Parametric Switching Chaotic System Based Crypto Compression Scheme

[1]G.Sekar and [2]Dr.S.Valarmathy
[1]AssistantProfessor, [2]Professor
[1]ECE, Sri Ramakrishna Institute of Technology, Coimbatore, India
[2]ECE, BannariAmman Institute of Technology, Sathyamangalam, Erode, India

Abstract**--** This paper proposes a novel scheme for lossy compression of an image using orthogonal transform and PSCS (Parametric Switching Chaotic System).PSCS based image encryption provides stronger security level than the existing Pseudo Random Permutation Method. PSCS algorithm is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principle content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. A new loss-less symmetric image encryption using a permutation and diffusion structure is proposed. A new key generation process generates secondary keys that act as control parameter for permutation order and diffusion bit generator. The Image pixels are scrambled in bit level. Permutation order is generated using the parametric switching type that permutes the pixel in bit wise manner. In the diffusion stage the different keys were used to diffuse in each round. In the diffusion stage the image pixel bits are masked with the randomly generated binary sequence. Three chaotic systems employed to generate the secondary key, permutation order and diffusion bits. The simulation results show that the proposed system produces the better MSE, PSNR and prove the satisfactory level of security for image encryption.

Keywords**--** *Image Encryption; Authentication; Compression*

I. INTRODUCTION

In recent years, compression of encrypted data has attracted considerable research interest. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating decompression and decryption functions will be used to reconstruct the original data. Several techniques for compressing/decompressing encrypted data have been developed. It has been shown in [2] that, based on the theory of source coding with side information at the decoder, the performance of compressing encrypted data may be as good as that of compressing non-encrypted data in theory. In the former approach, the original binary image is encrypted by adding a pseudorandom string, and the encrypted data are compressed by finding the syndromes with respect to Low-Density Parity-Check (LDPC) channel code [3]. In the latter one, the original data is encrypted by adding Gaussian sequence, and the encrypted data are quantized and compressed as the syndromes of trellis code. The compression of encrypted data for both memory less sources and sources with hidden Markov correlation using LDPC codes is also studied [4]. By employing LDPC codes into various bit-planes and exploiting the spatial and cross-plane correlation among pixels, a few methods for lossless compression of encrypted gray and color images are introduced in [5]. In [6], the encrypted image is decomposed in a progressive manner, and the most significant bits in high levels are compressed using rate-compatible punctured turbo codes. The decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to obtain the content in high levels. Furthermore, by developing statistical models for source data and extending these models to video, [7] presents some algorithms for compressing encrypted data and demonstrate blind compression of encrypted video. In [8], a compressive sensing technique is introduced to achieve lossy compression of encrypted image data, and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. The signal processing in the encryption domain using homomorphic calculation is also discussed in [9] and [10]. In most of the above-mentioned schemes for compressing encrypted image, the syndrome of channel code is exploited to generate the compressed data in lossless manner. In this work, we propose a novel system for lossy compression of encrypted image with flexible compression ratio, which is made up of image encryption, tailor-made compression, and iterative decompression phases. The network provider may remove the redundant and trivial data from the encrypted image, and a receiver can retrieve the principal content of the original image using an iterative procedure. The compression ratio and the quality of the reconstructed image are dependent on the values of compression parameters. Generally, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. Compared with the previous lossless encrypted-image compression approaches, with a cost of slight degradation of encryption security and reconstruction quality, the proposed scheme can significantly improve the compression efficiency. In the modern communication the sharing of multimediacontents, medical imaging and telemedicine over the internet security of these contents plays a major role. Images are the real integral part of the information in internet communication. To protect the information from unauthorized snooping is to use an encryption algorithm to disguise the information. In the past decades various number theory based encryption techniques such as DES, AES, RSA, etc. [2 and 3]. The conventional encryption techniques does not seems to be appropriate for images due to some characteristics of images bulk data, solid correlation between adjacent pixels and high redundancy. The significant characteristics of chaotic dynamical systems are periodicity, mixing property, sensitivity to initial conditions and system parameters [4]. Due to these properties of chaos the researchers enticed to make chaotic cryptosystem for image encryption. The hybrid1D chaotic system is denoted as Logistic-Tent system, Logistic-Sine system and Tent-Sine system. The use of hybrid 1D system generates the different chaotic sequences. When any one of the seed map is out of the chaotic range, then generated sequence is chaotic due to hybrid chaotic system. To analyze and overcome the problems of 1D chaotic maps and security analysis of the chaos based image encryption the hybrid chaotic system is used in this encryption algorithm. To demonstrate the security analysis a chaos based permutation diffusion image encryption is proposed, which has the excellent permutation and diffusion properties to resist the different attacks, particularly chosen-plain text attacks. Parametric switching based PO generation is more random than using single chaotic map based random sequence generation. While applying this encryption algorithm to plain image at each round the diffusion bits are updated. This diffusion bits updating produces the different cipher images for each round. This confirms that the proposed algorithm able to resists the differential attack.

