The concept was already proposed more than 50 years ago by Shannon [17] and Kotelnikov [18], which have recently acquired a renewed importance due to the work of Chung [10], Vaishampayan [19], Fuldseth [20], Ramstad [21], Hekland [22], [23], and Wernesson and Skoglund [24] on AJSCC as a capacity approaching bandwidth reduction scheme. In the case of bandwidth compression, the encoding idea to reduce the number of samples to be transmitted i.e. to represent a tuple of N source samples as a point in a N-dimensional space where a non-linear surface of dimension K lives. Then, the N-tuple is projected onto the hyper surface and the corresponding K-tuple is transmitted through the noisy channel. The AJSCC is applied for the transmission of digital images over AWGN channel.

Despite of the encoding and decoding process we introduce a secure image transmission by randomizing the data transmitted based on randomly generated key which is assumed to be symmetric and secure. Inorder to ensure the security and integrity of the transmitted image, a new encryption algorithm is introduced which is based on the shuffling of image pixels with an extended and sensitive key sets. This approach with the former model is successfully analyzed under a fraudulent scenario and is extended to study of attack [25] and information vulnerability.

The paper is structured as follows: Section II discuss the proposed secure analog joint source channel coding based image transmission and give a review of AJSCC approach over an AWGN channel. It also presents a novel symmetric key encryption. Section III present result of computer experiment and is devoted to results and simulation and section IV is finally dealt with conclusion.

2 Proposed System

This paper presents simulation of a secure transmission of bandwidth efficient 2:1 data compression with Archimedes spiral that can be used for a straight edge division of angle into n parts and a data shuffling scheme based on novel vigenere pseudo random number based permutation matrix given in Fig.3 and 4. The space filling spiral may be constructed by the uniform motion of point in a fixed direction and motion in circle with constant speed as depicted in Fig.1. A factor two bandwidth reductions is achieved by combining two consecutive samples using the parametric curve as briefly explained in Section II A. The obtained compressed data position are shuffled based on the random key generated using a retraceable algorithm (Section II B). Fig.1.2 show the block diagram of secure data transmission over AWGN channel and the simulation is performed for an image signal source.

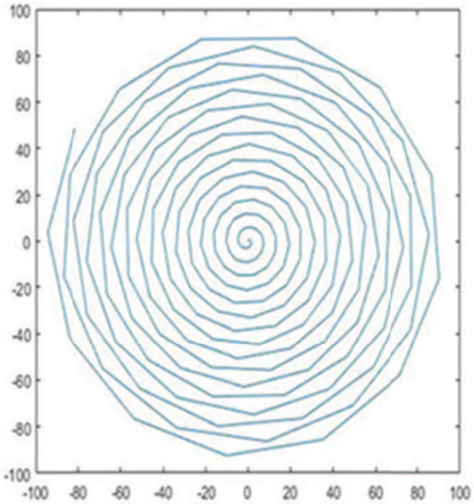

Figure 1. Archimedean Spiral Optimized for Image Transmission

2.1 Analog Joint Source Channel Coding

Here performance of a linear 1:1 mapping is discussed, where the source symbol x is directly transmitted through the channel with no additional processing therefore the channel symbol would be s=x. The received symbol at the destination is given by

$$\hat{s} = E[s / y] = \frac{R_{xy}}{R_{xy}} y \tag{1}$$

where, $\frac{R_{xy}}{R_{xy}}$ represent ratio of cross-correlation and auto-correlation respectively. In 2:1 dimension compression mapping Encoder consist of three stages as shown in Figure 2, a mapping function, a linear transformation function and a normalization factor. As compression of N=2 samples on to K=1 Channel symbols is performed it actually encode a source vector $x = (x_1, x_2)$ by mapping it on to one channel symbol , using a spiral like function as in Fig. 1 constructed following the equation given as [8].

$$X_\theta(\theta) = \begin{matrix} \mathrm{s}ign(\theta)\frac{\delta}{\pi}\theta\sin(\theta) \\ \frac{\delta}{\pi}\cos(\theta) \end{matrix} \tag{2}$$

