Design of Chaotic Block Cipher Operation Mode for Intelligent Transportation Systems

Graham Thoms, Radu Muresan
School of Engineering
University of Guelph
Guelph, Canada
{gthoms, rmuresan}@uoguelph.ca

Arafat Al-Dweik
Electrical and Computer Engineering Department
Khalifa University
Abu Dhabi, United Arab Emirates
dweik@fullbrightmail.org

***Abstract*—Information security is a vital aspect of Intelligent Transportation Systems (ITS) involving public data collection. Road images captured for use as a basis of traffic manipulation in ITS should take all precautions for encrypting the wirelessly transferred image. This paper presents an Enhanced Cipher Block Chaining (ECBC) operation mode to ensure optimal cryptographic properties in a block cipher image encryption scheme. ECBC is based on the Cipher Block Chaining (CBC) operation mode and uses chaos based initialization vectors. Results show ECBC yields better information entropy and correlation coefficients than CBC.**

***Index Terms*—Intelligent Transportation Systems, Enhanced Cipher Block Chaining, Image Encryption, Chaotic Initialization Vectors**

I. Introduction

Intelligent Transportation Systems are a vital part of the evolution toward smart cities. These systems involve many forms of data collection transmitted wirelessly to central servers, which can provide a basis for making real-time decisions for highway traffic. For example, the Scalable Enhanced Road Side Unit (SERSU) [1] captures highway images for the use of adaptive speed limits and visibility indicators [2].

Since these systems are so reliant on incoming data, every measure should be taken for the data to be properly encrypted. In the case of captured highway images, image encryption algorithms that utilize block ciphers need proper block cipher operation modes. Common block cipher modes utilize randomly generated initialization vectors in order to make distinct encrypted blocks. However, if the random initialization vectors are poor, patterns emerge that break the encryption scheme. There are several image encryption schemes and operation modes based around chaotic maps [3]–[5], [7]–[11], however no block cipher operation mode takes into account the high correlation and two dimensional nature of images.

This paper presents the Enhanced Cipher Block Chaining (ECBC) operation mode, a two dimensional cipher block chaining mode suitable for image encryption schemes with chaos based initialization vectors.

II. Block Cipher Mode of Operation

Block cipher encryption and decryption techniques only ensure secure transformation of the block in question, however, for data with a large number of blocks, a mode of operation is needed. Block cipher modes outline an iterative process of combining previous block data to the next block. This process allows for encrypted plaintext to be distinct through a randomly generated initialization vector (IV). There are several block cipher modes of operation, however Cipher Block Chaining (CBC) will be of interest for this paper. CBC uses a single IV, and XOR's the previous cipher block with the current cipher block before the block cipher encryption.

III. Chaotic Systems

Chaotic systems are sets of evolutionary functions that exhibit chaotic behavior. Chaotic systems are suitable for image encryption due to high initial condition sensitivity, randomness, unpredictability and are topologically mixing [6].

The Lorenz chaotic system is characterized by three first-order differential equations representing a coordinate for the next iteration of the system. Equations for the Lorenz system dynamics are shown in (1),

$$\begin{aligned}\frac{\mathrm{d}x}{\mathrm{d}t} &= \alpha(y-x)\\ \frac{\mathrm{d}y}{\mathrm{d}t} &= x(\rho-z)-y\\ \frac{\mathrm{d}z}{\mathrm{d}t} &= xy-\beta z.\end{aligned} \tag{1}$$

The Lorenz system exhibits chaotic behavior with parameters $\alpha = 10$, $\rho = 28$ and $\beta = 8/3$, which are used in this algorithm. For initial values of x=0.01, y=z=0, dt=0.01, the output coordinates are bounded to $-20 \leq x \leq 20$, $-30 \leq y \leq 30$, $0 \leq x \leq 50$.

IV. The Algorithm

The proposed ECBC operation mode for image encryption is based on the Lorenz chaotic map and CBC operation mode, used for 8-bit grayscale images.

This research is supported by the Ministry of Transportation Ontario (MTO) Highway Infrastructure Innovation Funding Program (HIIFP) grant No. 051938. The authors of this paper thanks the MTO for their support.

