Journal of Computer Science 8 (6): 994-1000, 2012
ISSN 1549-3636

# A Chaotic Block Cipher for Real-Time Multimedia

Radha, N. and M. Venkatesulu
Department of Computer Applications,
Kalasalingam University, Krishnankoil, Srivilliputtur (via), TamilNadu-626190, India

**Abstract: Problem statement:** The widespread use of image, audio and video data makes media content protection increasingly necessary and important. We propose a naive approach which treats the multimedia signal to be protected as a text and use proposed encryption design to encrypt the whole data stream. Upon reception, the entire cipher text data stream would be decrypted and playback can be performed at the client end with an initial time delay. **Approach:** We introduce a block cipher algorithm, which encrypts and decrypts a block size of 512 bits regardless of the file format. In this, a permutation algorithm using a chaotic system is employed to provide the shuffler function. A shuffler operator is defined using the shuffler function. A random key generator generates key sequences and the scheme employs key-dependant transformations based on distance in the shuffling operator. The process of encryption/decryption is governed by the shuffler function, shuffler operator and the pseudorandom key. **Results:** The basic operation used is logical XOR and so the algorithm has a very high encryption/decryption speed. The execution time shows the proposed scheme is faster than the existing cryptographic schemes. **Conclusion:** The proposal of the algorithm is to manage the tradeoffs between the speed and security and hence appropriate for real-time image and video communication applications.

**Key words:** Block cipher, data encryption, shuffler, naive approach

## INTRODUCTION

The widespread usage of Internet is providing additional channels for a pirate to easily and quickly distribute the copyrighted digital content. As a result, the protection of content is now receiving a significant amount of consideration and strong security technology is required to protect user's sensitive digital data. Cryptography is recognized as the best method of protecting the data against attacks. The three common cryptographic objects are block-encryption algorithms, public-key algorithms and additive stream ciphers.

Block ciphers are designed by using two general principles such as diffusion and confusion. Modern block ciphers consist of four transformations such as substitution transformation, permutation transformation, linear mixing transformation and key-adding transformation. Fiestel and SPN are the two main structures in designing a block cipher. Fiestel structure uses the same algorithm between encryption and decryption and SPN uses different algorithm between encryption and decryption. Examples of block ciphers using Fiestel structures are DES, Blowfish, Camellia, CAST-128, FEAL, KASUMI, Twofish, XTEA, Lucifer, MARS, RC5, TEA, Triple DES, GOST 28147-89. Example of block ciphers using SPN structures are AES, SAFER, SHARK, 3-way.

It is easier to handle text encryption by traditional commercial ciphers. Image and video encryption is different from text encryption due to unique features of video and image such as bulk data capacity and high correlation among pixels and therefore it is difficult to handle by traditional ciphers.

Commercial ciphers define operations using algebraic transformations which are derived from continuous maps. They are not associated with chaos or dynamical systems. Chaos, is unsystematic, a periodic dynamic process, seeming disorderly, sensitive to changes on initial conditions and random-like behaviors and this property specially suits to the diffusion and confusion process in cryptography. So a block encryption algorithm using chaotic maps involves a complicated but sufficiently efficient one-to-one transformation on a finite space.

**Related study:**

**Block encryption:** Many scholars have made efforts to investigate block encryption algorithm in order to promote short processing time in encryption and decryption. Wang and Yu (2009) have proposed a block

