Turbo Product Coding and Encryption Technique for Image Transmission

Anita Lahane
Thakur College of Engg and Technology, Mumbai, India

Dr. B. K Mishra
Thakur College of Engg and Technology, Mumbai, India
Prof. Zahir Aalam
Thakur College of Engg and Technology, Mumbai, India

Abstract

In wireless networks secure transmission strategy for high-quality image is considered a great challenge. However, majority of encrypted image transmission schemes do not consider well the effect of bit errors occurring during transmission and this issue is considered a problem that should be handled by an efficient coding scheme. In this, a modified wireless image transmission scheme that combines chaotic encryption and turbo product coding technique into one processing step is proposed. In the proposed scheme, selective encryption algorithm based on two-dimensional chaotic map is utilized for data security. Furthermore, error correction technique based on turbo product coding is employed as channel coding for data communication in order to solve the problem of limited bandwidth and throughput. The proposed scheme can achieve high degree of robustness against channel impairments and improve image quality with acceptable data rates.

1. Introduction

Encryption and Error control coding (ECC) are important issue in image transmission. ECC are used to protect data from channel errors. In the literature, ECC can be classified into two categories: convolutional codes and linear block codes. Generally, the encryption of images can be applied in special domain or in frequency domain. Spatial domain schemes are mainly related to the position of the pixels in the image. Encryption in spatial domain does not satisfy the securityapplication because they cannot survive most image processing attacks and geometric attacks [1].

In the other hand, frequency domain schemes deal with the digital transformation of the image and therefore can resist the image processing attacks [2]. An example of frequency transform is wavelet transforms, which have several properties that make them good candidates. First, the approximation coefficients provide a good low-resolution estimate of the image, while minimizing aliasing artefacts resulting from the reduction in resolution. Second, the wavelet coefficients are localized, so a corruption of a coefficient through channel errors has only local effect on the image [8]. Traditionally, error correction and encryption in communication networks have been addressed independently [4]. Several researchers have studied the trade-off between encryption and error correction by trying to combine these functionalities in one unit.

2. Related Work

M.A. El-Iskandarani , Saad Darwish, Saad M. Abuguba, proposed a scheme in which it is used to build a secure and reliable image transmission scheme that combine turbo coding based on error correction code and 2D chaotic map based encryption functionality into one single step in order to reduce the overall processing cost. The advantages of this scheme are achieving better security by utilizing 2D chaotic map instead of 1D chaotic map used by and improving the throughput of an image transmission system by using turbo coding. [1] M.A. El-Iskandarani , Saad Darwish, Saad M. Abuguba, proposed scheme has larger key space. It can resist differential attack, plaintext attack, chosen text known attacks and various brute-force attacks. The proposed scheme is suggested for secure image communication over wireless channels. From the results, it is concluded that the scheme is very effective for secure image communication over wireless noisy channels.[2] C. Nanjunda, M. A. Haleem and R. Chandramouli, robust encryption for secure image transmission over wireless channels this paper shows that encryption based on wireless channel states could

lead to significant gains in the throughput achieved for a specified security constraint. It considered the cases where the channel is exactly known for a finite horizon and only the average and the distribution of the channel SNR is known. For the case where assume exact channel knowledge and continuous encryption block length we get an improvement of 95% (around 5dB SNR) in the throughput over fixed block length encryption.[3] James E. Fowler and B´eatrice Pesquet-Popescu, they have surveyed a number of salient examples of the use of wavelets in source coding, communications, and networking, and the papers that follow in this special issues. However, by no means exhaustively covered all the image and video applications that have been impacted by wavelets and wavelet theory. Indeed, anticipate that wavelets will remain firmly entrenched in widespread applications in image and video processing for some time to come.**[4]** Hakan CAM Volkan OZDURAN Osman N. UCAN, introduced a new type of Encryption and Error Correction scheme, which is called "A Combined Encryption and Turbo Coding Scheme: AES-TURBO". Although in previous studies error correction and encryption are handled independently, it combined error correction and Encryption functionality into one single step. This combined System's performances are evaluated in AWGN (Additive White Gaussian Noise) channel type. The results are compared with the system employing ideal encryption and decryption.[5] Kamel Faraoun, Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption, it proposed an n-ary key stream generator, based on hierarchical combination of three chaotic maps. It demonstrate that the produced key streams have good statistical properties, such as uniform distribution, δ-like auto-correlation function, near-zero cross-correlation and
very height sensitivity to initial conditions, under precision restricted condition. An image cryptosystem is constructed using the proposed approach and proven to be enough secure to resist various attacks. Complexity is analysed and an effective acceleration of chaos-based image cryptosystems is shown to be achievable [6] N.K. Pareek,Vinod Patidar , K.K. Sud, image encryption using chaotic logistic map,proposed a new way of image encryption scheme which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both the logistic maps are derived using the external secret key by providing weightage to its bits corresponding to their position in the key. In this , eight different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the logistic map. To make the cipher more robust against any attack, the secret key is modified after encrypting a block of sixteen pixels of the image. statistical analysis, key sensitivity analysis and key It gives space analysis to demonstrate the security of the new image encryption procedure. [7] R. Hasimoto-Beltr´an**,** proposed a secure low-complexity encryption system based on a *4-array* of independently iterated chaotic logistic maps with a new *Spatiotemporal* feedback scheme as a diffusion process. The robustness of the system to opponents' attack is enhanced by using a periodic three-level pseudo-random perturbation scheme, one at the system-key level and two at the map array level. [8] John Justin M, Manimurgan **S,** it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.[9].