A. Initialization Vector Generation

The initialization vectors are produced using the Lorenz system dynamics(1), with parameters α = 10, ρ = 28 and β = 8/3. A chaotic 8-bit positive integer is produced by combining the Lorenz system $\Phi(s)$ output coordinates $(x_s, y_s, z_s) \in \mathbb{R}$ of iteration seed $s \in \mathbb{Z}^+$. The steps for Algorithm 1 are detailed below,

1) Set initial states $x_s = 0.01$, $y_s = z_s = 0$.
2) If $s \leq 100$, iterate $\Phi(100)$, else iterate $\Phi(s)$ to generate non-zero values for x_s, y_s, z_s, using dt=0.01.
3) Iterate $s = s + 1$ to generate new values of x_s, y_s, z_s.
4) Calculate $w' = \sum(x_s, y_s, z_s)$.
5) Denote $W_R = \mod((w' \times 100000), 256)$. A gain of 100000 is needed for w' as to have the modulus greatly affected by the rapidly changing decimals values of x_s, y_s, z_s, thus yielding greater chaotic behavior.
6) Produce the resulting chaotic positive 8-bit integer W_Z, such that $W_Z = \|W_R\|$, and add to Ψ_{sl}.
7) Repeat steps 3-6 for l iterations, to produce a chaotic initialization vector $\Psi(s, l)$ of l bytes long.

Algorithm 1 Chaotic Initialization Vector

```
Input: seed $s$, sequence length $l$
Output: InitVector
$x_s \leftarrow 0.01$
$y_s \leftarrow 0$
$z_s \leftarrow 0$
$\Psi_{sl} \leftarrow 0$
if $s < 100$ then
    $s = 100$
$i \leftarrow 0$
while $i < s$ do
    iterate_lorenz_system $\Phi(s)$
$j \leftarrow 0$
while $j < l$ do
    $s \leftarrow s + 1$
    iterate_lorenz_system $\Phi(s)$
    $w' \leftarrow \sum(x_s, y_s, z_s)$
    $W_R \leftarrow \mod((w' \times 100000), 256)$
    $W_Z = \|W_R\|$
    $\Psi_{sl} \leftarrow W_Z$
```

B. Enhanced Cipher Block Chaining

The proposed ECBC operation mode is based on the traditional Cipher Block Chaining (CBC) operation mode for block ciphers, however it is extended into two dimensions. ECBC's two dimensionality allows for more suitable cipher diffusion since image information is two dimensional by nature. This means that the cipher text propagation creates much higher entropy than CBC, even with highly redundant information found in images (such as large areas with low grayscale variance).

In ECBC mode, the encryption (3) and decryption (4) of a block depends on the key, the previous encrypted block and the encrypted block spatially above the block of interest. ECBC uses a set of chaotic initialization vectors IV (2) generated from Algorithm 1 with the number of blocks widthwise n and block size l such that,

$$IV(s, l) = \{\Psi(s, l), \Psi(s + 1, l), .., \Psi(s + n, l)\}. \quad (2)$$

In ECBC encryption mode (Fig. 1(a)) (3), if each block of the plainimage $P_{ij}, ..., P_{nm}$ with number of blocks widthwise n and height-wise m is encrypted with a block cipher E_k using key k, then the resulting cipher blocks C_{ij} are,

$$\begin{aligned} &C_{ij} = E_k(P_{ij} \oplus C_{i-1,j} \oplus C_{i,j-1}) \quad \forall \quad i \geq 1, j \geq 1 \\ &C_{i0} = E_k(P_{ij} \oplus C_{i-1,j} \oplus IV_{i+1}) \quad \forall \quad i \geq 1 \\ &C_{00} = E_k(P_{ij} \oplus IV_0 \oplus IV_1). \end{aligned} \quad (3)$$

ECBC mode decryption (Fig. 1(b)) (4) uses a reverse process such that the cipher and plainimage blocks are switched, using block cipher decryption D_k with key k,

$$\begin{aligned} &P_{ij} = D_k(C_{ij}) \oplus P_{i-1,j} \oplus P_{i,j-1} \quad \forall \quad i \geq 1, j \geq 1 \\ &P_{i0} = D_k(C_{ij}) \oplus P_{i-1,j} \oplus IV_{i+1} \quad \forall \quad i \geq 1 \\ &P_{00} = D_k(C_{ij}) \oplus IV_0 \oplus IV_1. \end{aligned} \quad (4)$$

ECBC allows for plainimages to be encrypted differently based on the cipher chaining output. Since each block cipher is dependent on two previous block ciphers, the information diffusion is much better than CBC. Furthermore, multiple chaotic initialization vectors create better information confusion than simply relying on a single initialization vector, which adds to the security of the chosen image encryption block cipher algorithm.