**Corresponding Author:** Radha, N., Department of Computer Applications, Kalasalingam University, Krishnankoil, Srivilliputtur (via), TamilNadu-626190, India Tel: +91 9442010367 Fax: 91 4563-289322

encryption algorithm based on dynamic sequences of multiple chaotic systems. Several one-dimensional chaotic maps are used to generate pseudo-random sequences which are independent and approximately uniform. It generates a new pseudo-random sequence after a series of transformations, which covers the plaintext by executing Exclusive-OR and Shift operations some rounds to form the cipher. The cipher has a desired pseudo random characteristic and the decoder shows high sensitivity to all parameter mismatches. Lee *et al*. (2004) has proposed a block encryption algorithm using dynamic key mechanism. Different encryption key value is generated for each block to resist the differential and linear cryptanalysis in plaintext and encryption key. Pareek *et al*. (2003; 2005) have developed a symmetric key block cipher algorithm using a one-dimensional and multiple one-dimensional chaotic maps. Xua *et al*. (2008) have proposed a scheme based on a 3-d chen's chotic system, in which permutation by a key dependent shift approach and substitution by the XOR approach are combined. Xiang *et al*. (2006) has developed a block cryptosystem based on iterating a chaotic map.

**Image encryption:** Some of the recently proposed image encryption schemes (Behnia *et al*., 2009; Chen *et al*., 2004; Kwok and Tang, 2007) are studied. Behnia *et al*. (2009), a symmetric key block cipher algorithm based on tripled chaotic maps was introduced. Chen *et al*. (2004) have proposed a real-time secure image encryption scheme in which 2-dimensional chaotic map is generalized to 3-d map to shuffle the positions of the image pixels and uses another chaotic map to confuse the relationship between original and the encrypted image. Kwok and Tang (2007), a fast chaos-based image encryption system with stream cipher structure has been proposed.

**Video encryption:** A large number of video encryption schemes have been proposed and they tried to optimize the encryption process with respect to the encryption speed and display process. *Naïve algorithm* ensures the security level to the entire stream by standard encryption schemes such as AES or Triple DES. However, this approach is not applicable for big video, because it is very slow especially when we use Triple DES. Because of the encryption operation the delay increases and overload will be unacceptable for real time encryption. *Pure Permutation approach* scrambles the bytes within a frame of data stream by permutation. It is vulnerable to known-plain text attack because by comparing the cipher text with the known frames, the adversary could easily find out the secret permutation list. Tang (1996), the *Zigzag permutation algorithm* maps the individual 8×8 block to a 1×64 vector by using a random permutation list. Qiao and Nahrstedt (1997); Shi and Bhargava (1998) and Shi *et al*. (1999), the VEA was proposed which uses a traditional symmetric key cryptography to encrypt the sign bit of DCT coefficients and motion vectors. To reduce the amount of processing overhead, several selective encryption techniques which encrypt different levels of selective parts have been proposed in (Spanos and Maples, 1995; 1996; Lookabaugh and Sicker, 2004).

It is noted that many of these schemes have been found insecure, especially against known and/or chosen-plaintext attacks, while the safer ones were typically too slow to compete with the conventional ciphers. Thus, the design of an efficient, rapid and secure encryption scheme for the digital medium remains a challenging problem.

The remaining part of the study is organized as follows: We have detailed the proposed algorithm steps and discuss the experimental results. Also we discuss the diffusion and confusion property incorporated in the proposed algorithm. The security analysis and finally the conclusion are presented.

## MATERIALS AND METHODS

**Proposed algorithm:** In this study, we propose a new scheme that has fast performance speed and high level security. The design tools of our scheme are based on primitive operations, shuffler function and chaotic map with non-linear transformation functions. It utilizes the discrete chaotic cryptosystem which provides the shuffler function which has values uniformly distributed in the value space. Again to increase the confusion in the encryption process and to provide more security, shuffler operator is used. The design tools provide effective role in converting the original file into an encrypted form in efficient way. The original file is divided into blocks, each block having size of n = 512 bits. Let the block be $B_0$, $B_1$, $B_2$, $B_{3,}$ …, $B_i$. Each block has 64 bytes of plaintext $P_j$, $P_{j+1}$,…….$P_{j+63}$ and combine all the 64 bytes to form a binary message block $B_j^0$ of size n = 512 bits. Generate two arrays which store the shuffler values and shuffler operator values of size 513 bits. Generate pseudorandom key K of size 513 bits. The encryption process involves taking one random bit from key K and insert into the binary message block $B_0$ and get a new binary message block, applying shuffling operator and XOR operation. The resulting cipher block $C_0$ is of size, n+1. i.e.,) 513 bits. The decryption process is the reverse of the encryption process.

