Compression of Encrypted Images using Chaos Theory and SPIHT

Amrita Sengupta
Thakur College of Engg. & Tech.
Dept. of Electronics Engineering
Kandivali (E), Mumbai-400101

Sanjeev Ghosh
Thakur College of Engg. & Tech.
Dept. of Electronics & Telecommunication Engineering
Kandivali (E), Mumbai-400101

ABSTRACT

Importance to security in every application on internet is a clear motivation to contribute in the field of Information Security. Security is one of the most challenging aspects in the internet and network applications. When it is desired to transmit redundant data over an insecure and bandwidth-constrained channel, it is customary to first compress the data and then encrypt it. In this paper, reverse the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. Here, all through the use of coding with side information principles, this reversal of order is indeed possible without loss of either optimal coding efficiency or perfect secrecy. In addition to proving the theoretical feasibility of this reversal of operations, a system which implements compression of encrypted data is described. The image encryption technology based on chaos theory is used which have been developed to overcome the disadvantages present in traditional encryption techniques.
In this paper a chaotic based encryption technique followed by compression by SPIHT algorithm and their results are compared.

General Terms

Algorithms, Performance, Security.

Keywords

Image encryption, Chaos theory, SPIHT algorithm, Image decryption

1. INTRODUCTION

The security of sensitive documents depends on filing cabinets with a combination lock for storing paper-based files or documents due to the widespread use of data processing equipment,. However the scenario has changed with the introduction of computer in handling businesses in organizations. Considering the problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel it is desirable to both compress and encrypt the data. Due to the impact of globalization, vast amount of digital documents such as texts, images, videos, or audio travel from one point to another via internet. The conventional approach shown in Fig. 1 is to first compress the data to strip it of its redundancy followed by encryption of the compressed bit stream. The source is first compressed to its entropy rate using a standard source code. Then, the compressed source is encrypted using one of the many widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression
This paper, investigates by reversing the order of these steps, i.e., first encrypting and then compressing the encrypted source, as shown in Fig. 2. At the receiver, there is a decoder in which both decompression and decryption are performed in a joint step. Here the decoder can use the cryptographic key to assist in the decompression of the received bit stream leads to the possibility that we may be able to compress the encrypted source. A significant compression ratio can be achieved if compression is performed after encryption is shown. This is true for both lossless and lossy compression. In some cases, even the same compression ratio as in the standard case of first compressing and then encrypting can be achieved. The fact that we can still compress the encrypted source follows directly from distributed source-coding theory. When consider the case of lossless compression, use the SPIHT algorithm to show that the same compression gain as if we had compressed the original, unencrypted source can be achieved. For encryption technique use a hybrid chaotic encryption system. Since, the image encryption technology based on chaotic dynamics systems has been developed to overcome the disadvantages presented by traditional encryption algorithms. Inherent excellences of chaotic systems for security communications and information encryption, such as non-periodicity, randomness, turbulence, good statistic characteristic, easy regeneration, and wondrous sensitivity for initial values prove that discrete chaotic encryption techniques work very well with digital images providing a sufficient amount of security.. Different chaotic sequences can be produced with the different initial values of the systems. Therefore, the encrypting space is very wide.
The system discussed in this paper proposes a new image encryption technique based on chaos theory that combines the pros of the two systems discrete chaotic encryption technique based on Chebyshev chaotic sequences [3] and a chaotic encryption algorithm based on Logistic Map [4].
The second system discussed in the paper is SPIHT algorithm and the results for the same are also presented here.The rest of the paper is distributed as follows: Section 2 gives a brief idea about the characteristics of chaotic system and also introduces the two chaos based systems [3, 4] respectively along with the proposed encryption scheme. Section 3 discusses about the SPIHT .The simulation results and the comparative analysis of the system is given in sections 4 and 5 respectively. Section 6 deals with the security analysis and finally the paper concludes in section 7.