Here, δ is the distance between two neighboring arm of the spiral. After obtaining corresponding mapped values of θ, we find the θ value for which the correspondingx_θ closest to the source vector using Mapping function $M_\delta(x)$ and a linear transformation function T_ϕ to improve SDR performance may be given by Eq. 3 and Eq. 4, with numerically optimized channel distribution shape parameter ϕ along with δ

$$\Theta = M_\delta(x) = \arg\min || x - x_\theta ||^2 \tag{3}$$

$$T_\phi = sign(\theta) | \theta |^\phi \tag{4}$$

For sake of brevity we refer to the optimized value given in [2]. As, the average power of the mapped symbol changes with the transmit parameter and with CSNR we apply normalization factor $\sqrt{Y}$ before transmission to ensure that $E\left[\left|\frac{T_\phi(M_\delta(x))}{\sqrt{Y}}\right|^2\right]$. Following normalization, an encryption is performed based on proposed novel scheme as described in Section II B. From the depicted block diagram Figure (2) it can be seen that the transmitted data is vulnerable to crypt-analyst.

A practical receiver can be designed by considering the recovery of x from y after decryption by using either ML or MMSE decoding. Many references shown that MMSE decoding perform in general better than the ML decoder, but at the expense of higher complexity. Alternatively, the use of a linear MMSE estimator of the transmitted symbols before ML decoding was proposed in [5]. This results in a performance very close to that of MMSE decoding, but with much lower complexity. Thus this work adopts ML decoding with a linear MMSE estimator as the decoding technique. Therefore, the proposed decoder consists of four stages: the de-normalization factor, a linear MMSE estimator, the inverse transform function and the inverse mapping function. The MMSE estimate of s is similar to, $\hat{s} = E[s|y]$, while the decoded symbol $\hat{\theta}$ is obtained by inverting transformation function

$$\hat{\theta} = T_{\phi}^{-1}(\hat{s}) = sign(\hat{s}) \,|\, \hat{s}\,|^{\frac{1}{\phi}} \tag{5}$$

and $x_{\hat{M} L}$ is obtained finally by simply applying $\hat{\theta}$ in the mapping function on x_{θ}[5].

$$X_{\hat{M}L} = M_{\delta}^{-1}(\hat{\theta}) = X_{\hat{\theta}}(\hat{\theta}) \tag{6}$$

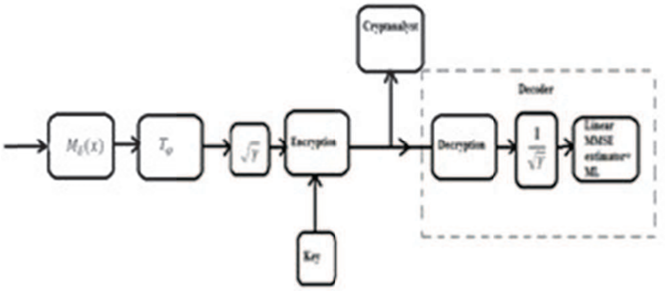

Figure 2. Block diagram for AJSCC with encryption

2.2 Vigenere Pseudo Random Matrix Based Permutation Approach (VPMBPA Encryption)

This section describes the novel symmetric key encryption scheme proposed for an analogously mapped n x n image input in to a n/2 theta values which is the compressed image element available after 2:1 compression for the encryption scheme. The compressed image element with bandwidth efficiency are permuted based on the key $Km = (k1\ k2,k3....\ kn\ )$ for m=1,2 ....q denote the number of key, generated by a pseudo random number generator that is assumed to be shared with the receiver in a secured manner. Larger the number and length of the key, security of the system could be increased .The permutation of the system is initially performed based on the generated key and then by the use of vigenere matrix [26] generated using the random choice of any key from m=1,2.....q keys in various round of operation. The advantage of the use of pseudo random key is that it gives secrecy of data in addition to the intelligible data due to the compressed state of mapped output.

In this paper discussion on an efficient image encryption scheme with an idea of vigenere matrix constructed using an integer series generated by a pseudo random number generator and the pre-defined key is carried out. This approach of vigenere pseudo random number matrix based permutation approach (VPMBPA) take an advantage of compressed image element shuffling in all direction in a maximum possible manner compared to the traditional permutation techniques. The concept of construction of vigenere cipher which is an alphabetic encryption method has a reputation of being exceptionally strong but is simple enough if known the process of construction and encoding process at the receiver. Here an idea of the vigenere cipher is utilized for the integer matrix formation using a pseudo random number set Z generated with size p. Therefore any chosen key of size n which form the column size of vigenere matrix with p number of rows having a shift with the choice from set Z. The idea can be repeated for different choice of keys.