**Algorithm steps:**

Step 1: Generation of shuffler function $\pi$
Step 2: Generation of shuffler operator S
Step 3: Generation of pseudorandom key K
Step 4: Encryption process
Step 5: Decryption process

**Step 1: Generation of shuffler function $\pi$:** It is generated using the permutation approach and Let M be a random binary string of size n+1, ie.513 bits. Generate the shuffler values of size n+1, say M = ($a_{0,}$ $a_{1,}$ ......, $a_{n-1,}$ $a_n$) using the following shuffler function $\pi$.

Below, we present the permutation algorithm with the following pseudo-code:

```
A = B = 0
    For I = 0 to n step 1
Begin
        A = (A + 1) % n;
        B = (B + X[i]) % n;
        SWAP (shuff[A], shuff[B]);
    End loop
```

Here:

A: Sequence values starts from 0 and ends with n
B: Random values along with X[i] ranges between 0 to n
Swap: The INDEX values in an array

The Shuffler function uses CHAOS function X[i], a Non-Linear equation given by Eq. 1:

$$X[i] = P * X[i-1] * (1-X[i-1]) \quad (1)$$

Where:

X [0] = 0.2930000001

P = our key (by default its value is 2.96f. We can choose any value less than 4.0f.).

X [0 to n] contains random values between 0 to n. Some of the values may be repeated and depends on P (by default 2.96f)

Equation 1 is called a Simple Logistic Function (SLF) which is a single parameter second order function and exhibits various chaotic behaviors for different parameters X[i] and P (Masuda *et al*., 2006; Ou, 2008).

**Step 2: Generation of shuffler operator S:** Let $\pi$ be a permutation from the set {1, …, n+1} to itself using step 1.

Define a generalized shuffling operator S on M as follows:

Let $\pi(i) = j$, where i and j $\varepsilon$ {1… n}
Define $b_{j-1}$ = {$a_{i-1}$, if |i-j| = even
$1 - a_{i-1}$, if |i-j| = odd}
Set S(M) = ($b_0$,$b_1$,……$b_{n-1,}$ $b_n$ ).

This operator makes the spatial domain complex since it is not a simple one to one relation.

**Step 3: Generation of pseudorandom key K:** Generate, K, of size n+1, say K = ($K_{0,}$ $K_{1,}$ $K_{2,.........,}$ $K_n$).

**Step 4: Encryption process:** Let P be a plain text of size n, P = ($Q_{0,}$ $Q_{1,......,}$ $Q_{n-1}$).

**Key bit insertion in plaintext:** Take a bit from K at $i^{th}$ position and insert it in P at $i^{th}$ position. Call this as modified plaintext, $P^{\wedge}$ of size n+1.

**Apply shuffling operator, S on $P^{\wedge}$:** Get $S(P^{\wedge})$, of size n+1.

**Perform XORing operation:** It is represented as follows:

$$C = P^{\wedge} \oplus S(P^{\wedge}) \oplus K$$

where, C = ($C_{0,}$ $C_{1,}$ $C_{2,.........}$ $C_n$) is the cipher text, of size n+1.

**Step 5: Decryption process:** Clearly, $C \oplus K = P^{\wedge} \oplus S(P^{\wedge})$. We note that, the inserted $i^{th}$ bit of K is the $i^{th}$ bit of $P^{\wedge}$. Therefore, by using $P_i^{\wedge}$ and $C_i \oplus K_i$, we obtain $S(P_i^{\wedge})$. Again, from $P_i^{\wedge}$, letting $\pi(i) = j$, we obtain $j^{th}$ bit of $P_i^{\wedge}$. Repeating the process (n-1) times, we obtain the entire modified plaintext, $P^{\wedge}$ of size n+1.

