IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. I (May-Jun. 2014), PP 39-45
www.iosrjournals.org

Image Security With Different Techniques Of Cryptography And Coding: A Survey

Mona F. M. Mursi[1], Hossam Eldin H. Ahmed[2], Fathi E. Abd El-samie[3], Ayman H. Abd El-aziem[4]

[1]*Professor, Dept. Of Electrical Engineering Shubra Faculty of Engineering Benha University, Egypt.*
[2]*Dept. Of Electronics Comm. Eng. P. Dean of the Faculty of Electronic Eng. Menouf-32952, Menufiya University, Egypt.*
[3]*Assoc. Prof. Dept. of Electronics& Comm. Eng. Faculty of Electronic Eng - Menufiya University. Egypt.*
[4]*Ph.D Student, Dept. Of Electrical Engineering, Shubra Faculty of Engineering, Benha University, Egypt.*

Abstract: *Due to the growth of multimedia applications, the protection of this multimedia data becomes a very important issue of communication and storage; especially when it is transferred over an insecure channel, where apart from preventing illegal data access, images are used in many fields such as medical science and military. The protection of images can be done with image encryption. The majority of encrypted image transmission schemes does not adequately take into account the effect of bit errors occurring during transmission and this issue is considered a problem that should be handled by an efficient coding scheme. Hence, error correction code should be applied after encryption to protect encrypted images against channel errors. In this paper, we present a survey of image encryption techniques and channel coding techniques.*
Keywords: *Image Encryption, Channel coding, chaotic theory.*

I. Introduction

Image encryption techniques try to convert the original image to another image that is hard to understand. There are two main types of cryptography: Secret key cryptography and public key cryptography. In secret key cryptography both the sender and the receiver know the same secret code, but public key cryptography, uses a pair of keys for encryption and decryption.

Encryption algorithms can be classified with respect to the mode of operation of the algorithms: block or stream cipher. A block cipher is a type of symmetric key encryption algorithm that transforms a fixed length of plaintext data into a block of ciphertext data of the same length, stream ciphers typically operate on smaller units of plain text, usually bits. A block cipher may also be divided into two groups: chaos and non-chaos based methods. Moreover, it can be further divided into full encryption and partial encryption according to the percentage of the data encrypted. Finally it can be classified into compression and non-compression methods [1].

Traditional encryption algorithms such as AES, RSA and IDEA are used in text or binary data. It is difficult to use them for image encryption because of the high correlation among pixels, high redundancy, bulk capacity of data, so that these algorithms are not suitable for real-time application [2].

Chaos theory has properties of deterministic nonlinear systems that exhibit sensitivity to initial conditions and have random like behaviors. Many researchers have noticed that there exists the close relationship between chaos and cryptography [4].

Chaotic maps and cryptographic algorithms have some similar properties as sensitivity to tiny changes in initial conditions and parameters, both have random-like behavior. There are two differences in characteristics between cryptography and chaos; in cryptography, the encryption operations are defined on finite sets of integers while chaos is defined on real numbers; cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic via iterations [4]. There are two general principles that guide the design of block ciphers; diffusion and confusion, which are closely related to the mixing and ergodicity properties of chaotic maps.

Hence we can use a chaotic map in image encryption because it satisfies the requirements of a good cryptosystem [5-7].

In this paper we present a survey of the security of images using chaotic map and the channel coding techniques. The rest of the paper is organized as follows: In section2 we describe some image encryption schemes. Section 3 presents channel coding technique, Section 4 present relations between coding and encryption. Finally, the conclusions of the paper are presented in section 5.

II. Some Image Encryption Schemes

We introduce a brief description of the various techniques used for image encryption.

A new encryption algorithm based on using the chaotic logistic map produced pseudo random sequence on image and makes double time encryption with improved DES. The combination of Chaos and improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption [8].

A new image encryption scheme based on a chaotic system is presented in [8]. It is based on power and the tangent function instead of linear function. It uses a chaotic sequence generated by chaotic map to encrypt image data with different keys for different images. Plain-image can be encrypted by the use of the XOR operation with the integer r sequence.

A block based transformation algorithm is used in [9], where the image is divided into a number of blocks. These blocks are transformed before going through an encryption process. It uses blowfish algorithm for encryption. At the receiver side these blocks are retransformed into their original position and decryption process is performed. It has the advantage of no loss of information in reconstruction of image for the encryption and decryption process.