II. PARAMETRIC SWITCHING CHAOTIC SYSTEM

A. Encryption Algorithm

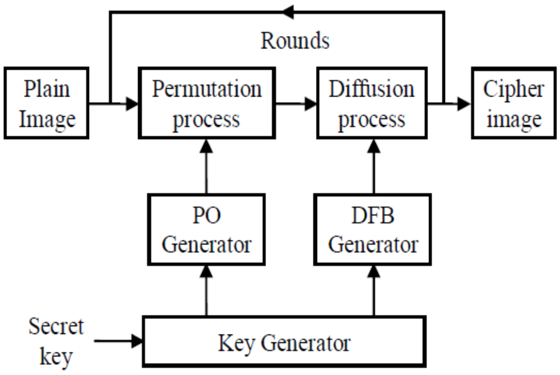


Figure 1: Proposed Encryption Technique

The proposed encryption algorithm [1] has the following steps to get the uncorrelated cipher image.

Step 1: The external keys (K1, K2, K3 and K) are fed into the key generator to produce the secondary keys (PK4, PK3 and PK) plain image is converted to binary form of N x M x 8 lengths.

Step 2: Feeding secondary key to the permutation order generator (PO). The permutation sequence will be generated by using the permutation sequence the pixel bits are shuffled.

Step 3: For i^{th}round the secondary key feed as the initial condition for Tent and Sine chaotic system. The system iterated for length of the shuffled binary sequence to generate the diffusion bits (DFB).

Step 4: Permuted image pixel bits are masked with the generated random bits and this will be repeated for four rounds. For each round the secondary key will be updated.

B. Decryption Algorithm

In the decryption process is the reverse process of the encryption algorithm. The external keys are sent through the secured channel between the users. The same key generation is processed in retrieval side. The decrypted image is an original image without any lossless of original image information. The produced cipher image is secure against statistical and differential attacks.

III. BLOCK CIPHER BASED ON A SUITABLE USE OF THE CHAOTIC STANDARD MAP

Due to their features of ergodicity, sensitivity to initial conditions and sensitivity to control parameters, etc., chaotic maps have good potential for information encryption. In this paper, a block cipher based on the chaotic standard map is proposed, which is composed of three parts: a confusion process based on chaotic standard map, a diffusion function, and a key generator. The parameter sensitivity of the standard map is analyzed, and the confusion process based on it is proposed. A diffusion function with high diffusion speed is designed, and a key generator based on the chaotic skew tent map is derived. Some cryptanalysis on the security of the designed cipher is carried out, and its computational complexity is analyzed. Experimental results show that the new cipher has satisfactory security with a low cost, which makes it a potential candidate for encryption of multimedia data such as images, audios and even videos.

A. A symmetric image encryption scheme based on 3D chaotic cat maps

Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity and high redundancy, which are generally difficult to handle by traditional methods. Due to the exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. In this paper, the two-dimensional chaotic cat map is generalized to 3D for designing a real-time secure symmetric encryption scheme. This new scheme employs the 3D cat map to shuffle the positions (and, if desired, grey values as well) of image pixels and uses another chaotic map to confuse the relationship between the cipher-image and the plain-image, thereby significantly increasing the resistance to statistical and differential attacks. Thorough experimental tests are carried out with detailed analysis, demonstrating the high security and fast encryption speed of the new scheme.

B. Image encryption with compound chaotic sequence cipher shifting dynamically

We design a new two-dimensional chaotic function using two one-dimensional chaotic functions, and then prove the chaotic properties to a new function based on a strict Devaney definition. And we propose a new encrypting image scheme using the new compound chaotic function by choosing one of the two one-dimensional chaotic functions randomly. We give statistical analysis, sequence random analysis, and sensitivity analysis to plaintext and key on the proposed scheme. The experimental results show that the new scheme has a very fast encryption speed and the key space is expanded and it can resist all kinds of cryptanalytic, statistical and brute-force attacks, and especially, our new method can be also used to solve the problem that is easily exposed to chosen plaintext attack and low digitization of one-dimensional chaotic function.

C. Cryptanalysis of a one round chaos-based Substitution Permutation Network

The interleaving of chaos and cryptography has been the aim of a large set of works since the beginning of the nineties. Many encryption proposals have been introduced to improve conventional cryptography. However, many of possess serious problems according to the basic requirements for the secure exchange of information. In this paper we highlight some of the main problems of chaotic cryptography by means of the analysis of a very recent chaotic cryptosystem based on a one round Substitution Permutation Network. More specifically, we show that it is not possible to avoid the security problems of that encryption architecture just by including a chaotic system [12] as the core of the derived encryption system.