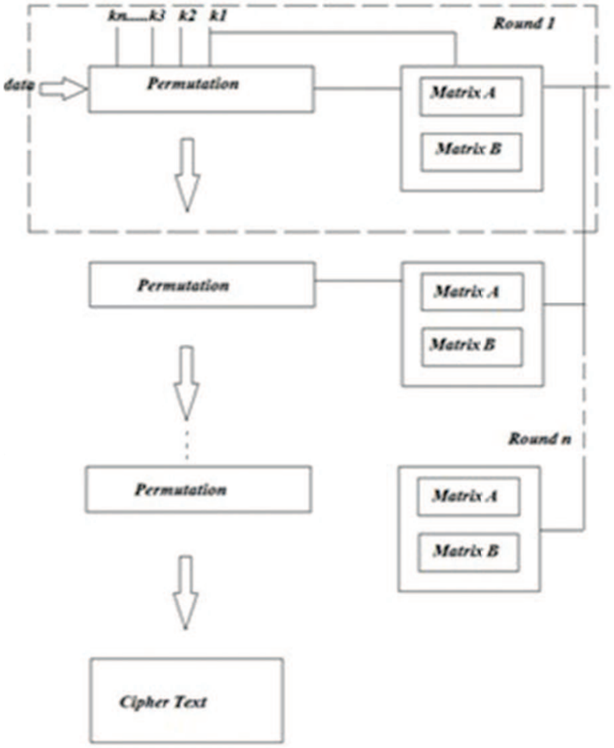

Figure 3. Block diagram of VPMBPA encryption scheme with n round operation

The block diagram of VPMBA encryption scheme is depicted in Fig. 3. The first round of the set shuffle the data set using different sets of key generated in an interdependent manner using a function f((f(x))..). The set of key generated

K_m =(k_1 k_2,$k_{(3)}$ ...... k_n) for m=1,2,....q ,with each of key element is of size 1 x n. The shuffling based on the defined function chooses the random position of k_j from k_i for i, j m and so on in a predetermined pattern, which indeed make a choice on data to be transmitted. It reduces the interdependency of the pixel values to an extent. This can be interpreted as a class of symmetric key encryption with the known pattern of function followed by the transmitter and the receiver. To overcome the amount of correlation effect that still exist we perform another stage of permutation based on vigenere matrix. In the second stage, after the initial permutation a random choice of keys from vigenere number matricesis done. Based on this choice permutation is performed which again shuffles data output from first stage of operation. The random choice of p value which would make the key prediction difficult for brute force attack. This permutation is repeated for several rounds to obtain a desirable reduced correlation between image elements.

2.3 Correlation Coefficient Analysis

Correlation coefficient analysis defines the similarity between the pixel and the strength of resistance towards the security attack which give a statistical relation between them and its sensitivity on adjacent pixel when it is altered. Here the correlation analysis of adjacent image element has been performed based on following equation of correlation coefficient.

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\overline{D(x)}\,\overline{D(y)}} \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x - E(x_i))^2 \tag{8}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{9}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{10}$$

Where x and y denote the grey value of two adjacent pixels. D(x) and E(x) denote the variance and mean value of x respectively [6].

3 Result and Discussion

In this we discuss various results obtained at different stages of operation during the process of simulation of the proposed compression and encryption scheme. Experiment evaluation of the first set of system described was performed on a data set from a Gaussian source assumed to be transmitted over an AWGN channel. In the proposed 2:1 scheme we consider a point-to-point transmission of data with the evaluation of its SDR performance with respect to the channel SNR. It should be noted that the AJSCC and parameters of the space filling curve have been numerically optimized for AWGN channel and thus we make use of the same scheme as discussed in [1]. Following the evaluation is extended to image with an idea of reduced approximation error with a codebook which can be extended to a generalized idea for any image .Following this we perform an idea of a novel encryption scheme so as to reduce maximum interdependency of the image element values analyzing its correlation coefficients along with Peak signal to noise ratio (PSNR), number of pixel change rate (NPCR) and Unified average changing intensity (UACI) of reconstructed image.