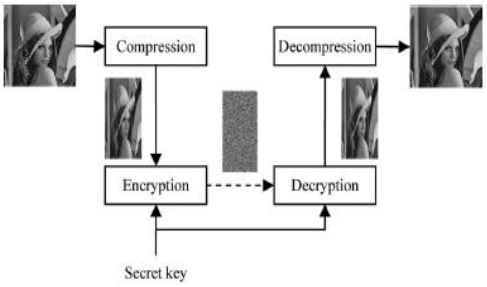

Figure1. Conventional Approach

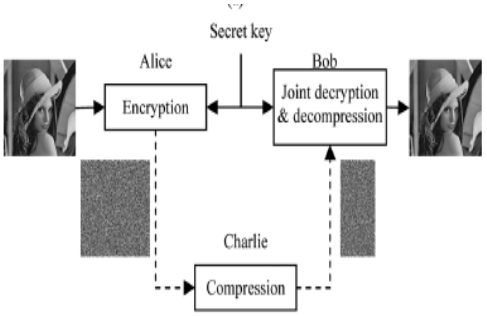

Figure 2. Practical Approach

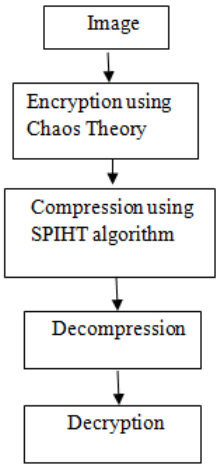

Figure 3. Flowchart

2. THE HYBRID TECHNIQUE BASED ON CHAOTIC ENCRYPTION TECHNIQUE

The hybrid technique combines the benefits provided by both systems mentioned above. The first system based on Chebyshev chaotic sequence, is relatively simple and hence the time taken for the encryption process is very less. Chaotic systems are very suitable for data message encryption because they have several good properties, for example, (a) chaotic motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain, namely the ergodicity of the chaotic orbit; (b) the flexing and collapsing are carried continually through the limited domain. Therefore the outputs of chaotic systems are very irregular, similar to the random noise; (c) because chaotic systems are extremely sensitive to their initial conditions, the movement of any two closed points can be separated in an exponent rule. The long-term movement trace of systems cannot be forecasted. These dynamics characteristics cause chaotic sequences to be wideband, pseudo-random, and unmasked hardly. Different chaotic sequences can be produced with the different initial values of the systems. Therefore, the encrypting space is very wide.

The Discrete Chaotic Encryption [3] proposed is based on Chebyshev chaotic sequences. Chebyshev mapping is a simple mapping, and the n rank Chebyshev mapping can be represented as:

$T_n(x) = \cos(n \arccos(x))$

It can be easily deduce

$Tn+1(x) = 2x\ Tn(x) - Tn-1 \quad (1)$

For $n \in N$, $n \geq 2$, and $x \in [-1,1]$, every $T_n(x)$ is chaotic [5,6].

The discrete sequences of the chaotic dynamical system are gained by the following equation

$X\ k+1 = Tn\ (xk) \quad (2)$

For n = 5, from Eq. (1) & Eq. (2), the following relationship is established

$$x_{k+1} = T_5(x_k) = 16x_k^5 - 20x_k^3 + 5x_k \quad (3)$$

Where $k = 0, 1, 2...$

Choosing any initial value x_0 in [-1, 1], a discrete Chebyshev chaotic sequence with any length $\{x_1 1, x_1 2, x_1 3, .. x_1 k, ...\}$ can be generated using Eq. (3).

The second system based on Logistic Map has two encryption stages. The first encryption stage uses a chaotic system that is based on the Logistic Map, but unlike the second system, the second encryption stage in the proposed system uses a discrete chaotic sequence based on Eq. (3).

The basic Logistic-map is formulated

$f(x) = ux(1-x)$

Where $x \in (0, 1)$. The parameter μ and the initial value x0 can be adopted as the system key (μ, x_0). The research result shows that the system is in chaos on condition that $3.569 < \mu < 4.0$ [7].

