Efficient Technique of Encrypting a Video Based on Chaotic Encryption in the Domain of Sine Function

S. Gayathri, M. Thamizh Illakiya and K. John Singh

School of Information Technology and Engineering, VITUniversity, Vellore, Tamil Nadu, India

Abstract: With the world facing major threats from different kinds of evil forces, it is necessary to protect those important data that are transmitted from one source to another source. There are many encryption and decryption algorithms existing already for safer data transmission. Though an ultimate algorithm, which is completely unknown to unreliable sources has not been found till date. The video encryption method is a challenging phase and works related to it are less in numbers. In this work, the video is fragmented depending on its size using Discrete Sine Transform (DST) function. A matrix is formed out of these obtained values and the dimension of the matrix is purely based on the size of the video. The further work will be discussed deeply in this paper where chaotic encryption technology is about to be used to encrypt the matrix data.

Key words: Chaos · Chaotic encryption · DST · Matrix

INTRODUCTION

The encryption techniques which currently exist are majorly based on the DCT domain [7]. DCT has found its application as the main tool for data compression/decompression in international image and audio coding standards. DST has been found recently as an alternative transform coding standard. DST has some specific mathematical properties which can be put into use for major works of encryption.

The matrices formed out of DST are real and orthogonal. All DSTs are transferable form; they can be transformed into one-dimensional transforms from multi-dimensional transform. Some of the basic properties of DST are the Unitarity property, the Linearity property, Convolution-Multiplication property and the shift property, Scaling and Difference property. Before getting into the detailed explanation of the properties of DST, it is necessary to give the definition of DST. The DST is defined in four forms as following.

\[
\text{DST I: } [S_{1}]_{n,k} = \frac{2}{\sqrt{N}} \varepsilon_q \sin \left( \frac{(2n + 1)(k + 1)}{2N} \right),
\]

\[n, k = 0,1,...,N-1.\]

\[
\text{DST II: } [S_{2}]_{n,k} = \frac{2}{\sqrt{N}} \varepsilon_q \sin \left( \frac{(2n + 1)(2k + 1)}{4N} \right),
\]

\[n, k = 0,1,...,N-1.\]

\[
\text{DST III: } [S_{3}]_{n,k} = \frac{2}{\sqrt{N}} \varepsilon_q \sin \left( \frac{(2n + 1)(2k + 1)}{2N} \right),
\]

\[n, k = 0,1,...,N-1.\]

\[
\text{DST IV: } [S_{4}]_{n,k} = \frac{2}{\sqrt{N}} \varepsilon_q \sin \left( \frac{(2n + 1)(2k + 1)}{4N} \right),
\]

\[n, k = 0,1,...,N-1.\]

where

\[\varepsilon_q = \begin{cases} 
1 & \text{for } \frac{1}{2} q = N - 1 \\
0 & \text{for other cases} 
\end{cases}\]

Unitarity property:

For Inverse DST matrices,

\[ [S_{N-1}]^{-1} = [S_{N-1}]^T = [S_{N-1}] \]
Paper [3] is based on image cryptosystem. In general, cryptosystem is the process of referring the public key for cipher text and are used for symmetric key techniques. The above titled paper uses multi-chaotic system for which same sequence for four chaotic systems are generated. As same shuffling of systems is used there is problem with the cryptosystem in processing the plain image. To overcome that shuffling is implemented in two stages: first, shuffling is done for bits of all pixels. Second, the bits for individual pixels are shuffled by themselves. For an image with RGB value the pixels are denoted as byte and this method uses m*n for an original plain text. With the help of row scan the plain text is directed for encryption. The vector’s resulting vector is N*1 where N=m*n.

**Multi Chaotic Systems Based Pixel Shuffle for Image Encryption, 2009:** A technique called pixel shuffle is introduced for image encryption with multi-chaotic systems. Chaotic systems are dynamic and are highly sensitive during the initial phase. Pixel shuffle drive away the outlines of image and disorders the RGB values. Since there is uncertainty in the system few tests like FIPS, correlation coefficient, NPCR and UACI are conducted to analyze the security level of encrypted image. By this process it decreases the error and brings out digital-color image [4].

By using logistic map and chaos encryption a new encryption algorithm is presented by predicting with their performance and security. Results are produced by coupled chaotic maps for the effectiveness of newly proposed algorithm. This system uses stream-cipher architecture which brings about two chaotic maps, one for stream generation and another for random mixing. This architecture strengthens the randomness in spite of finite precision. By analyzing the process it is known that this new algorithm for encryption is better than the existing techniques in speed and security. This technique [5] describes only the case study and is yet to perform in the real time encryption techniques.

**Chaotic Encryption under Dst Domain:** Consider a video of size 2000 kB which is about to be fragmented into frames using any one of the DST forms. According to the condition, N denotes the size of the video and subsequently the values of n and k are obtained from N. Let us consider the type II formula of DST to fragment the video.

\[
DST_{II}: [S_{II}^T] = \frac{2}{\sqrt{N}} \sum_{x=0}^{N-1} x e^{i \frac{\pi (2n+1)(x+1)}{2N}}
\]
where \( n, k = 0, 1, \ldots, N-1 \) and

\[
\varepsilon_q = \sqrt{\frac{2}{q}} = N - 1
\]

We have assumed the value of \( N \) to be 2000 and proceeding with this, we will obtain following calculations.

\[
S_1 = 0.0274 \\
S_2 = 0.0581 \\
S_3 = 0.0789 \\
\vdots \\
S_{2000} = 0.0075.
\]

The frames are now fragmented and each frame has the above mentioned unique values [6]. The next important step is to find the key to encrypt the video or which now can be referred to as fragmented frames. With DST functions, \( S_1, S_2, S_3, \ldots, S_N \) we can choose a sequence of functions to represent the key for encryption. For example, for the above mentioned values, \( S_{1000}, S_{1001}, S_{1002}, S_{1003}, \ldots \) and so on can be chosen [8]. The functions are to be chosen in a way so that when a graph is drawn out of the values, it should look more chaotic (as shown in Figure 1).

With the key value now being chosen, the respected selected frames will obviously be \( S_{1000}, S_{1001}, S_{1002} \) and so on. The following diagram shows the process which has been carried out so far and the future process which is about to take place.

A sample scrambled and encrypted frame is depicted below in Figure 3.

The encrypted frame can be decrypted by doing the process in the reverse manner. Using the key value, the values can be identified and the corresponding \( S_n \) values can be calculated from which the original frame can be retrieved. A sample decrypted image is shown below in Figure 4.

Procedure DST(N:float)

Var
CONCLUSION

The proposed system involves two major operations to be done: firstly, to determine the DST coefficients in order to scramble the video and secondly, to identify the key values and map them along with S values in order to find if they are chaotic. With these operations done efficiently without creating any trouble, the future process can be carried out very smoothly. This method is quite secure as there are no works being done using DST coefficients so far in the field of video encryption.