An algorithm using two chaotic systems is in [10]. One chaotic system generates a chaotic sequence, which was changed into a binary stream using a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, using the binary stream as a key stream, random the pixel values of the images were modified. Then, the modified image was encrypted again by a permutation matrix.

In [13], two kinds of schemes based on higher dimensional chaotic maps are presented. By using a discretized chaotic map, pixels in an image are permuted in shuffling after several rounds of operations between every two adjacent rounds of permutations, a diffusion process is performed, which can significantly change the distribution of the image histogram which makes statistical attack infeasible.

Image encryption scheme utilizes the SCAN language to encrypt and compress an image simultaneously in [14].Fridrich [15] demonstrated the construction of a symmetric block encryption technique based on two-dimensional standard Baker map. There are three basic steps in the method of Fridrich

- Choose a chaotic map and generalize it by introducing some parameter.
- Discretize the chaotic map to a finite square lattice of points that represent pixels.
- Extend the discredited map to three dimensions and further composes it with a simple diffusion mechanism.

A chaotic Kolmogorov-flow-based image encryption technique was designed [16], in which whole image is taken as a single block and which is permuted through a key-controlled chaotic system. In addition, a shift registers pseudo random generator is also adopted to introduce the confusion in the data.

An encryption method called BRIE based on the chaotic logistic map is presented in [17]. The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map.

An encryption method called CKBA (Chaotic Key Based Algorithm) [18], in which a binary sequence as a key is generated using a chaotic system. The image pixels are rearranged according to the generated binary sequence and then XORed and XNORed with the selected key.

An image encryption algorithm using logistic map in [3], uses a chaotic map with suitable initial condition for varying the pixel values randomly with respect to its initial values of the original image. Next the chaotic sequences of the logistic map are used for pixel shuffling. The algorithm uses a secret key of 32 characters (256-bits).

A chaos-based image encryption scheme was introduced in [20]. An image is first converted to a binary data stream by masking these data with a random keystream generated by the chaos-based PRKG, the corresponding encrypted image is formed.

In most of the previous algorithms a security analysis is made; such as key space analysis, statistical analysis and differential analysis. A comparison between original image and encrypted image in terms of correlation between the initial and transformed images, number of pixels change rate and unified average changing intensity are also performed.

III. Channel Coding Theory

The goal of any communication system is to transmit information from an information source to a destination via a communication channel. There are many factors that cause the output of a communication channel to be different from its input. Among these factors are attenuation, nonlinearities, bandwidth limitations, multipath propagation and noise [13].

The main objective when transmitting information over any communication channel is reliability, which is measured by the probability of correct reception at the receiver.

3.1 Channel Capacity

Entropy H (X) defines a fundamental limit on the rate at which a discrete source can be encoded without errors in its reconstruction. A fundamental result of information theory is that reliable transmission is possible even over noisy channels as long as the transmission rate is less than the channel capacity [21]**.** The capacity of a discrete memoryless channel is given by

$$C = \max p(x)\, I(X; Y) \quad (1)$$

Where I (X; Y) is the mutual information between the channel input X and the output Y, If the transmission rate R is less than C, then for any $\delta > 0$ there exists a code with block length n large enough whose error probability is less than δ. If R >C, the error probability of any code with any block length is bounded away from 0. The communication channel is characterized by a number called capacity that determines how much information can be transmitted over it [23].

3.2 Bounds On Communication

The capacity of an additive white Gaussian noise channel is given by

$$c = W * \log X \left(1 + \frac{p}{X * W}\right) \quad (2)$$

The basic factors that determine the channel capacity are the channel bandwidth W, the noise power spectrum No and the signal power P. There exists a trade-off between P and W in the sense that one can compensate for the other. Increasing the input signal power obviously increases the channel capacity, because when one has more power to spend, one can choose a larger number of input levels that are far apart and, therefore, more information bits/transmission are possible.

3.3 Channel Coding Techniques

Channel coding techniques are divided into two main types; block codes and convolution codes. In a block code, the information sequence is broken into blocks of length k and each block is mapped into channel inputs of length n. This mapping is independent from the previous blocks. In convolutional codes, there exists a shift register. The information bits enter the shift register bits at a time and then output bits which are linear combinations of various shift register bits are transmitted over the channel. The main difference between block codes and convolutional codes is the existence of memory in convolutional codes.