3.1 Dimension Compression Mapping on Gaussian Sample

We initially perform a linear transmission of a Gaussian sample over an AWGN channel. It is a linear 1:1 mapping were direct transmission of Gaussian source sample x as channel symbol s through an AWGN channel occur. Here no additional operations are being performed as both the channel and source are assumed to follow Gaussian characteristics. The received symbol $\hat{s}$ may be obtained by (1). In 2:1 dimension reducing mapping we perform a dimension compression by mapping 2 data symbols of source to a channel symbol as discussed in section II A .We analyze the SDR performance of this with CSNR with choice of an optimum delta and channel shape parameter as discussed in [6]. Fig 3 shows that the performance is 12 dB away from the OPTA while transmitting Gaussian source symbol over AWGN channel using a 2:1 compression Experiment evaluation of this same idea was extended to gray scale images such as Airplane, Lena and Cameraman image. Here, there may occur components of approximation threshold and channel errors in a visible manner, hence a new idea of codebook creation is being introduced to overcome the approximation error .Initially the image element are mapped on to an optimized space filling structure . Here we prefer to follow Archimedes spiral with an optimum delta value that defines the distance between two spiral arm and a channel defining parameter [2], [7]. The image element are mapped on to the spiral so as the transmitted symbol would be the minimum possible point on the spiral defining the channel characteristics. The obtained theta and corresponding image pixel element are stored as codebook. The so obtained mapped value theta of the spiral is being transmitted through the AWGN channel for different SNR values and reconstructed by decoding stages i.e. ML and MMSE decoding with approximation error and is depicted in Fig. 5. It can be noted that the pixel loss of the image is very high as compared to the original image transmitted the visible pixel information loss is due to the channel, threshold and the approximation noise of AJSCC. Next analysis of the same performed with an additional step of known codebook for image element

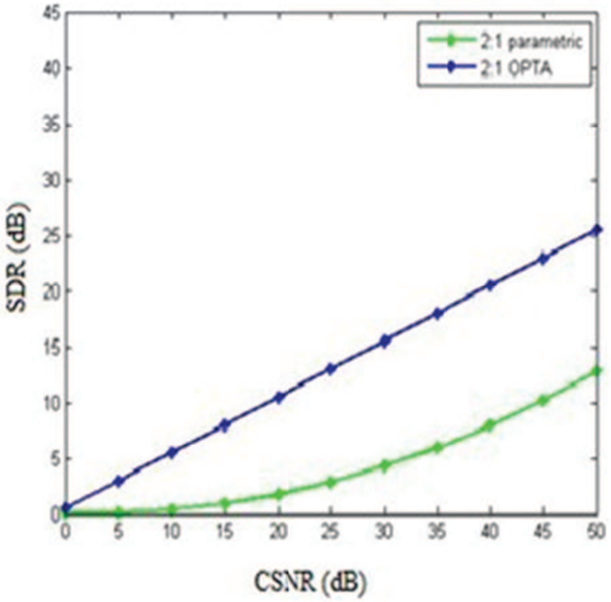

Figure 4. Performance of Parametric 2:1 Dimension Compression Analog Joint source

