Image Scrambling Techniques: A Review

Neetesh Malaiya[1] Vikas Gupta[2]
[1]M.Tech Research Scholar [2]Professor
[1,2]Technocrats Institute of Technology, Bhopal, India

Abstract— The development of mobile and internet technology have made the access, transmission and storage of huge multimedia data easy. However the prevalence of these technologies has led to serious security concerns and handling needs. This paper explores the overview of scrambling process for image signal over a channel, its features, technologies related to fulfil requirements of security related concerns such as unlawful, unofficial, unauthorized and illegal use.

Keywords: PSTN, PRBS, LFSR, SNR, LPC, IDEA, DES, AES, BCD, UES, crmiLTP

I. INTRODUCTION

The technology related to communication improving day by day with the advancement of devises to encode and decode. The transmission of data either voice, image or video signal becomes so fast and easy accessible. But the main concern is the security of data i.e. to make data confidential and should not be easily attack by everyone especially in the field of defense, online transaction and in mobile communication.

This paper consist a brief review about the process of scrambling used till now for a image signal and its merits and limitation related to either security or signalling process related to bandwidth concern.

Scrambling is the process in which the original signal is invert encoded and transmitted to the receiver and further decoded which is widely used in communication world. Scrambling is widely used in satellite, radio relay communications and PSTN modems. Modern scrambling process is different from classical approach, now the process is summarized with cryptography using public key system which makes the scrambler (device perform the function of scrambling process) much more secure than earlier analog counterparts.

In section II, the image scrambling process summarized. Then different methods till now with their efficiency are presented. In section III reasons for using scrambling is discussed. In section IV challenges present are given. Section V concludes the paper.

II. OVERVIEW OF IMAGE SCRAMBLING

The image scrambling method uses the image signal which may be in any format like jpg., png. etc to transmit. Digital image scrambling is commonly used for image data security. Till now different paper are published on image scrambling method considering different image signal parameters. In this review, papers discussed covers different methods like Image scrambling without bandwidth expansion, unified data embedding and scrambling, Binary codes based (BCD) image scrambling for multiple application.

In [6] scrambling without bandwidth expansion which is based on 2D discrete prolate spheroidal sequences where the full 2D multimedia data consider as 1D texture bit stream and then applied to any conventional cipher that has been validated in modern cryptography DES, IDEA, AES is discussed. The method does not introduce many high frequency components into the spectrum of cipher text, but causes negligible expansion of Bandwidth. Also the method not able to provide content protection for digital images i.e. not secure to attack like cipher text only attack, known chosen plain text attack, chosen cipher text attack.

Another method for image scrambling unified data embedding (UES)[7] which mainly concern to the image quality by high payload and adaptive scalable quality degradation.UES guides the embedding scrambling algorithm to handle the exact number of pixels i.e. The perceptual quality of the embedded scrambled image can be controlled. The method is able to severely degrade quality of the host image by embedding external information into it and the distortion level can be controlled by changing level of processing.

The demerit is that the method in not secure to different attack and fails at security level. Also the method can be apply in frequency domain in order to predict the frequency coefficient.

Similar to UES another method [8] based on minimizing the distortion on the texture a secure binary image steganography is proposed to achieve statistical security without degrading the image quality or the embedding capacity, the method based on CrmiLTP(compliment rotation and mirroring-invariant local texture pattern).

So far many methods[6], [7], [8] have been proposed related to image scrambling but the main thing is to achieve the security level apart from these a Binary codes based speedy image encryption algorithm for multiple application is used which uses [5]the BCD code based decomposition reordering and scrambled. In this method of image scrambling a shift column is applied after scrambling to make it security proof. This is speedy encryption approach which is based on decomposition and modified AES algorithm to cipher hd images. Binary codes are used to decompose a secret image as an improvement to binary system-based traditional decomposition operation AES algorithm are used and scrambled. This approach is stronger than previous used method in reference to various attacks including statistic, plain text, data loss and noise attack specially used in medical and remote sensing images.