3.3.1 Linear Block Codes

A block code is completely defined by(n, k),$M = 2^k$ binary sequences of length n called code words. A code C consists of M code words Ci for $1 \leq i \leq 2^k$.

C = {c1, c2, . . . ,cM}

where each Ci is a sequence of length n with components equal to 0 or 1 and it denoted by.

$$C = X \times G \quad (3)$$

Where g is the generator and the parity check matrix, the generator matrix of a code completely describes the code. If we denote the generator matrix of the dual code by H, which is an $(n - k) \times n$ matrix, then any code word of the original code is orthogonal to all rows of H.

$$C.H^t = 0 \quad (4)$$

Soft decision decoding is used for decoding information as follow after receiving the output of the channel and passing it through the matched filters, we choose one of the message signals that is closest to the received signal in the Euclidean distance sense. These are bounds on the error probability of a coded communication system when optimal demodulation is employed. By optimal demodulation, we mean passing the received signal r (t) through a bank of matched filters to obtain the received vector **r**, and then finding the closest point in the constellation to **r** in the Euclidean distance sense.

Hard decision decoding is simpler and more frequently used decoding scheme to make hard binary decisions on the components of the received vector **r**, and then to find the code word that is closest to it in the Hamming distance sense. There are three basic steps involved in hard-decision decoding. First, we perform demodulation by passing the received r (t) through the matched filters and sampling the output to obtain the **r** vector. Second, we compare the components of **r** with the thresholds and quantize each component to one of the two levels to obtain the **y** vector. Finally, we perform decoding by finding the code word that is closest to **y** in the Hamming distance sense.

3.3.2 Cyclic Codes

Cyclic codes are a subset of linear block codes with the extra condition; it is easily implementable encoders and decoders. A cyclic code is a linear block code that if **C** is a code word, a cyclic shift of it is also a code word. It is easier to represent each codeword as a polynomial, called the code word polynomial. The code word polynomial corresponding to

C=(c1, c2, . . . ,cn−1, cn) is simply defined to be

$c_i p_{n-i} = c_1\, p_{n-1} + c_2\, p_{n-2} + \cdots + c_{n-1}\, p + c_n$

And the code word polynomial corresponding to **x** is given by

$$C(p) = X(p) \times g(p). \qquad (7)$$

Any code word polynomial is the product of the generator polynomial and the information sequence polynomial, this fact is very important in designing cyclic encoders.

Cyclic codes have more built in structure and this extra structure makes the implementation of their encoders easier. The main advantage of cyclic codes is the existence of an easily implementable decoder for them.

3.3.3 Convolution Codes

Convolutional codes are different from the block codes by the existence of memory in the encoding scheme. In convolutional codes, each block of k bits is again mapped into a block of n bits to be transmitted over the channel, but these n bits are not only determined by the present k-information bits but also by the previous information bits.

Because a convolutional encoder has finite memory, it can easily be represented by a state-transition diagram as shown in figure 1.

In the state-transition diagram, each state of the convolutional encoder is represented by a box and transitions between states are denoted by lines connecting these boxes. On each line both the inputs causing that transition and the corresponding output are specified. The number of lines emerging from each state is, therefore, equal to the number of possible inputs to the encoder at that state

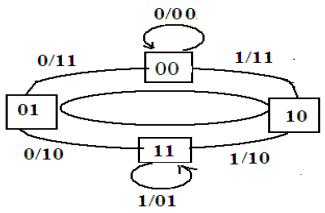

Fig1 State transition diagram for convolution code

The second and more popular method to describe convolutional codes is to specify their trellis diagram as shown in figure 2 . The trellis diagram is a way to show the transition between various states as the time evolves. The trellis diagram is obtained by specifying all states on a vertical axis and repeating this vertical axis along the time axis. Then, each transition from a state to another state is denoted by a line connecting the two states on two adjacent vertical axes. In a sense, the trellis diagram is nothing but a repetition of the state transition diagram along the time axes.