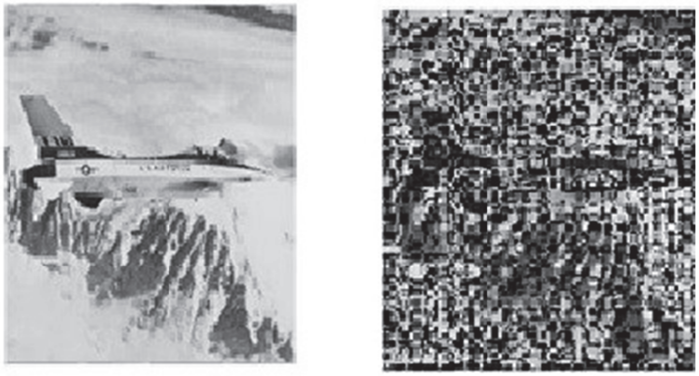

Figure 5

transmission which would help to point out the transmitted information back to the approximate image element with a thresh-old error rate of 0.0476. The creation of codebook can be introduced for mapping of any image. Eq. 1 to 3 may be used with the spiral chosen in such a way that it is optimized for image transmission so that the source space overlaps the channel space which indeed is used to find the theta value for all possible pixel combination and further the obtained data is stored. The theta value stored is used to de-map the structure after the recovery at the receiver side. It indeed reduces the approximation error occurring due to mapping data which is comparatively high when considering the visible image. The idea of reduced pixel loss is applied to the Airplane, Lena and Cameraman image for different Channel Signal to Noise Ratio (CSNR) and obtained an output as in Fig. 6. The result show that by addition of the concept of codebook provides a better visible and reduced pixel loss image compared to the image reconstruction retaining the approximation loss and channel loss. Inorder to evaluate the same a PSNR peak to signal noise ratio of the reconstructed image of airplane is being analyzed and found to give a best performance over the range of 6 dB to 8 dB and the analysis is depicted in Fig. 7.

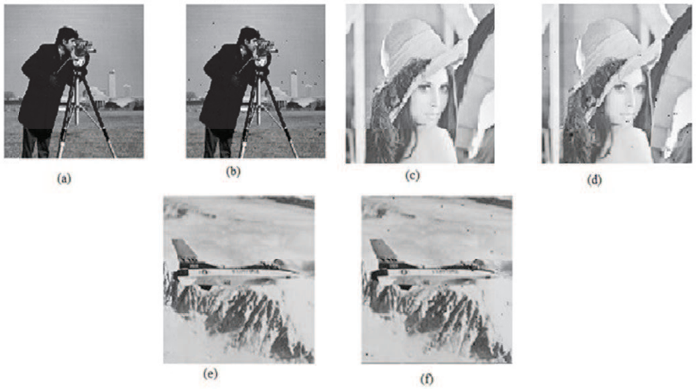

Figure 6. (a) Original Image of cameraman (b) Reconstructed image with CSNR 20 dB with reduced Approximation noise. (c) Original Image of lena (d) Reconstructed image with CSNR 20 dB with reduced Approximation noise. (e) Original Image of airplane. (f) Reconstructed image with CSNR 20 dB with reduced Approximation noise

Encryption was performed as the next stage of the proposed scheme using the retraceable algorithm. For this we choose the Airplane image. The algorithm shuffle and reshuffle the compressed data of the mapped image element providing minimum correlation between the pixel values after 10 rounds of operation as depicted in Fig. 8 (b) compared to the original image depicted in Fig. 8. (a).Here the size of key chosen is n=65536 and p= 8. The reconstructed image is shown in Fig. 8.(c) which seems to be comparable with the original image. The histogram analysis of the image is done based on the encrypted image with an expected histogram of random behavior. Fig shows the obtained histogram plot of the encrypted image and the reconstructed at an SNR of 15dB.The cipher image of airplane depicted show the encrypted image and the reconstructed image after 2 stage encryption performed with pseudo random key and vigenere matrix of numbers. . It can be observed that the histogram plot of the encrypted image show a uniform distribution compared to the histogram of original and reconstructed image hence attained a comparable result. The correlation of the encrypted and the original image is being analyzed and found to be minimum in case of encrypted image and maximum for original image which is tabulated as shown below.

Table 1. Correlation Analysis of Original and Encrypted Image

Horizontal	Vertical	Diagonal	Correlation coefficient
0.9735	0.9638	0.9287	Plain image
-0.014	-0.09638	0.0197	Encrypted image

Analysis may be performed by randomly selecting 3000 pairs of adjacent in all direction for both plain and encrypted image. It can be observed that the correlation of plain image is maximum as most of the pixels are interdependent and it shows the correlation to be maximum in all directions depicted in Figure 8(d-f) when compared to the original image Figure 8(a-c). The delay of the system is reduced when compared to the digital system as the proposed algorithm require no long block codes for encoding .The introduction to the creation of codebook Inorder to reduce the approximation error is a time consuming process when implemented in MATLAB16. To get rid of the time consumption we can perform parallel processing operation.

The overall Delay analysis of the data is being studied. The analysis was concluded as follows i.e. the image reconstructed based on the codebook was approximately obtained to be 4.035 sec and the encrypted image obtained in 8.306 sec whereas the reconstruction of image to without the codebook was found to be 7.3308 sec and the image reconstructed was with approximation error due to mapping.