The encryption scheme is composed of two chaotic systems. One creates a binary stream and the other creates a permutation matrix P. First, the pixel values of the plain image are modified randomly using the binary stream by the traditional stream ciphers technology, namely bit-wise XOR operation. Then the modified image is encrypted again by matrix P.

The hybrid system as in the second system based on Logistic Map has two encryption stages. The first encryption stage uses a chaotic system that is based on the Logistic Map, but unlike the second system, the second encryption stage in the proposed system uses a discrete chaotic sequence based on Eq. (3). The key is denoted as $k = (k_1; k_2)$, where $k_1 = (\mu, x_{01})$ and $k_2 = (x_{02}, y_{02})$. The parameter μ is selected such that $3.569 < \mu < 4.0$ and $x_{01} \in (0, 1)$. The initial conditions x_{02} and y_{02} for the chaotic system of the second stage lie in [-1, 1]. Consider the plain image to be represented by A of size M x N, and A (i, j) stands for an individual pixel in the image.

The decrypting process is the reverse process of encrypting.

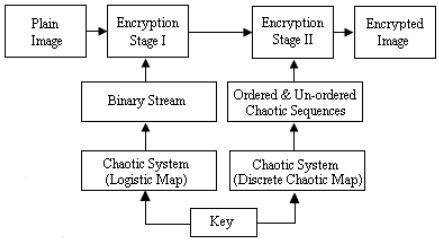

Figure 4. The hybrid encryption scheme

2.1 Generation of Binary Stream

The process for generating the binary stream mentioned in step 2 of section 5.1 above is as follows:

1. Generate a chaotic sequence using the sub-key k_1 as the initial conditions of the first chaotic system. i.e. $\{x_1, x_2, \ldots, x_{M*N}\}$
2. Generate a binary stream from the above chaotic system x_i by using a threshold function F. The threshold function F is as given below:

$$F(x) = \begin{cases} 00000000 & 0 \le x < \frac{1}{2^8} \\ 00000001 & \frac{1}{2^8} \le x < \frac{2}{2^8} \\ 00000010 & \frac{2}{2^8} \le x < \frac{3}{2^8} \\ \vdots & \\ 11111111 & \frac{255}{2^8} \le x < 1 \end{cases} \quad (5)$$

3. THE SET PARTITIONING IN HIERARCHICAL TREES (SPIHT) ALGORITHM

Set partitioning in hierarchical trees (SPIHT) is an image compression algorithm that exploits the inherent similarities across the subbands in a wavelet decomposition of an image.

The Inherent Characteristics of SPIHT algorithm is efficient, completely embedded, precise rate control and idempotent. simple and fast self-adaptive, supports

Images of 8, 16, or larger bit depth, images of unrestricted dimensions, progressive lossy to lossless compression, multiresolution encoding or decoding, modularity. Goals of SPIHT are to sort transform coefficients by msb, use transform characteristics to identify, efficiently groups with same msb, send remaining bits by order of importance first those identifying msb then those of same bit plane with larger msb's, Binary results of msb tests sent to decoder, enables decoder to duplicate encoder's execution path.

In the SPIHT algorithm, the image is first decomposed into a number of sub bands by means of hierarchical wavelet decomposition. For example, the sub bands obtained for a two-level decomposition are shown in Fig. 5. The sub band coefficients are then grouped into sets known as spatial-orientation trees, which efficiently exploit the correlation between the frequency bands. The coefficients in each spatial orientation tree are then progressively coded from the most significant bit-planes (MSB) to the least significant bit-planes (LSB), starting with the coefficients with the highest magnitude and at the lowest pyramid levels.