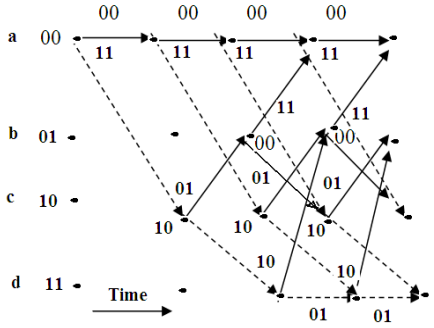

Fig 2. Trellis diagram for convolution code

3.3.4 Complex codes

The performance of block and convolutional codes depends on the distance properties of the code and, in particular, the minimum distance in block codes and the free distance in convolutional codes. In order to design block codes with a given rate and with high minimum distance, we have to increase n, but increasing n and increasing the constraint length will, increases the complexity of the decoding. We discuss two widely used methods for combining simple codes to generate more complex codes. These techniques generate product codes, and turbo codes.

Product Codes

The structure of product codes is very similar to a crossword puzzle as shown in figure 3.

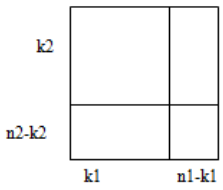

Fig 3.Product codes

Product codes are generated by using two linear block codes arranged in a matrix form. Two linear block codes, one with parameters n1, k1, d1 and another with parameters n2, k2, d 2, are used in a matrix of the resulting code is an (n1n2, k1k2) linear block code. It can be shown that the minimum distance of the resulting code is the product of the minimum distances of the component codes.
d = d1*d 2, and is capable of correcting d1* d2−1

This process can be repeated in an iterative fashion, improving the quality of the guess in each step. This process is known as iterative decoding and is very similar to the way a crossword puzzle is solved. To employ this decoding procedure, we need to decode schemes for the row and column codes that are capable of providing guesses about each individual bit. In other words, decoding schemes with soft outputs (usually, the likelihood values) are desirable.

Turbo Codes

Turbo codes use an interleaver between two parallel or serial encoders as shown in figure 4. The existence of the interleaver results in very large code word lengths with excellent performance, particularly at low SNRs. Using these codes, it is possible to get as close as 0.7 dB to the Shannon limit at low SNRs. The turbo encoder consists of two constituent codes separated by an interleaver of length N.

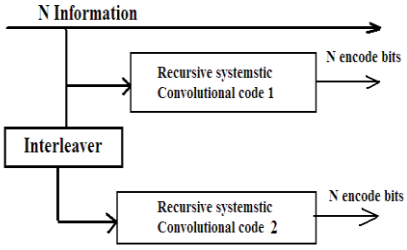

Fig 4. Block diagram of Turbo encoder

Because the encoders are systematic, each encoder generates the N-information bits applied to its input followed by N parity check bits. After the encoding, the N information bits and the 2N parity check bits of the two encoders, a total of 3N bits, are transmitted over the channel. Therefore, the overall rate is R = N/3N =1/3.
The interleaver in turbo codes is usually very long, in the order of thousands of bits. Pseudorandom interleavers perform well, although some improvement in the performance of the code can be obtained by clever choice of the interleaver. This improvement is more noticeable at short interleaver lengths. Due to the existence of the interleaver, it is, in most cases, impossible to return both codes to the all-zero state.

Since turbo codes have two constituents-code components, an iterative algorithm is appropriate for their decoding. Any decoding method that yields the likelihood of the bits as its output can be used in the iterative decoding scheme as shown in figure 4. One such decoding scheme is the maximum a posteriori (MAP) decoding method.

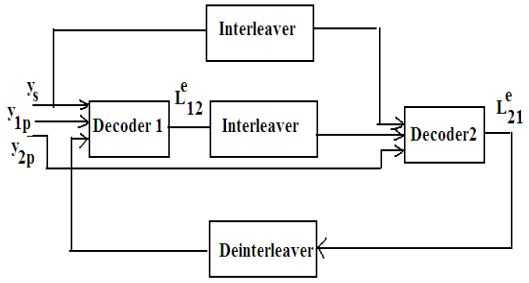

Fig 5. Block diagram of Turbo decoder

3.4 Bit error rate performance

The measure of that performance is usually bit-error rate (BER), which quantifies the reliability of the entire radio system from "bits in" to "bits out", including the electronics, antennas and signal path in between. On the surface, BER is defined as: BER = Errors/Total Number of Bits with a strong signal and an unperturbed signal path, this number is too small as to be insignificant. It becomes significant when we wish to maintain a sufficient signal-to-noise ratio in the presence of imperfect transmission through electronic circuitry.