3.2 Security Analysis

It can be analyzed based on the vulnerability of the cipher text or the encrypted message information to any statistical type attack. Beyond the analysis we also discuss the key sensitivity, complexity of key space and also the vulnerability of the algorithm towards brute force attack, known plain text attack, known cipher text attack and so on. All possible key that can be used to encrypt and decrypt the algorithm can be termed as key space. In this novel approach the generated key of size n and p, and number of keys m when chosen to be large and random with its number of occurrence to be one would exhibit a high complex and large key space for a crypt analyst. The key sensitivity which is another measure define how sensitive the key is to different type of attack and is indeed much complex in the proposed system. This implies that even if there is a slight change in the secret keys, the final cipher image is fully different.

Here when analyzed we could identify the key generated randomly would be difficult to be chosen from the large key space available as it give a combination of n^n his make the Brute force attack to be much complex in nature as a wrong prediction of choice of key would randomize the data pattern in a different manner. It can be also noticed that each time the key shuffle the previously randomized data and since the process occur in a sequential manner the final output would be with a decreased correlation of the data output. Here, the problem arises with finding the key length. It involves mainly 2 steps: First step is to find the period of the cipher (i.e. key length), second step is to find the key used. Given only the cipher text, we must find the Plaintext and the key. This kind of crypt Analysis that involve the idea of know cipher text attack may be difficult as the key ones used is random in nature and is further randomized in various round of operation. Considering the known plain text attack even does not contribute much to identifying the key pattern due to the random choice of chosen key encryption and the number of rounds would be unique to the user and can differ from one to another under the assumption that the key and its parameters are securely transmitted.

Another parameter measured to ensure security and integrity is NPCR and UACI. It is widely used security analysis in the field of image encryption community for differential attack. The range of NPCR and UACI is [0 1] when equal to 1 implies that all pixel values of cipher images are changed compared to the original image. The analysis of NPCR and UACI of the proposed system is performed and obtain a result of 1 and 0.4606 respectively. The analysis shows that for small key space and plaintext the proposed algorithms are Vulnerable [25].

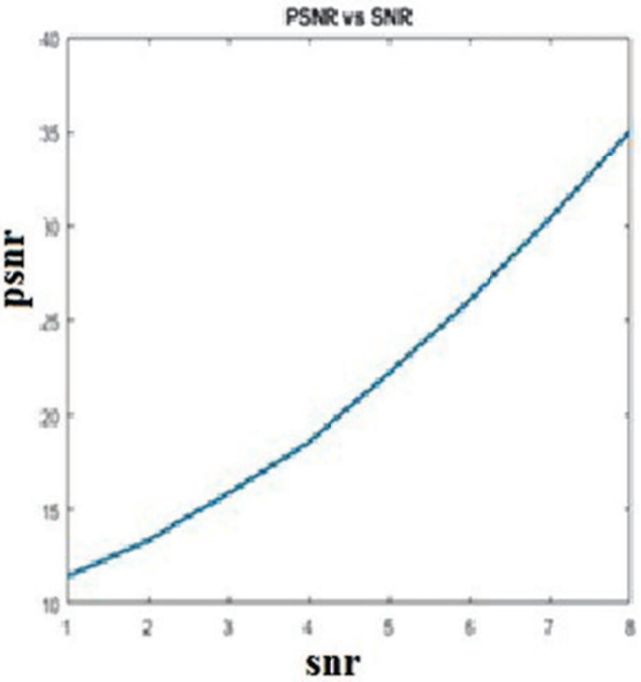

Figure 7. Performance of the image reconstructed for the transmission of compressed image elements over AWGN channel for different CSNR