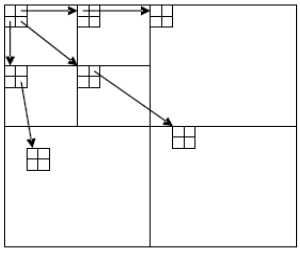

Figure 5. 2-level wavelet decomposition and spatial orientation tree

The SPIHT multistage encoding process employs three lists and sets:

1. The list of insignificant pixels (LIP) contains individual coefficients that have magnitudes smaller than the threshold.
2. The list of insignificant sets (LIS) contains sets of wavelet coefficients that are defined by tree structures and are found to have magnitudes smaller than the threshold (insignificant). The sets exclude the coefficients corresponding to the tree and all sub tree roots and they have at least four elements.
3. The list of significant pixels (LSP) is a list of pixels found to have magnitudes larger than the threshold.
4. The set of offspring (direct descendants) of a tree node, $O(i, j)$, in the tree structures is defined by pixel location (i, j), The set of descendants, $D(i, j)$, of a node is defined by pixel location (i, j). $L(i, j)$ is defined as $L(i, j) = D(i, j) – O(i, j)$.

The threshold, T, for the first bit-plane is equal to $2n$, and $n = \log2(\max(i, j)\{|c(i, j)|\}$, (1) where $c(i, j)$ represents the (i, j)th wavelet coefficient. All the wavelet coefficients are searched in order to obtain the maximum $c(i, j)$ after executing the discrete wavelet transform. For operations in the subsequent bit-planes of threshold T, n is reduced by 1.For each pixel in the LIP, one bit is used to describe its significance. If it is not significant, the pixel remains in the LIP and no more bits are generated ;otherwise, a sign bit is produced and the pixel is moved to the LSP. Similarly, each set in the LIS requires one bit for the significance information. The insignificant sets remain in the LIS; the significant sets are partitioned into subsets, which are processed in the same manner and at the same resolution until each significant subset has exactly one coefficient.

Finally, each pixel in the LSP is refined with one bit. SPIHT produces a better compression rate and image quality.

4. EXPERIMENTAL RESULTS

4.1 Results for chaotic encryption technique

The encryption algorithms of the three systems have been implemented in MATLAB 7.4. For the hybrid encryption scheme the system key or the initial conditions taken are as follows: $\mu_1 = 3.9$, $x_{01}=0.400005674$, $x_{02} = 0.496264538324968$, $y_{02} = -636856254848635$.

The results for the encryption process are shown below:

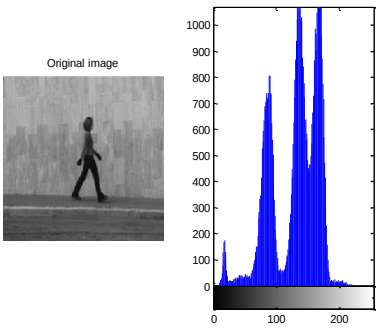

Figure 6. The original image 1 with histogram

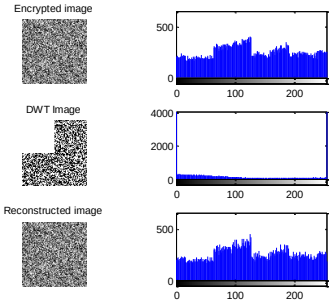

Figure 7: Image 1 after Chaotic encryption technique with histogram

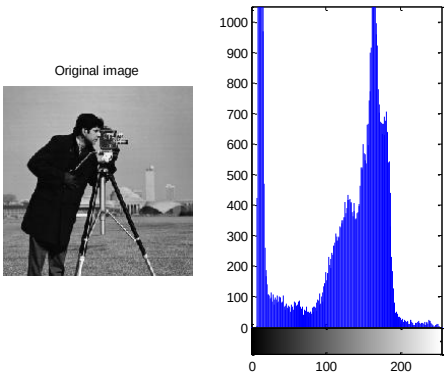

Figure 8: The original image 2 with histogram

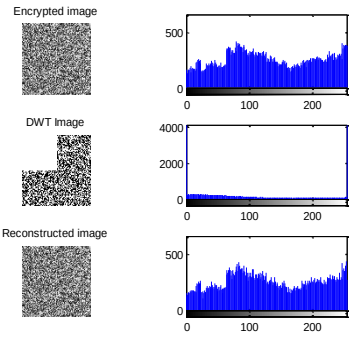

Figure 9: Image 2 after chaotic encryption technique with histogram

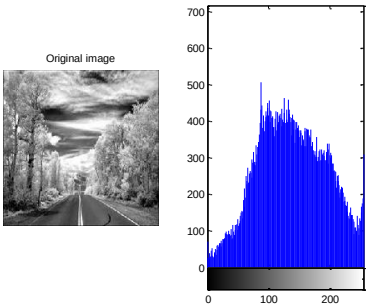

Figure 10: The original image 3 with histogram

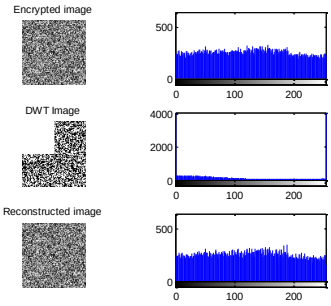

Figure 11: Image 3 after Chaotic encryption technique with histogram

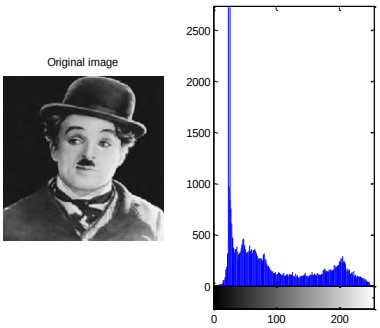

Figure 12 : The original image 4 with histogram

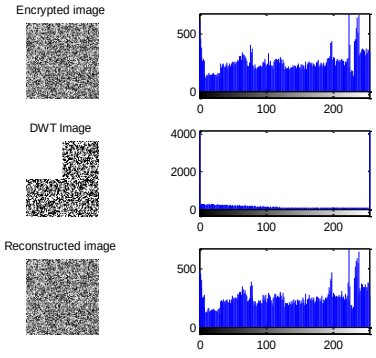

Figure 13: Image 4 after Chaotic encryption technique with histogram

4.2 Decryption results

The decrypting process of the image is the inverse process of the encryption.

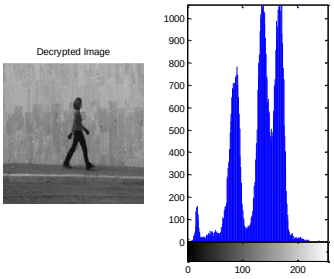

Figure 14: Image 1 after Decryption with histogram

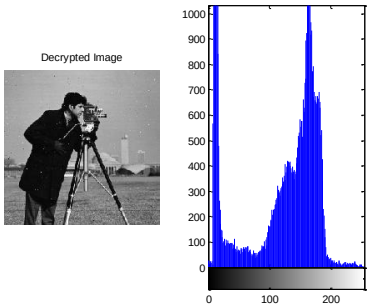

Figure 15: Image 1 after Decryption with histogram

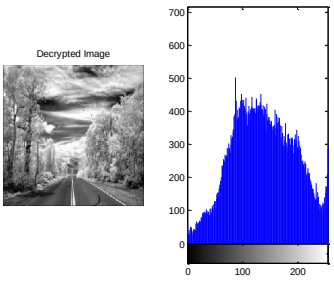

Figure 16: Image 3 after Decryption with histogram

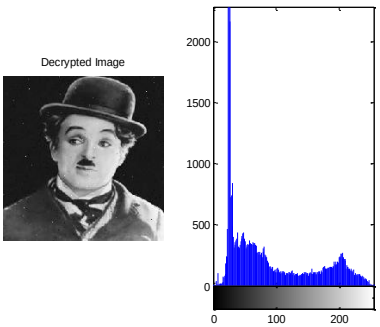

Figure 17: Image 3 after Decryption with histogram

5 COMPARATIVE ANALYSIS

The hybrid chaotic encryption scheme and the selective encryption scheme are compared on the basis of statistics and time.

The three systems were simulated on MATLAB 7.4 running on a Pentium D 3 GHz processor.

The hybrid technique based on chaos theory is able to successfully combine the benefits of the two reviewed chaos based encryption schemes viz. faster execution time and higher de-correlating ability.