The two performance parameters used are Message Error Rate MER and Bit Error Rate BER, MER define as = (No. of messages received in Error after error correction) / (Total no. of messages transmitted), Expressed as a percentage for a given signal to interference ratio.

While the basic concept of BER measurement is simple send a data stream through the system and compare the output to the input. However, we don't want to wait forever to make a BER measurement! So a pseudorandom data sequence is used for this test, some smart mathematicians have worked out sufficient approximations of random behavior so we can quickly make accurate BER measurements.

IV. Relation between Source coding and encryption

There is a relation between source and channel coding and encryption we introduce the combine of error correction code with encryption and the combine of compression and encryption as follow in sub sections.

4.1 Combine Encryption and Error Correction Code

While cryptographic algorithms, in order to provide information security, in the process of decryption need an errorless input, error-correcting algorithms are meant to handle a certain amount of errors in the input data, but they are not designed to provide any security of the data they process. However, there are many situations where both information security and error-correction are needed or required.

In this case a combination of cryptographic algorithms and error correction code introduces, called "A Combined Encryption and Turbo Coding which basically means encryption, decryption, encoding and decoding, is realized by AES-TURBO". AES was chosen for the encryption and decryption process, and turbo codes for encoding and decoding [12]. According to the general perspective of the system turbo encoder block is embedded in an AES encrypted block in the first round after subbytes block. The remaining steps of the AES encryption are followed normally. In the decryption phase turbo decoder block is embedded in an AES decryption block in the last round before Subbytes block.

Turbo codes mimic the good performance of random codes using an iterative decoding algorithm based on simple decoders individually matched to the simple constituent codes. The turbo decoder iterates between the outputs of the two constituent decoders until reaching satisfactory convergence. The final output is a hard-quantized version of the likelihood estimates of either of the decoders.

4.2 Combine Source and Channel Coding

Nowadays source compression and channel coding techniques are necessary for transmitting images efficiently [20], source coding is needed to remove as much redundancy as possible and to combat the errors introduced by noisy channels, channel coding is often employed to add controlled redundancy. Therefore, using characteristics of channels and compressed bit stream may be interested in practical systems. When transmitting progressively coded images, such as those encoded by set partitioning in hierarchical trees SPHIT or JPEG2000 that can provide efficient compression, over wireless channels. Due to its embedded property, the source bit stream is susceptible to transmit noise and sensitive to bit errors. Typically, a single error could render a whole bit stream useless. Thus it is important to combine source and channel coding to protect such bit stream over noisy channels. Given a particular source encoder, the key point lies in how to partition the limited total bit budget between source and channel coders such that the image distortion is minimized. We introduce a robust image transmission strategy over wireless channels by adding a coding controller between source code and channel coding, According to the characteristics of the channel and compressed bit stream, the coding controller dynamically allocates the coding rate for source code and channel coder.

Error protection with different coding rates. On the receiving side, the decoding controller extracts the important priority of the demodulated data.

4.3 Joint authentication and channel coding

We present a joint authentication, integrity verification and channel coding scheme, applied to secure image transmission through wireless networks and make it suitable for real-time image applications [6]. In noisy environments, channel coding has to be performed after encryption. Forward Error Correction (FEC) has to be specified in order to guarantee that the original messages can be properly deciphered and authenticated. A tight cooperation between channel coding and security mechanisms should be exploited to reduce the security overhead, to decrease the requested computational complexity, and to achieve the secrecy capacity limit. The

guarantees a strong resilience to the errors introduced by noisy channels, while providing the means to discriminate between data modifications performed by malicious attackers, and data distortions due to noise. Moreover, data encryption, performed before channel coding to prevent illegal data access, is also exploited to improve the performances of the scheme. The encoder employed to safely transmit an authenticated image over a noisy channel in the presence of a malicious opponent, and the decoder employed to receive the image and determine if it is original.

4.4 Combine Image-Encryption and Compression

A new and efficient method to develop secure image-encryption techniques may be realized by combining two techniques: encryption and compression. In this technique, a wavelet transform was used to decompose the image and decorrelate its pixels into approximation and detail components. The most important component is encrypted using a chaos-based encryption algorithm. The remaining components are compressed using a wavelet transform. This algorithm was verified to provide a high security level. This algorithm produces a good diffusion and confusion properties [19].