V. Experimental Results

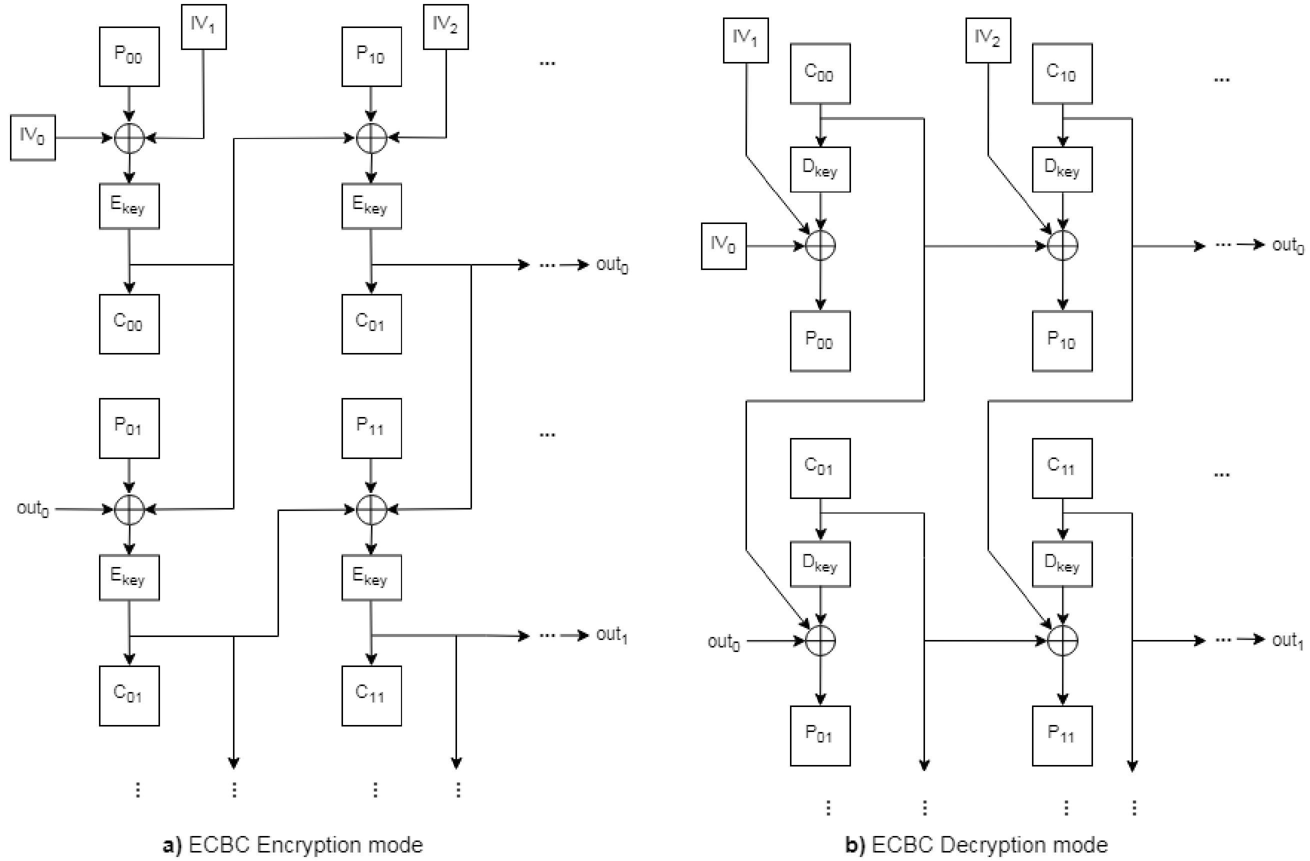
In this section, the ECBC mode with a 128-bit block size is analyzed and compared to CBC mode (with random IV) in regard to information entropy analysis and correlation coefficient analysis of different images. For the sake of ECBC and CBC comparison, no block cipher encryption/decryption algorithm will be used in the ECBC and CBC process (i.e. $E_k(P) = P, D_k(C) = C$), which will allow direct comparison of information diffusion.

A. Information Entropy

A term often used in image encryption and in cryptography is information entropy. Information entropy $H(x)$ (5) is the average amount of information from a set of data, expressed as the average logarithm of a variable X within a probability distribution $P(X)$,

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i \quad P(X) = \{p(x_1), .., p(x_n)\}. \quad (5)$$

Information entropy (5) relates the probability of a variable to the amount of information in the variable, which can be thought of as a measure of randomness. The entropy of an



a) ECBC Encryption mode

b) ECBC Decryption mode

Fig. 1: ECBC diagram of encryption mode (a) and decryption mode (b).

image can be directly calculated from it's histogram, since the histogram directly correlates with the probability distribution of the image. For a cryptic image scheme, extremely high information entropy is needed (bounded by codeword length) since high entropy will likely produce patternless data (uniform histogram distribution).

As shown in Table I, ECBC yields consistently higher information entropy than that of CBC, resulting in visually patternless data. Even with highly correlated images, ECBC still produces high entropy output images that appear almost identical to lower correlated images using ECBC.

B. Correlation Coefficient

In Table II, ECBC yields the smallest correlation coefficient amongst all pixel pairs in each image in Fig. 2, even with highly correlated input images such as Fig. 2b. This can clearly be seen in Fig. 2; the CBC mode (center column) results in repetitive patterns as oppose to ECBC which produces patternless data. This is because ECBC can propagate more initialization vectors faster through the image in two dimensions, which is advantageous when dealing with encryption of highly correlated data such as images.