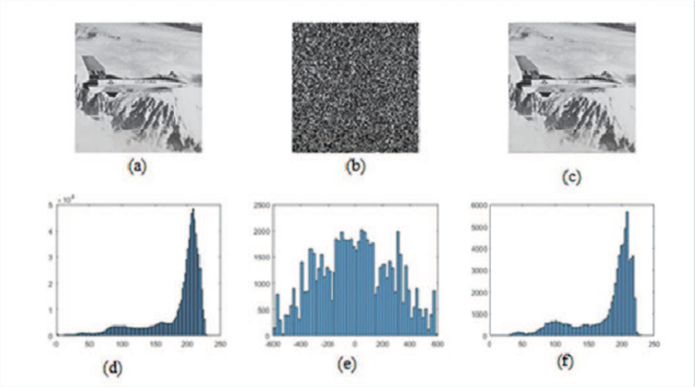

Figure 8. (a) Original image (b) Encrypted Image (c) Reconstructed (d) Histogram Plot for original image (e) Histogram plot of encrypted image (f) Histogram plot of Reconstructed Image

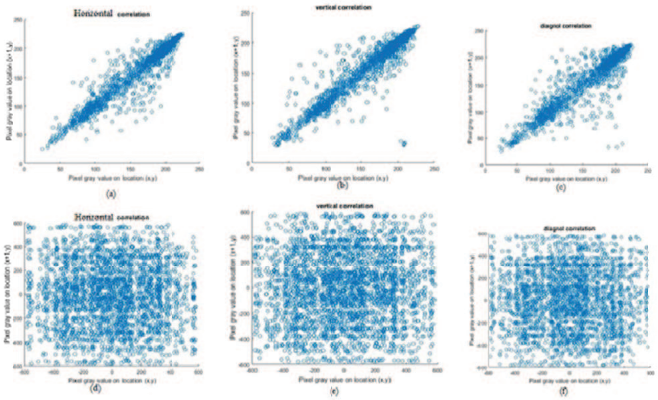

Figure 9. Correlation analysis (a) Correlation distribution of plain image along horizontal direction (b) correlation distribution of plain image along vertical direction (c) Correlation of plain image along diagonal direction (d) Correlation distribution of encrypted image along Horizontal direction (e) Correlation distribution of encrypted image along Vertical direction (f) Correlation distribution of encrypted image along Diagonal direction

4 Conclusion

In this work we have studied a robust secure technique of image transmission over an AWGN channel. This is implemented with reduced distortion, delay and complexity providing an analogous data transmission with a literate choice of optimized mapping structure. A 2:1 dimension compression mapping is performed based on Shannon Kotelnikovs mapping using the optimized mapping structure The concept define dimension reduced mapping scheme with a 0.5 compression rate using Shannon Kotelnikovs mapping provide an additional security to the image information mapping on to a lower dimension. The reconstruction accuracy with codebook found to be better than that of image reconstructed tolerating Approximation error. Furthermore the compressed image elements are randomized using the vigenere pseudo random matrix based permutation approach in various rounds of operation until the correlation between them is obtained to be very low. Security analysis of the proposed system is proven to resist brute force and other possible attack with a choice of maximum key size and a larger number of rounds of encryption algorithm.