IV. SIGNIFICANCE OF THE PROPOSED WORK

The significance of this work is to protect confidential image data from unauthorized access. That means sender should encrypt the original data and the network provider may tend to compress the encrypted data [11] without any knowledge of the cryptographic key and the original data. In the existing work we use pseudo random permutation for encryption of an image. But the security level is weaker than stream cipher. Thus we propose a technique called PSCS (Parametric Switching Chaotic System).Compression reduces the time for sending images over the internet or downloaded from Webpages. In order to achieve this, we propose a novel scheme for lossy compression of an encrypted image with flexible compression ratio. After receiving the compressed data, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. Since the coefficients are generated from all elastic pixels, the errors in a final reconstructed result are distributed over the image with an approximately uniform manner. Thus by using a technique called PSCS (Parametric Switching Chaotic System) for the encryption of the original image; we achieve a higher security in image encryption.

V. SIMULATION RESULTS

The simulation results proved the satisfactory level of security for image encryption and compression at a higher rate using a technique called orthogonal transform. PSNR values are inversly propotional to the bit error rate. So high PSNR values provide better result. Compared to [13], the proposed method provides the PSNR values ranges from 27 dB to 27.5 dB.

A. Existing system (Pseudo Random Permutation Method)

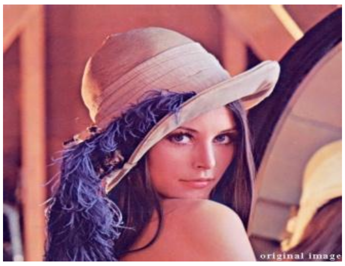


Figure 2: Input Image

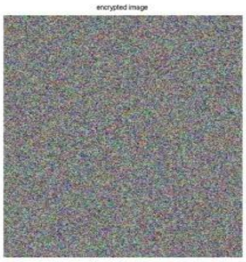


Figure 3: Encrypted Image

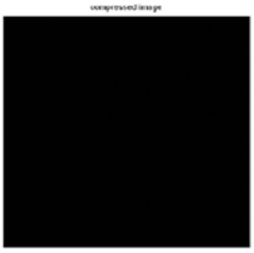


Figure 4: Compressed Image

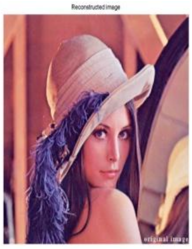


Figure 5: Reconstructed Image

The above images show the simulation results of image encryption by pseudorandom permutation and compression by Orthogonal Transform in the existing system.