Table 1. Run time for Encryption and Decryption

Sr.No	Image	Processing Time for Encryption (sec)	Processing Time for Decryption (sec)
1.	Image 1	2.3888	1.0388
2	Image 2	2.8382	1.2682
3	Image 3	2.2933	1.01452
4	Image4	2.5262	1.1297

Table 2. Comparison of Compression Ratio and Entropy

Sr.No	Image	Entropy	Compression ratio
1.	Image 1	6.8294	0.8799
2	Image 2	7.0521	0.8776
3	Image 3	7.791	0.8780
4	Image 4	6.4577	0.8728

6 SECURITY ANALYSIS

A good encryption scheme should resist all kinds of known attacks such as known-plain-text attack, cipher-text only attack, statistical attack, differential attack, and various brute force attacks. Some security analysis has been performed on the hybrid image encryption scheme, including the most important ones like key space analysis. The tests performed have demonstrated the satisfactory security of the new scheme.

6.1 Key Space Analysis for Chaos Based Image Encryption

The key chosen for the system i.e. the initial conditions μ_1, x_{01}, x_{02}, y_{02} are of data type double. So they represent a 256 bit key. In the hybrid scheme, at least 2^{256} mathematical steps are required for brute force cryptanalysis. However, this is not true for chaotic systems as they can be analyzed using more systematic approaches, which drastically reduce the computational effort required. Sobhy [8] has developed a method of attacking chaotic encryption algorithms and almost all chaotic systems are broken in very short computer times. Sobhy concluded that all chaotic encryption algorithms using constant key are prone to attack. The first step of this attack is to determine the system used. The second step is to build the system and minimize the output to obtain the key.

7. CONCLUSION

A new technique that combines the benefits of the two systems under analysis has been proposed. Security analysis and simulation results show that the encryption scheme is effective. The scheme can resist most known attacks, such as statistical analysis and brute-force attacks. The SPIHT

Algorithm gives good compression ratio for the four different gray scale images. In the practical approach the compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image.

For securing large visual data with requirements of real-time communication and use in resource constrained applications such method would be in demand in the future as well.

8. REFERENCES

[1] Sanjeev Ghosh, Sangeeta Mishra, Payel Saha. *Chaos Based Encryption Technique for Digital Images*. 2010 International conference ICWET.

[2] Marc Van Droogen broeck and Raphael Benedett, *Techniques for a selective encryption of uncompressed and compressed images***.** Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 9-11, 2002

[3] Zhang Dinghies, GU Qiujie, Pan Yonghua and Zhang Xinghua.2008. *Discrete Chaotic Encryption and Decryption of Digital Images*. 2008 International Conference on Computer Science and Software Engineering.

[4] Huang-Pei Xiao and Guo-Ji Zhang. 2006. *An Image Encryption Scheme Based on Chaotic Systems*. Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

[5 Jiri Fridrich.1997.*Image Encryption Based on Chaotic Maps*. Proceedings of IEEE Conference on Systems, Man and Cybemetics. 1105-1110, 1997.

[6] S Wang Ying, Zheng, DeLing Ju Lei, et al.2004.*The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System*. Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176, December. 2004.

[7] Huang Xiaosheng, Gu Jingwen. *Image Encryption Algorithm Based on Compound Chaotic Sequence and Wavelet Transform* [J]. 2007. Computer Engineering, 200733(14): 128-129,135.

[8] Sobhy, M.I. and Shehata, A.R. *Methods of Attacking Chaotic Encryption and Countermeasures*. 2001. IEEE Proceedings of ICASSP 2001, Vol 2, pp. 1001-1004 May. 2001.

[9] D. Slepian and J. K. Wolf, "*Noiseless coding of correlated information sources*," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 471–480, July 1973.

[10] Mark Johnson, *Student Member, IEEE*, Prakash Ishwar, Vinod Prabhakaran, *Student Member,* IEEE*On Compressing Encrypted Data*IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 52, NO. 10, OCTOBER 2004