References

1. Eduardo Alves Hodgson, Glauber Brante, Richard Demo Souza, Javier Garca-Fras, and Joo Luiz Rebelatto, *Compensating Spectral Efficiency Loss of Wireless RF Energy Transfer With Analog Joint Source Channel Coding Compression* , IEEE sensors journal, VOL. 16, NO. 16, 2016.
2. C.E Shannon, *A mathematical theory of communication*, Bell syst. techn. J., vol.7, pp.379-423, 1948.
3. P. A. Floor and T. A. Ramstad, *Dimension reducing mappings in joint source-channel coding*, in Proc. 7th Nordic Signal Process. Symp. (NORSIG), pp. 282–285. 2006.
4. P. A. Floor and T. A. Ramstad, *Noise analysis for dimension expanding mappings in source-channel coding,* in Proc. IEEE 7th Workshop Signal Process. Adv. Wireless Commun. (SPAWC), Jul. 2006, pp. 15.
5. O. Fresnedo, F. J. Vazquez-Araujo, L. Castedo, and J. Garcia-Frias, *Low-complexity near-optimal decoding for analog joint source channe coding using space-filling curves,* IEEE Commun. Lett., vol. 17, no. 4, pp. 745748,2013.
6. Oscar Fresendo, Jose P.Gonzalez-Coma, Mohamed Hassanin, Luis Castedo, Javeir Gracia-Frias, *Evaluation of analog joint Source Channel Coding System for Multiple Access Channels* .vol 63.No 6. 2015.
7. F. Hekland, P. A. Floor, and T. A. Ramstad, *Shannon-Kotelnikov mappings in joint source-channel coding*, IEEE Trans. Commun., vol. 57, no. 1, pp. 94105, Jan. 2009.
8. Y. Hu, J. Garcia-Frias, and M. Lamarca, *Analog joint source-channel coding using non-linear curves and MMSE decoding*, IEEE Trans. Commun., vol. 59, no. 11, pp. 30163026, Nov. 2011.
9. O. Fresnedo, F. J. Vazquez-Araujo, J. Garcia-Frias, M. Gonzalez-Lopez, and L. Castedo, *Comparison between analog joint source-channel coded and digital BICM systems,* in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 15.
10. A. Fuldseth and T. A. Ramstad, *Bandwidth compression for continuous-amplitude channels based on vector approximation to a continuous subset of the source signal space*,” in Proc. ICASSP, Apr. 1997.
11. Yichuan Hu and Javier Gracia-Frias, Meritxell Lamarca, *Analog Joint Source Channel Coding Using Space filling curves and MMSE decoding*”, IEEE Computer society Data Compression Conference 2009.
12. V. A. Kotelnikov, “*The Theory of Optimum Noise Immunity*”. New York: McGraw-Hill Book Company, Inc,1959
13. Padmapriya Praveenkumar, Rengarajan Amritharajan, Karuppuswamy Thenmozhi, John Bosco Balaguru Rayappan, *Fusion of Confusion and diffusion :A novel image encryption approach”*. Telecommun Syst (2017). DOI 10.1007/s11235-016-0212-0.

14. Hussain, I.,Shah T.,&Asif Gondal, M.(2012). Cryptanalyzing a chos-based on S8 S-box transformation ans NCA map. Optics communication, 285(24), 4887-4890.doi:10.1016/j.optcom.2012.06.001
15. Praveenkumar, P., amritharajan, R., thenmozhi K.,& rayapan J.B.B (2015).”*Pixel Scattering matrix formalism for image encryption- A key scheduled substitution and diffusion Approch”* (2015) AEU-International journal of Electronics and Comunication,69(2),562-572.
16. Yichuan Hu and Javier Gracia-Frias, Meritxell Lamarca, *Analog Joint Source Channel Coding Using non linear curves and MMSE decoding*, IEEE transaction on communication vol.59.,No.11,Nov 2011.
17. C. E. Shannon, *Communication in the presence of noise,*” Proc. IRE, vol. 37, pp. 10-21, Jan.1949.
18. V. A. Kotelnikov, *The Theory of Optimum Noise Immunity*. McGrawHill, 1959.
19. V. Vaishampayan, *Combined source-channel coding for bandlimited waveform channels,”* Ph.D. dissertation, University of Maryland, College Park, 1989
20. S.-Y. Chung, *On the construction of some capacity-approaching coding schemes,”* Ph.D. dissertation, Dept. EECS, Massachusetts Institute of Technology, 2000.
21. T. A. Ramstad, *Shannon mappings for robust communication,”* Telektronikk, vol. 98, no. 1, pp. 114-128, 2002.
22. F. Hekland, G. E. Oien, and T. A. Ramstad, *Using 2:1 Shannon mapping for joint source- channel coding,”* in Proc. DCC, Mar. 2005.
23. F. Hekland, P. A. Floor, and T. A. Ramstad, *Shannon-Kotelnikov mappings in joint source-channel coding,*” IEEE Trans. Commun., vol. 57, no. 1, pp. 95-104, Jan. 2009.
24. N. Wernersson, M. Skoglund, and T. Ramstad, *Polynomial based analog source-channel codes,”* IEEE Trans. Commun., vol. 57, no. 9, pp. 2600-2606, Sep. 2009.
25. Shrija somaraj, mohammed Ali Hussain.,Performance and Security Analysis for Image Encryption For key Image., Indian journal of science and Technology, vol8(35), DOI:10.17485/ijst/2015/v8i35/73141.
26. *William Stalling, “Cryptology and Network Security”* 4th edition Pearson Education.
27. Shu Lin and Daniel j Costello *Error Control Coding* 2nd Edition, Pearson.