III. REASON FOR USING SCRAMBLING

In telecommunications, a scrambler is a device that transposes or inverts signals or otherwise encodes a message at the transmitter to make the message unintelligible at a receiver not equipped with an appropriately set descrambling device. Whereas encryption usually refers to operations carried out in the digital domain, scrambling usually refers to operations carried out in the analog domain. Scrambling is accomplished by the addition of components to the original signal or the changing of some important component of the original signal in order to make extraction

of the original signal difficult. Examples of the latter might include removing or changing vertical or horizontal sync pulses in television signals; televisions will not be able to display a picture from such a signal. Some modern scramblers are actually encryption devices, the name remaining due to the similarities in use, as opposed to internal operation.

In telecommunications and recording, a scrambler (also referred to as a randomizer) is a device that manipulates a data stream before transmitting. The manipulations are reversed by a descrambler at the receiving side. Scrambling is widely used in satellite, radio relay communications and PSTN modems.

A scrambler can be placed just before a FEC coder, or it can be placed after the FEC, just before the modulation or line code. A scrambler in this context has nothing to do with encrypting, as the intent is not to render the message unintelligible, but to give the transmitted data useful engineering properties.

- To enable accurate timing recovery on receiver equipment without resorting to redundant line coding. It facilitates the work of a timing recovery circuit (see also Clock recovery), an automatic gain control and other adaptive circuits of the receiver (eliminating long sequences consisting of '0' or '1' only).
- For energy dispersal on the carrier, reducing inter-carrier signal interference. It eliminates the dependence of a signal's power spectrum upon the actual transmitted data, making it more dispersed to meet maximum power spectral density requirements (because if the power is concentrated in a narrow frequency band, it can interfere with adjacent channels due to the intermodulation (also known as cross-modulation) caused by non-linarites of the receiving tract).

Scramblers are essential components of physical layer system standards besides interleaved coding and modulation. They are usually defined based on linear feedback shift registers (LFSRs) due to their good statistical properties and ease of implementation in hardware.

IV. CHALLENGES

The scrambling process uses the different algorithm which may be used in any domain or any algorithm method either bcd codes, frequency domain, space domain, colour domain the algorithm should be such that the image quality should be remain same as original i.e. to maintain the scalable quality and there should be short signal with limited use of bandwidth without its expansion, to remove the heavy communication overhead, signal features under exploitation with desirable channel usage, notable resistibility to hostile attack and make it security proof.

V. CONCLUSION

This paper presented a brief description of image scrambling technique till now. It has been observed that the number of scrambling related to voice or image techniques are used which have merits and demerits but till now the main thing is to maintain the confidential content and avoid brutal attacks the technology is, it must be affordable in cost and worth deploying in throughput.

REFERENCES

[1] Video Scrambling and descrambling for satellite and cable TV, Rudolf F. graf, William.
[2] Scrambling Techniques for digital Transmission, Byeong G.lee, and Seok.kim.
[3] Scrambling Techniques for digital transmission, Byeong G.lee www.springer.
[4] Scrambling-based speech encryption via compressed sensing-li-zieng, xiongwei zhang, liang chen, zhangjun fan and yonggang Wang..Eurasip journal-2012.
[5] Decomposition by BCD based speedy algorithm by Salim Mushin Wadi, Nasharuddin Zainal-www.ietdl.org.
[6] Cryptanalysis of an image scrambling scheme without bandwidth expansion ShujunLi, Chengqing Li,Kwok-Tung Lo, Member, IEEE and Guanrong Chen fellow, IEEE.
[7] A unified data embedding scrambling method Reza Moradi Rad, student member, IEEE, Koksheik wong member IEEE, Jing-Ming guo senior member, IEEE.
[8] Secure Binary Image Steganography, based on minimizing the distortion on the texture, Bingwen Feng,Wei Lu, and Wei Sun-vol.10.,2february2015-IEEE transaction on information forensics and security.

