Security Analysis of Multimedia Data Encryption Technique Using Piecewise Linear Chaotic Maps

Swati Rastogi
Department of Computer Sc. & Engineering
Amity School of Engineering & Technology
Noida, India
Swatirastogi13@gmail.com

Sanjeev Thakur
Department of Computer Sc. & Engineering
Amity School of Engineering & Technology
Noida, India
sthakur3@amity.edu

***Abstract*— In the current age of globalization file sharing has become an important part of every business process. Also in recent years, transfer of image or multimedia content across the world has become increasingly popular. To provide security, to large amount of multimedia content, a strong cryptographic technique is required, which can secure the multimedia content at desired transmission rate. Unfortunately, none of the traditional cryptographic algorithms provides enough security at required transmission rate. But chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure multimedia or image encryption techniques. This paper aims to analyze the security of "Multimedia Data Encryption Algorithm", on different kind of multimedia images and further to propose a new encryption technique for multimedia data.**

Keywords- Cryptography, Chaotic Maps, Encryption, Decryption.

_____*****_____

I. Introduction

The design of encryption techniques can be classified into 3 major types: Position permutation, which mix up or scrambles the original data according to some predefined schemes. Position Permutation function doesn't destroy the statistical properties of the plaintext and provides low security. Permutation function must be a reversible mapping. Value transformations, changes the value of original data or plaintext using simple transformation schemes. It destroy the statistical properties of the plaintext, it must also be a reversible mapping e.g. *XOR* function. Combination form implements both i.e. they apply both position permutation and value transformation to the original data to produce cipher text. Generally position permutations provide low security and are simple whereas value transformation techniques have low computational complexity. But when both the designs combined together i.e. combination form, it provides high data security together with low computational complexity. Traditional ciphers e.g. DES, IDEA, AES, RSA etc. doesn't fulfill the requirement of low computational complexity and high security simultaneously for image and multi-media data encryption, so they are not suitable for real time data encryption.

Since 1992, many researchers are trying to get a new cryptosystem to remove the problems in the existing encryption techniques mentioned above. They found that properties of chaotic systems have their analogous in Cryptosystems. The chaotic maps have properties like Ergodicity, Sensitivity to initial conditions/control parameters, Deterministic Dynamics etc. whose analogous in cryptosystems are Confusion, Diffusion, Deterministic Dynamics etc.

II. Chaotic Maps

In mathematics, a function that possesses some kind of chaotic behavior is defined as a chaotic function or map. Chaotic behavior of the function ensures that it is highly sensitive to initial conditions or parameters. This ensures that even an infinitesimal small change in the initial conditions could result a very large or dramatic change in the behavior of the chaotic map. As a result of this sensitivity to initial conditions or parameters, the behavior of chaotic systems "appears to be random". Here the phrase "appears to be random" signifies that being random, the future dynamics of the chaotic system are fully defined and determined by the initial conditions or parameters, without involvement of any random element. Because of the above-mentioned property, the behavior of the system is called Deterministic Chaos or simply "Chaos".

All chaotic systems must have following properties:

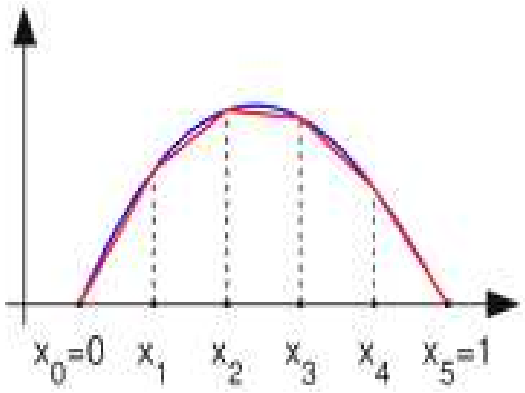
1. Sensitivity to initial conditions.
2. Topological mixing/ Ergodicity.
3. Dense periodic orbits.