3. Methodology
Turbo Product Code

Recently, the progress of error correcting codes is very great, many codes with excellent performances have been presented such as turbo codes , turbo product codes (TPCs) and low-density parity check (LDPC)codes . Among them, TPCs based on linear block codes have low complexity in encoding and decoding. They are constructed with short linear block codes. Turbo product codes (TPCs) are high performance error-correction codes which employ iterative algorithms for decoding .Turbo product codes (TPC), also known as block turbo codes, are built from two-, three-, or multi-dimensional array of block codes. In general, the larger the dimension, the higher the TPC complexity Efficient communication systems are systems that permit a high rate of information to be communicated with the lowest possible power. One type of code that has tremendous potential is the turbo product code. Turbo product codes have been found to improve power efficiency and maximize the rate of data transmission.Turbo product codes are error-correction codes that offer a wide range of tradeoffs in performance, complexity, and code rate. While they have some similarities to turbo-concatenated codes that have been incorporated into recent standards for future cellular communication, turbo product codes have different structure and characteristics. Turbo product codes are built from product block codes (e.g., pair of extended Hamming codes). Their performance can be within 1 dB of the Shannon limit.Turbo product codes have different structure and characteristics. Turbo product codes are built from product block codes (e.g., pair of extended Hamming codes). Their performance can be within 1 dB of t Concatenation of two block codes Principle of "iterative soft-input/soft-output (SISO)" decoding applied in a phased manner.TPCs are built on 2 or 3 dimensional arrays of hamming codes or BCH codes. Wide range of code rates and block sizes.

Turbo Product Code Construction:

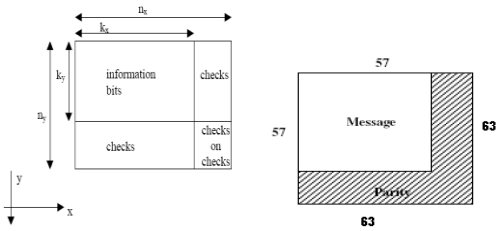

Figure:3.1 Two Dimensional Turbo Product Code

A turbo product code is a relatively large code built from smaller code word blocks

Turbo Product Code Decoding:

In the procession of decoding, the Chase algorithm is applied on the rows/columns of a product code in order to obtain extrinsic soft information for each bit position. This information is then passed to the next stage of an iterative decoder.The decoding of a turbo product code is performed one block at a time using iterative decoding.The horizontal blocks are decoded first and then all of the vertical blocks are decoded. Iteration can be done several times to reduce the probability of error. Optimal iterative decoding requires soft-decision decoding. This is based on a soft-decision metric, which is a measure of the likelihood or confidence that the decoder has in each of the bits in the received block. Each decoding iteration builds on the previous decoding performance. Many decoders use the soft in soft out Viterbi algorithm , but there are also other alternatives.