V. Conclusion

In this paper we presented a survey of some recent image encryption techniques and channel coding. We see that image encryption techniques using chaotic map give high security and a high rate of security and is suitable for real time applications. Each technique has advantages and the advantage depends on the design of these algorithms.

We find that it is not sufficient to secure the multimedia image by applying image encryption, especially when transmitting it over noisy channels.

It is necessary to apply channel coding after encryption. Forward Error Correction (FEC) has to protect the encrypted image from noise induced error, and make BER small as possible and close to the Shannon limit[11]. We introduced some different types of channel coding.

Also source coding as JPEG, JPEG2000 and SPHIT should be applied to the image to remove as much redundancy as possible before it is encrypted. There is a close relationship between channel coding and source coding; and security mechanisms should be exploited to increase the security of multimedia, and to decrease the requested computational complexity. These relations should be taken into consideration in the design to render high performance of security.

References:

[1] Komal D Patel, Sonal Belani "Image Encryption Using Different Techniques: A Review" International Journal of Emerging Technology and Advanced Engineering www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011).

[2] Varsha S. Nemade, R. B.Wagh "Review of different image encryption techniques" National Conference on Emerging Trends in Computer Technology (NCETCT-2012).

[3] Mrinal K. Manual, GourabD. Banik, DebasishChattopadhyay and DebashisNandi"An Image Encryption Process based on Chaotic Logistic Map " IETE Technical Review Vol 29 ISSUE 5 - SEP- OCT 2012.

[4] Yaobin Mao and Guanrong Chen" Chaos-Based Image Encryption"

[5] Shubo Liu, Jing Sun, ZhengquanXu"An Improved Image Encryption Algorithm Based on Chaotic System" 1100 Journal Of Computer, VOL. 4, NO. 11, November 2009.

[6] 6 Alessandro Ne., Daniele BL., Patrizio CA., and Emanuele Ma." Joint Authentication and forward Error Correction of Still Images "18th European Signal Processing Conference (EUSIPCO-201 Aalborg, Denmark, August 23-27, 2010.

[7] J. Fridrich. "Secure image ciphering based on chaos," Technical Report RL-TR-97-155, the Information Directorate (former Rome Laboratory) of the Air Force Research Laboratory, New York, USA, March 1997.

[8] Rajinder Kaur, Er. Kanwalprit Singh"Image Encryption Techniques: A Selected Review" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 80-83 www.iosrjournals.org

[9] A. Gautam, M. Panwar, Dr.P.R Gupta "A New Image Encryption Approach Using Block Based Transformation Algorithm" 2011 (IJAEST) Vol No. 8, Issue No. 1, 090 - 096 .

[10] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariy "A Survey On Different Image Encryption and Decryption Techniques."

[11] C.E. Shannon, A Mathematical Theory of Communication, Bell Sys. Tech. J., 27:379 {423, 623 {656, 194.

[12] Hakan Cam, Volkan O. Osman N. UCAN " A cobmnine Encryption and Error Correction Scheme: AES-TURBO" Journal of Electrical&Electronics Engineering, VOL 9 ,2009, (891-896) 05.01.2009.

[13] Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation and Chaos 8 (6): 1259 – 1284.

[14] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCANpattern, Pattern Recogn. 25 (1992) 567–581.

[15] Fridrich Jiri, "Symmetric ciphers based on two dimensional chaotic maps" Int. J. Bifurcat Chaos 8 (6) (1998) 1259–1284.

[16] J. Scharinger, "Fast encryption of image data using chaotic Kolmogrov flow", J. Electronic Eng 7 (2) (1998) 318–325.

[17] J.C. Yen, J.I. Guo, A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, 1999, pp. 430–437.

[18] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52.

[19] Somaya Al-Maadeed, 1 Afnan Al-Ali, 2 and Turki Abdalla" A New Chaos-Based Image-Encryption and Compression Algorithm "Journal of Electrical and Computer Engineering Volume 2012, Article ID 179693, 11 pages

[20] Daniel J. Costello, Jr. and G. David Forney, Jr" "Channel Coding: The Road to Channel Capacity" IEEE | Vol. 95, No. 6, June 2007.

[21] Jorge C. Moreira and Patrick G. Farrell. "Essential of Error Control Coding," John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,West Sussex PO19 8SQ, England. 2006.