Key bit removal in modified plaintext: Remove the inserted bit at the $i^{th}$ position in modified plaintext $P^{\wedge}$. Now we get the original plaintext P of size n.

## RESULTS

We used our algorithm to encrypt and decrypt all kinds of files. This encryption algorithm is independent of encoding format and therefore it is fit for all files. The algorithm uses the experimental environment, CPU: Intel[R] Core[TM]2 Duo CPU E7200 @ 2.53GHz, 0.99 GB of RAM; Operating system: Windows XP Professional.

Table 1 shows the Encryption/decryption time for various file sizes of different file types. The execution time shows the proposed scheme is faster than the existing schemes (Wang and Yu, 2009; Pareek *et al*., 2003; 2005; Baptista, 1998; Wong, 2002). The proposed algorithm is producing the cipher text, which is slightly longer than its corresponding plaintext and this is due to the insertion of a single bit in the plaintext block. Some of the cryptographic algorithms take a long computing time and the length of the cipher text is likely to be several times larger than that of plaintext. In the crypto-algorithms (Baptista, 1998; Wong, 2002), the ciphers size is two times of the plaintext size, which is difficult for bigger files in network transmission.

## DISCUSSION

The proposed algorithm is an ideal cryptosystem as it assures the diffusion and confusion theory proposed by Shannon (1949). The diffusion property can be achieved by using the shuffler function and the confusion property by the shuffler operator. Different keys make completely different cipher's distribution sequences. Figure 1 shows that the distribution of a cipher text's ASCII code evenly distributes in ASCII values [0,255] for the plaintext's ASCII code distributed in [0,125].

Figure 2 shows that the distribution of cipher text [0, 255] for the 10,192 bytes of all zero plaintext.

Figure 1 and 2 shows that the algorithm has high security enforcement.

The encryption and decryption are done simultaneously for all files without any loss of data. It is noted a very small time delay between the encryption/decryption process for the audio and video files. However, the proposed algorithm is a naive algorithm, which sees image, video and audio data as common data and does not require compatibleness of formats.

**Security analysis:**

**Key space analysis:** Key space size represents the total number of different keys that can be used for encryption. For an ideal system, the key space should be large enough to make brute force attacks infeasible. The proposed cipher has $2^{512}$ combination of keys. Thus it has various combinations of keys and has large key space and is reliable for practical use.

**Correlation analysis of two adjacent pixels:** The correlation between two adjacent pixels in horizontal, vertical and diagonal direction is given by the formulae Eq. 2 and 3:

$$r_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (2)$$

$$\mathrm{Cov}(x,y) = 1/N\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (3)$$

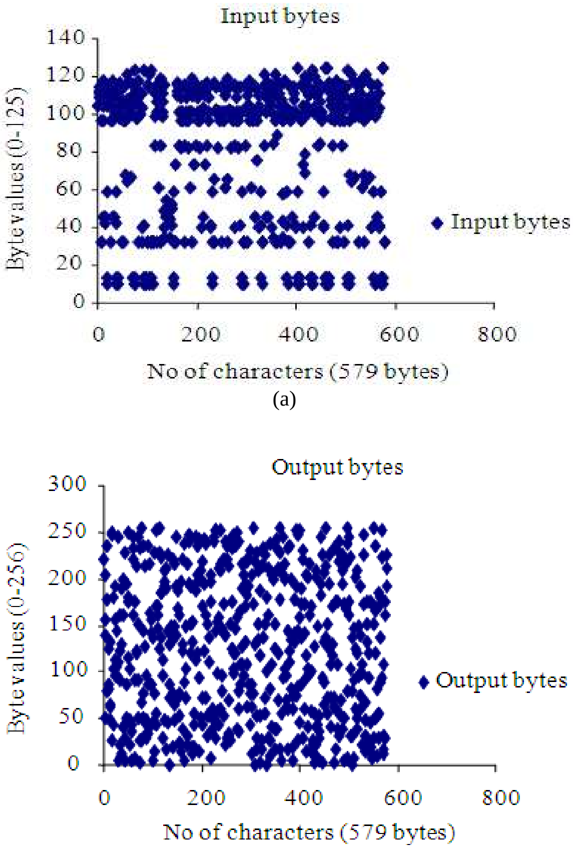
Where:

Cov(x, y) = Covariance
D(x) = Variance
x and y = The gray-scale values image

The following discrete formulas are used in numerical computations Eq. 4 and 5:

$$E(x) = 1/N\sum_{i=1}^{N}x_i \quad (4)$$

$$D(x) = 1/N\sum_{i=1}^{N}(x_i - E(x))^2 \quad (5)$$



(a)

(b)

Fig. 1: (a) Distribution of plaintext's ASCII code value [0,125] (b) Vs Distribution of cipher text's ASCII code value [0,255]

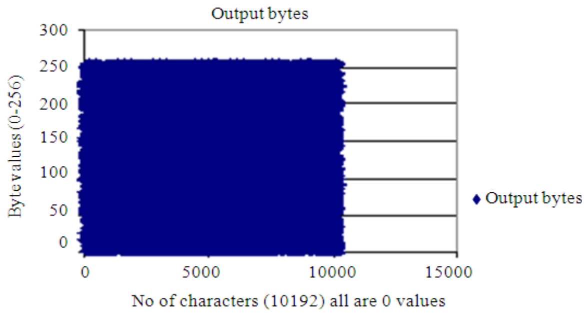


Fig. 2: Distribution of cipher text's ASCII code value [0,255] for the plaintext's ASCII code 0

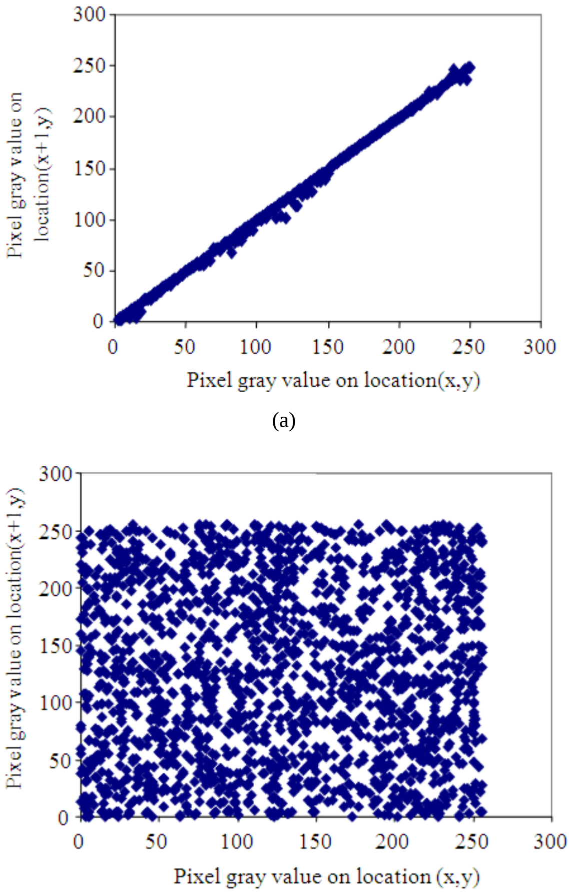


Fig. 3: Correlation of horizontally adjacent pixels in plain image (a) and the encrypted image (b) respectively

From Table 2, we find that the correlation between the two adjacent pixels in all the directions for the encrypted image are negligible and are very small. However, the two adjacent pixels in the plain image are highly correlated.