Discrete Wavelet Transform

Wavelet Transform has become an important method for image compression. Wavelet based coding provides substantial improvement in picture quality at high compression ratios mainly due to better energy compaction property of wavelet transforms [8]. Wavelets are functions which allow data analysis of signals or images, according to scales or resolutions. comparing the results of different transform coding techniques i.e. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) we see that DWT provides higher compression ratios & avoids blocking artifacts. Allows good localization both in spatial & frequency domain. Transformation of the whole image introduces inherent scaling. Better identification of which data is relevant to human perception higher compression ratio and we also see that DCT takes more time than DWT.Discrete wavelet transform (DWT) is becoming popular in many image/video applications due to its multi-resolution representation feature. The DWT represents an image as a sum of wavelet functions, known as *wavelets*, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2.The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient [9]. This procedure is one dimensional (1-D) DWT.but in this research work we are using two dimensional (2-D) DWT. The basic idea of the DWT for a two-dimensional image is described as illustrated in figure 3.2 With the pyramid-structured wavelet transform, the original image will encounter different combinations of a low pass filter and a high pass filter and then based on the convolution with these filters to generate the low-low (LL), low-high (LH), high-low (HL) and high-high (HH) sub-bands [10]. The most of the previous works for DWT [9,10] noticed that with only LL4, a large amount of image information can be extracted, but encrypting only LL4 may reveal higher frequency information such as edge components and it can be used to infer useful information.In case of in two directions, both rows and columns. The outputs are then down sampled by 2 in each direction as in case of 1-D DWT [8]. Output is obtained in set of four coefficients LL, HL, LH 2-D DWT, the input data is passed through set of both low pass and high pass filter and HH. The first alphabet represents the transform in row where as the second alphabet represents transform in column. The alphabet L means low pass signal and H means high pass signal. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively [10].

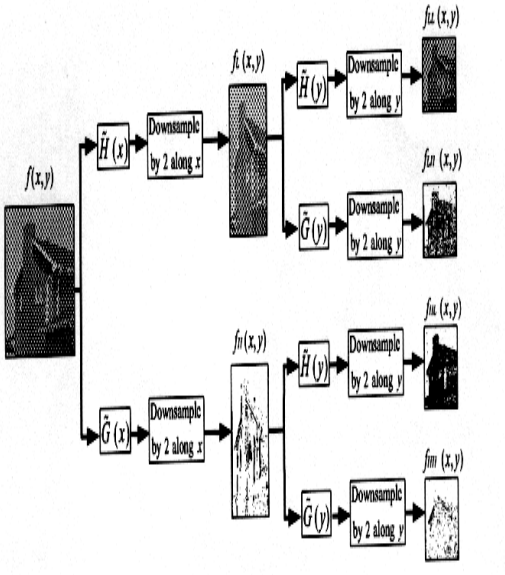

Fig 3.2 2D-Discrete Wavelet Transform

Chaotic Encryption Technique

The systematic procedure of the proposed image encryption as well as decryption process using two chaotic logistic maps. The basic logistic map is formulated as:

$$X_n+1 = \mu X_n (1-X_n)$$

where μ represents the parameter of chaotic map. To satisfy the best encryption, i.e. chaotic sequence is unpredictable, μ must lies between $3.569 < \mu < 4.0$ [14], consequently the chaotic encryption and decryption provides guaranteed high security. The encryption using chaotic sequence produced by 1-D logistic system is known to be weak in security, since it cannot resist known/chosen-plaintext attacks. More information about the implementation of 1-D chaotic map can be found in [11,12]. In order to deal with the problem of 1-D chaotic map, proposed scheme utilizes 2-D chaotic logistic map shown in figure 3.3

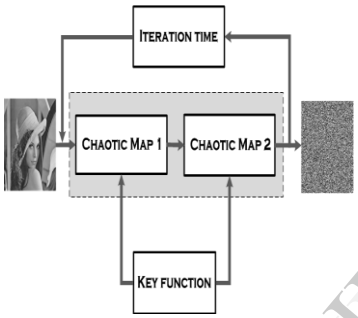

Fig 3.3 : Two dimensional chaotic Image encryption

4. Proposed System Architecture

Multimedia wireless applications have become very popular mainly due to the advances of wireless technologies that are now able to offer high data rates. Majority of encrypted image transmission schemes do not consider well the effect of bit errors occured during transmission and is considered a problem that can be handled by an efficient coding scheme and also efficient encryption technique**.** Secure transmission strategy for high quality image through wireless networks is considered as a great challenge. So, a wireless image transmission scheme that combines encryption and turbo product coding technique into one processing step can be used. The main aim is to build a secure and reliable image transmission scheme that combine turbo product coding based on error correction code and 2D chaotic map based encryption functionality into one single step in order to reduce the overall processing cost. The advantages of scheme are achieving better security by utilizing 2D chaotic map instead of 1D chaotic map used by [1] and improving the throughput of an image transmission system by using turbo product coding. The systematic block diagram of the proposed scheme is shown below.