B. Proposed System (PSCS)

a. Input Image

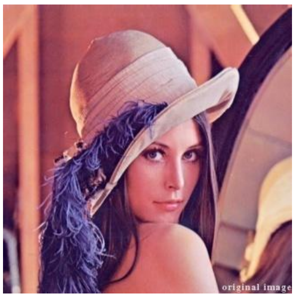


Figure 6: Input Image

b. Encrypted Image

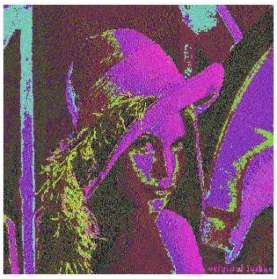


Figure 7: Encrypted Image

c. Compressed Image

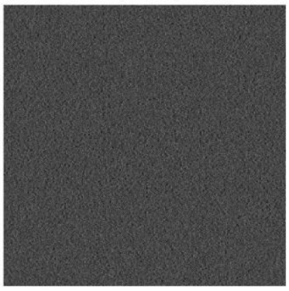


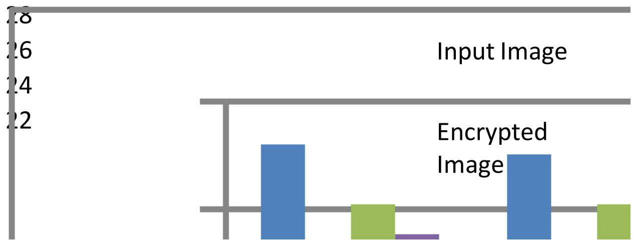
Figure 8: Compressed Image

d. Reconstructed Image

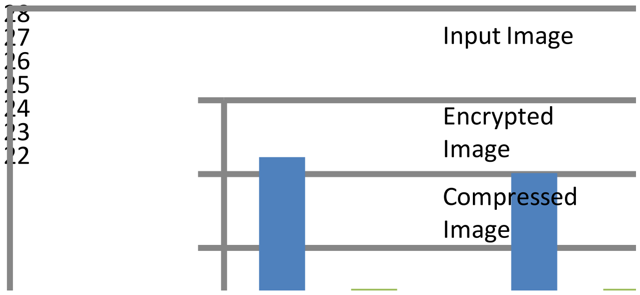
Figure 9: Reconstructed Image

C. Comparison of PSNR and MSE for Existing System and Proposed System

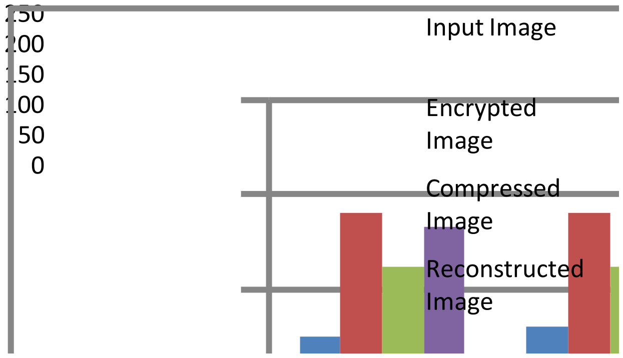
a. PSNR- Existing Method



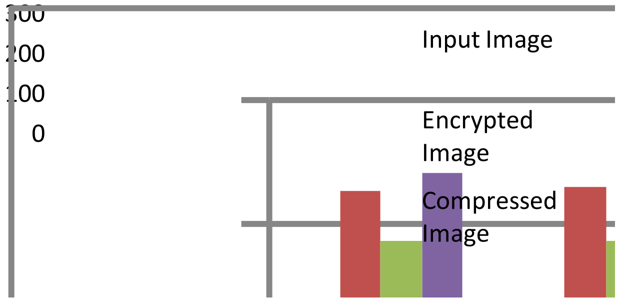
b. PSNR- Proposed Method



c. MSE- Existing Method



d. MSE- Existing Method



CONCLUSION

This paper conferred the knowledge for compressing an encrypted image and designed a practical scheme made up of image encryption, lossy compression, and iterative reconstruction. The original image is encrypted by pseudo random permutation, and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. In general, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. In the encryption phase of the existing system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data. On the other hand, the security of encryption used here is weaker than that of standard stream cipher, which can be cooperative with the proposed technique called PSCS. In the proposed system to test the security of the image encryption algorithm various performance analysis such as security analysis, statistical analysis and differential analysis were performed. The robustness and key sensitivity of the proposed scheme are demonstrated using MATLAB platform. Different test images were used to test the proposed algorithm. The Simulation outputs of proposed method shows that the value of MSE and PSNR are comparatively better when compared with the existing methodologies.

References

[1] Quist AphetsiKester, Laurent Nana and Anca Christine Pascu“A Hybrid Image Cryptographic and Spatial Digital Watermarking Encryption technique for Security and authentication of digital images”, IEEE International conf. on Modeling and Simulation, pp. 322–326, 2015.

[2] T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage-efficient processing of encrypted signals”, IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[3] T. Bianchi, A. Piva, and M. Barni, “On the implementation of the discrete Fourier transform in the encrypted domain”, IEEE Trans. Inf.Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[4] N. Bourbakis and C. Alexopoulos, “Picture data encryption using SCAN patterns”, Pattern Recognit., vol. 25, no. 6, pp. 567–581, 1992.

[5] R. G. Gallager, “Low Density Parity Check Codes”, Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, 1963.

[6] M. Johnson, P.Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, “On compressing encrypted data”, IEEE Trans. Signal Process., vol. 52, no. 10, pt. 2, pp. 2992–3006, Oct. 2004.

[7] A. Kumar and A.Makur, “Lossy compression of encrypted image by compressing sensing technique”, in Proc. IEEE Region 10 Conf.(TENCON 2009), pp. 1–6,2009.

[8] R.Lazzeretti and M. Barni, “Lossless compression of encrypted gray-level and color images,” in Proc.16th Eur. Signal Processing Conf. (EUSIPCO 2008), Lausanne, Switzerland, Aug. 2008.

[9] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images”, IEEE Trans. Image Process., vol. 19, no. 4,pp. 1097–1102, Apr. 2010.

[10] D. Schonberg, S. C. Draper, and K. Ramchandran, “On blind compression of encrypted correlated data

approaching the source entropy rate", in Proc. 43rd Annu. Allerton Conf., Allerton, IL, 2005.

[11] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences", IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[12] J.-C. Yen and J.-I.Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization", Proc. Inst. Elect. Eng., Vis. Image Signal Process., vol. 147, no. 2, pp. 167–175, 2000.

[13] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.