Table 1: Encryption/Decryption time for various file sizes

| File type | File size | Ciphersize | Execution time (Encryption and decryption) | Time delay for audio and video files |
|---|---|---|---|---|
| Bmp | 2.15 MB | 2.152 MB | 4 sec | - |
| Jpeg | 3.50 MB | 3.503 MB | 8 sec | - |
| Mp3 | 5.36 MB<br>Play time:<br>5.51 min | 5.365 MB | 12 sec | 0. 33 sec |
| Dat | 182 MB<br>Play time:<br>18. 05 min | 182.17 MB | 6 min 45 sec | 0. 34 sec |
| Vob | 976 MB<br>Play time:<br>14. 29 min | 976.25 MB | 9 min 47 sec | 0. 35 sec |

Table 2: Correlation coefficients of two adjacent pixels in the plain and the encrypted image

| Direction | Plain image | Encrypted image |
|---|---|---|
| Horizontal | 0.9845 | 0.0107 |
| Vertical | 0.9978 | 0.0239 |
| Diagonal | 0.9712 | 0.0348 |

This negligible correlation proves that the attacker cannot obtain any valuable information by exploiting a statistical attack. Figure 3 shows the correlation of horizontally adjacent pixels in a plain image (a) and its corresponding encrypted image (b) and the correlation coefficients are 0.9845 and 0.0107 respectively.

**Differential attack analysis:** To determine the influence of one-pixel change on the encrypted image, two common measures, NPCR and UACI are used. The Number of Pixels Change Rate (NPCR) measures the different pixel numbers between two images and Unified Average Changing Intensity (UACI) measures the average intensity of differences between the plain image and the cipher image. Let us take two encrypted images $E_1$ and $E_2$ and let their corresponding plain images have only one-pixel difference. The two measures are defined as follows Eq. 6 and 7:

$$NPCR = \frac{\Sigma_{i,j} D(i,j)}{W * H} * 100\% \quad (6)$$

$$UACI = \frac{1}{W * H} * \Sigma_{i,j} \frac{\left| E_1(i,j) - E_2(i,j) \right|}{255} * 100\% \quad (7)$$

Let H and W are the height and width of images and the gray-scale values of the pixels at grid (i,j) of $E_1$ and $E_2$ are labeled as $E_1(i,j)$ and $E_2(i,j)$ respectively. Define a bipolar array, D, with the same size as images $E_1$ and $E_2$. Then D(i,j) is related to $E_1(i,j)$ and $E_2(i,j)$, if $E_1(i,j) = E_2(i,j)$, then $D(i,j) = 1$ else $D(i,j) = 0$.

Tests have been performed on the proposed algorithm, taking randomly a pixel of the original image and make a slight change on the gray-scale level of this pixel. The encryption algorithm is performed on the modified original image and the two measures

NPCR and UACI are computed. We obtained NPCR = 99.62% and UACI = 32.58%. The results show that a slight change in the original image results in a great change in the encrypted image implies that the proposed algorithm has a good capability to resist the differential attack.

## CONCLUSION

In this study, a new naive approach suitable for real-time secure image, audio and video communication applications is proposed. Based on the effective shuffler function, non-linear key-dependant transformations and chaotic scheme, the system encrypts and decrypts 512-bits data stream using a pseudorandom key. The scheme is secure against brute force, statistical and differential attacks and capable to encrypt in an efficient way. Security analysis shows that the proposed algorithm has desirable properties such as diffusion and confusion and it can be used to realize the security cryptosystems over the internet.

## REFERENCES

Baptista, M.S., 1998. Cryptography with chaos. Phys. Lett., 240: 50-54. DOI: 10.1016/S0375-9601(98)00086-3

Behnia, S., A. Akhshani, A. Akhavan and H. Mahmodi, 2009. Applications of tripled chaotic maps in cryptography. Chaos Soliton Fract., 40: 505-519. DOI: 10.1016/j.chaos.2007.08.013

Chen, C., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Soliton Fract., 21: 749-761. DOI: 10.1016/j.chaos.2003.12.022

Kwok, H.S. and W.K.S. Tang, 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Soliton Ftact., 32: 1518-1529. DOI: 10.1016/j.chaos.2005.11.090