III. Piecewise Linear Chaotic Map

In mathematics, a piecewise linear function,

$$f : \Omega \rightarrow V$$

where V is a vector space and Ω is a subset of a vector space, is any function with the property that Ω can be decomposed into finitely many convex polytopes, such that f is equal to a linear function on each of these polytopes.



A special case is when f is a real-valued function on an interval $[x1,x2]$. Then f is piecewise linear if and only if $[x1,x2]$ can be partitioned into finitely many sub-intervals, such that on each such sub-interval I, f is equal to a linear function

$$f(x) = aIx + bI.$$

The absolute value function $f(x) = |x|$ is a good example of a piecewise linear function. Other examples include the square wave, the sawtooth function, and the floor function.

PWLC map used in this paper are of the form

$$F(x) = \begin{cases} x/p, & x \in [0, p) \\ (x-p)/(0.5-p), & x \in [p, 0.5] \\ F(1-x, p), & x \in [0.5, 1). \end{cases}$$

IV. Proposed Encryption Algorithm

The proposed encryption process uses a 128 bit long secret key. Then the key is divided into sixteen 8-bit blocks, which are called session keys where k_i represents one 8- bit block of session key.

$k = k_1k_2\ldots\ldots\ldots\ldots k_{15}k_{16}$.

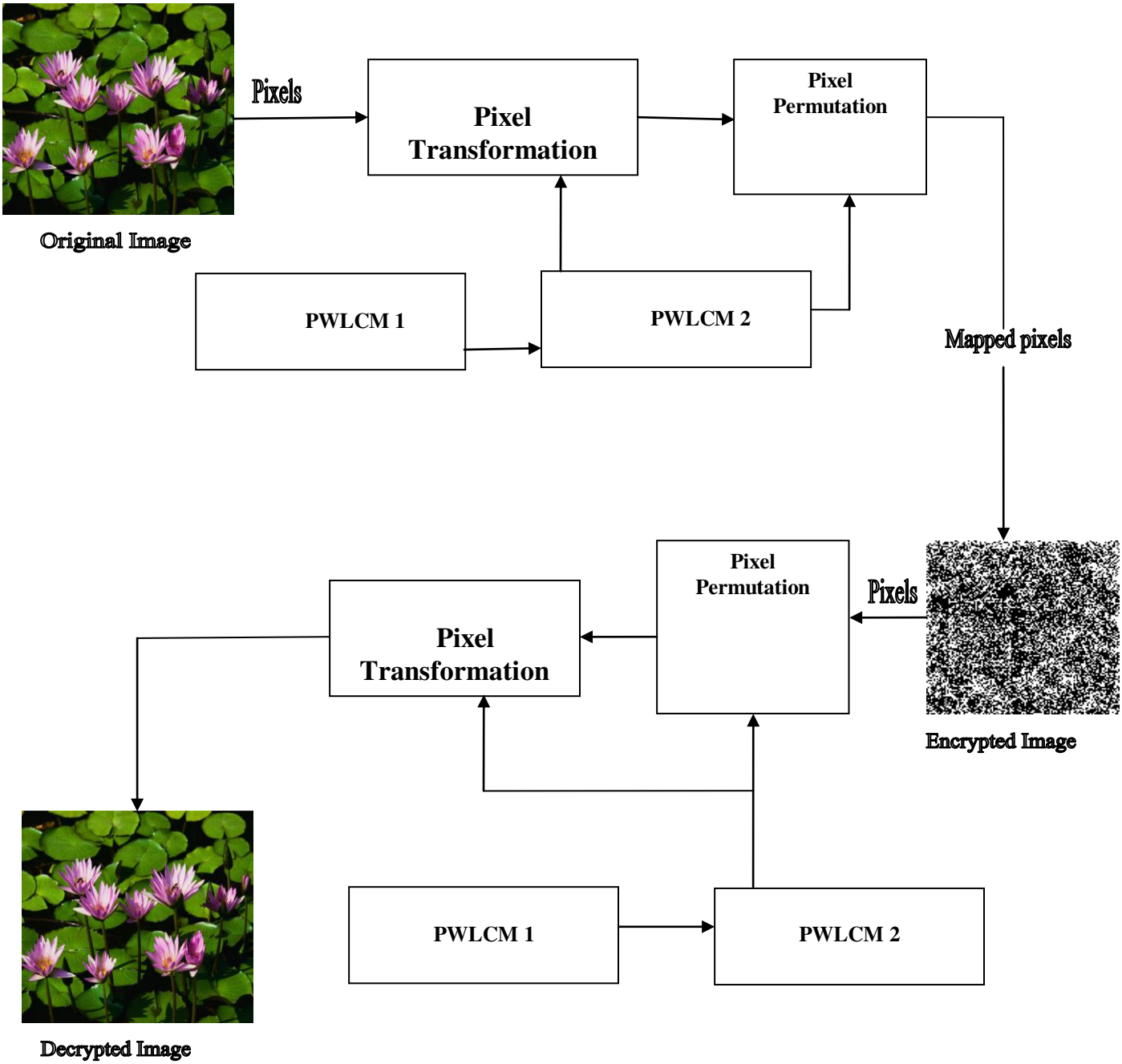
- Two PWLC maps are implemented in the proposed encryption technique.