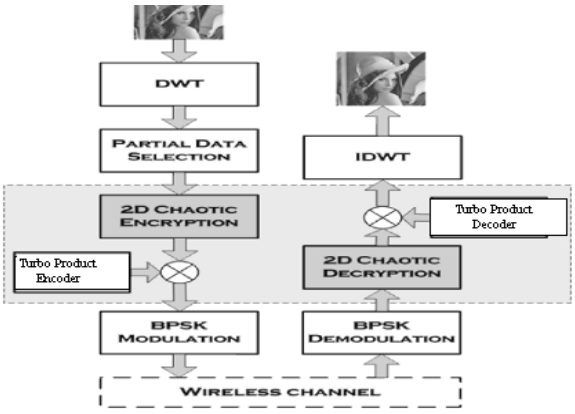

Fig 4.1: Block diagram of Proposed Scheme

5. Expected Results

The performance of the combination between 2-D chaotic encryption and turbo product coding on image transmission through wireless channels will be studied using Histogram of encrypted images An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level. We will analyze the histogram of the several encrypted as well as its original image.Image quality measurement will be done using the Peak signal to noise ratio(PSNR).The bit error rate(BER**)** performance of overall system will be investigated after decoding,as a function of signal to noise ratio Eb/N0 where Eb is the energy received per information bit and N0 is the noise power spectral density.A combination of image encryption based on 2D chaotic map and error correction code based on turbo product coding proposed in a unified framework for secure image communication over wireless channels. In this scheme, two-dimensional chaotic map is utilized for data security. Furthermore turbo product coding is employed as channel coding for data communication in order to solve the problem of limited bandwidth and throughput, to reduce overall processing cost, achieving better security, improving the throughput and improve the image quality with acceptable data rates.

References

[1] M.A.El-Iskandarani, Saad Darwish, Saad M. Abuguba, IEEE 2009 "Reliable Wireless Error Correction Technique for Secure Image Transmission".

[2] M.A.El-Iskandarani, Saad Darwish, Saad M. Abuguba November 2010 "Combination of 2D Chaotic Encryption and Turbo coding for secure Image Transmission", IJCSNS International Journal of Computer Science and Network Security,Vol.10 No.11

[3] J. Fowler and B. Popescu, April 2007 "An Overview on Wavelets in Source Coding, Communications, and Networks," EURASIP Journal on Image and Video Processing, Vol. 2007, pp. 1-27.

[4] H. Cam, V. Ozduran and O. Ucan, Feb.2004 "A combined encryption and error correction scheme: AES-Turbo", Journal of electrical & electronics engineering, vol.1, 2009, pp.861-866.

[5] K.Deergha and K.Sudha, "Chaotic image encryption and decryption –A comparative study", Conference on Systemics, Cybernetics and Informatics, Hyderabad, pp.433-438, 12-15.

[6] C.Nanjunda,M.Haleem, R.Chandramouli,May 2005,"Robust Encryption for Secure Image Transmission over wireless channels", IEEE ICC Conference Record,pp.287-1291,Korea.

[7] J.Fowler and B.Popescu, 2008, "An Overview on Wavelets in Source coding, Communication and Networks", Proceedings of the 4th International Industrial Simulation Conference., Palermo, pp. 125-132.

[8] Seo Y., Kim D., Yoo J., Dey S. and A. Agrawal, May 2003 "Wavelet domain in image encryption by Subband selection and data bit selection", World Wireless Congress(3G Wireless) Conference Record, pp.1-6.

[9] A. Pommer and A. Uhl, 2002 "Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data", IEEE Benerux Signal Processing Symposium, pp. 25-28

[10] G.Sheng and G.Qiang,October 2006 "The application of Chaos and DWT in image scrambling," IEEE, Informatica vol.31, pp. 3729–3733.

[11] Kamel Faraoun, July2010"Chaos-based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption",International Arab Journal of Information Technology,Vol.7,No.3.

[12] N.K.Pareek, Vinod Patidar,K.K.Sud,2006 "Image Encryption using Chaotic Logistic Map",Image and Vision Computing 24(2006)926-934

[13] R.Hasimoto-Beltran,"Low-Complexity Chaotic Encryption System", Revista Mexicann De Fisica 53(1) 58-65,Feb.2007

[14] D.Gligoroski,S.Knapskog,andS.Andova,June 2006 Cryptocoding- Encryption and Error Correcting Coding in a Single Step," International Conference on Security and Management,pp.1-7.

[15] John Justin M,March2012 ," A Survey on Various Encryption Techniques," International Journal of Soft Computing Engineering(IJSCE),ISSN:2231,Volume2,ISSUE1.

[16] Jessica Pursley,"Turbo Product Codes and Channel Capacity,",Clemson University,Region3 IEEE