Lee, C.D., B.J. Choi and K.S. Park, 2004. Design evaluation of a block encryption algorithm using dynamic key mechanism. Future Generat. Comput. Syst., 20: 327-338. DOI: 10.1016/S0167-739X(03)00148-1

Lookabaugh, T. and D.C. Sicker, 2004. Selective encryption for consumer applications. IEEE Commun. Mag., 42: 124-129. DOI: 10.1109/MCOM.2004.1299355

Masuda, N., G. Jakimoski, K. Aihara and L. Kocarev, 2006. Chaotic block ciphers: From theory to practical algorithms. IEEE Trans. Circ. Syst. I: Regular Papers, 53: 1341-1352. DOI: 10.1109/TCSI.2006.874182

Ou, C.M., 2008. Design of block ciphers by simple chaotic functions. IEEE Comput. Intell. Mag., 3: 54-59. DOI: 10.1109/MCI.2008.919074

Pareek, N.K., V. Patidar and K.K. Sud, 2003. Discrete chaotic cryptography using external key. Phys. Lett. A., 309: 75-82. DOI: 10.1016/S0375-9601(03)00122-1

Pareek, N.K., V. Patidar and K.K. Sud, 2005. Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci. Numerical Simulat., 10: 715-723. DOI: 10.1016/j.cnsns.2004.03.006

Qiao, L. and K. Nahrstedt, 1997. A new algorithm for MPEG video encryption. University of Illinois at Urbana-Champaign.

Shannon, C.E., 1949. Communication theory of secrecy system. Bell Syst. Techn. J., 28: 656-715.

Shi, C. and B. Bhargava, 1998. A fast MPEG video encryption algorithm. Proceedings of the 6th ACM International Conference on Multimedia, Sept. 12-16, ACM, Bristol, United Kngdm, pp: 81-88. DOI: 10.1145/290747.290758

Shi, C., S.Y. Wang and B. Bhargava, 1999. MPEG video encryption in real-time using secret key cryptography. Proceedings of the International Conference on Parallel and Distributes Processing Techniques and Applications, (PDPTA' 99), the Pennsylvania State University.

Spanos, G.A. and T.B. Maples, 1995. Performance study of a selective encryption scheme for the security of networked, real-time video. Proceedings of the 4th International Conference on Computer Communications and Networks, Sept. 20-23, Las Vegas, Nevada, USA., pp: 0002-0002.

Spanos, G.A. and T.B. Maples, 1996. Security for Real-time MPEG compressed video in distributed multimedia applications. Proceedings of the IEEE 5th Annual International Phoenix Conference on Computers and Communications, Mar. 27-29, IEEE Xplore Press, pp: 72-78. DOI: 10.1109/PCCC.1996.493615

Tang, L., 1996. Methods for encrypting and decrypting MPEG video data efficiently. Proceedings of the 4th ACM international conference on Multimedia, Nov. 18-22, ACM, Boston, MA, USA., pp: 219-229. DOI: 10.1145/244130.244209

Wang, X.Y. and Q. Yu, 2009. A block encryption algorithm based on dynamic sequences of multiple chaotic systems. Commun. Nonlinear Sci. Num. Simulat., 14: 574-581. DOI: 10.1016/j.cnsns.2007.10.011

Wong, W.K., 2002. A fast chaotic cryptography scheme with dynamic look-up table. Phys. Lett. A., 298: 238-242. DOI: 10.1016/S0375-9601(02)00431-0

Xiang, T., X. Liao, G. Tang, Y. Chen and K.W. Wong, 2006. A novel block cryptosystem based on iterating a chaotic map. Phys. Lett. A., 349: 109-115. DOI: 10.1016/j.physleta.2005.02.083

Xua, S., J. Wang and S. Yang, 2008. A novel block cipher based on chaotic maps. Proceedings of the 2008 Congress on Image and Signal Processing, May 27-30, IEEE Xplore Press, Sanya, China, pp: 17-21. DOI: 10.1109/CISP.2008.409