$$F(x) = \begin{cases} x/p, & x \in [0, p) \\ (x-p)/(0.5-p), & x \in [p, 0.5] \\ F(1-x, p), & x \in [0.5, 1). \end{cases}$$

$$F(y) = \begin{cases} y/q, & y \in [0, q) \\ (y-q)/(0.5-q), & y \in [q, 0.5] \\ F(1-y, q), & y \in [0.5, 1). \end{cases}$$

- The system parameters p and q are kept constant for both the PWLC maps which represent the highly chaotic case. Initial parameters X_0 and Y_0 are calculated from the set of session keys.
- Stage 1: First PWLC map generates 32 distinct integer values ranging between [1, 32] and those values are converted into 32 real values using second PWLC map. Output of second PWLC map is also 32 real values between [0, 1]. These real values are grouped together in three non-overlapping subgroups and depending on the value, some simple encryption operations are performed on each pixel.
- Stage 2: 32 real values generated using second PWLC map are converted into integer values and thus further used by a pixel permutation function which takes a block of 32 pixels as an input, to generate the encrypted 32 pixel block. The input to the pixel mapping function is a block of 32 pixels encrypted in stage 1.

After encrypting each 32-pixel block the session keys are modified using some predefined rule to ensure high chaotic behavior.



REFERENCES :

1. H.-C. Chen, J.-I. Guo, L.-C.Huang, and J.-C. Yen, "Design and realization of a new signal security system for multimedia data transmission," *EURASIP J. Appl. Signal Process.* vol. 2003, no. 13, pp. 1291–1305, 2003.
2. N.K. Pareek, Vinod Patidar, *"Image encryption using chaotic logistic map"* Image and Vision Computing 24 (2006) 926–934.

3. J.-C. Yen and J.-I. Guo, "Design of a new signal security system," in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS '02)*, vol. 4, pp. 121–124, Scottsdale, Ariz, USA, May 2002.
4. J.-C. Yen and J.-I. Guo, "A new image encryption algorithm and its VLSI architecture," in *Proc. IEEE Workshop on Signal Processing Systems (SiPS '99)*, pp. 430–437, Taipei, Taiwan, October 1999.
5. K.-L. Chung and L.-C. Chang, "Large encrypting binary images with Higher security," *Pattern Recognition Letters*, vol. 19, no. 5-6, pp. 461–468, 1998.
6. N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.
7. C. Alexopoulos, N. Bourbakis, and N. Ioannou, "Image encryption method using a class of fractals," *J. of Electronic Imaging*, vol. 4, no. 3, pp. 251–259, 1995. Australia, December 2000.