TABLE I: Information Entropy Comparison

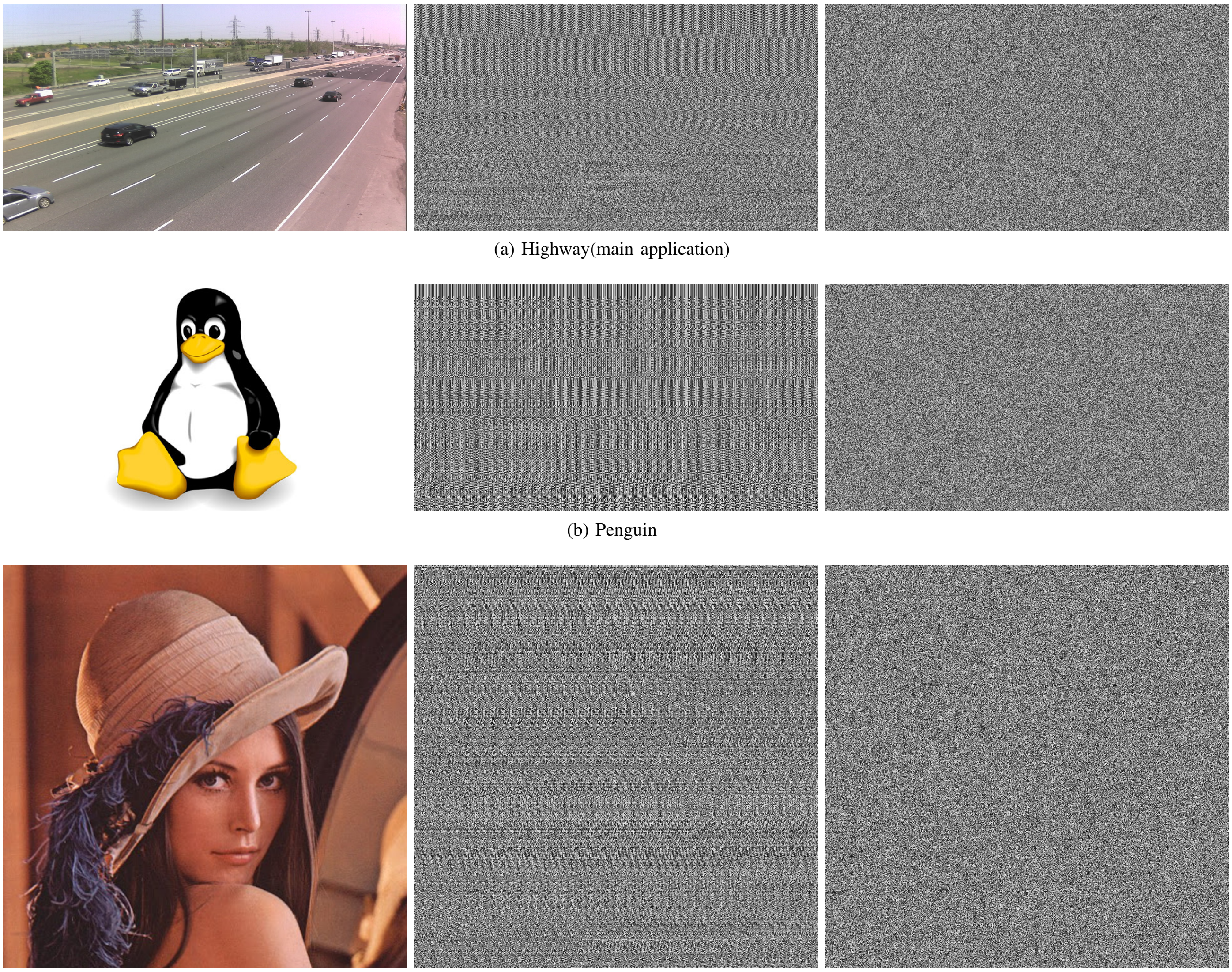
Image	**CBC**	**ECBC**
Highway	7.99886	7.99978
Penguin	7.91526	7.99984
Lena	7.99962	7.99981

TABLE II: Correlation Coefficient Comparison

Image	**CBC**	**ECBC**
Highway	0.006435	0.000475
Penguin	0.123136	0.000585
Lena	-0.002995	-0.001653

VI. Conclusion and Future Work

A major concern in Intelligent Transportation Systems is the security of surveillance data using image encryption algorithms and associated modes of operation. An enhanced version of cipher block chaining mode for block cipher encryption is presented called ECBC. The algorithm extends CBC to two dimensions with the use of initialization vectors based on the Lorenz chaotic map. Obtained Results show that ECBC gives better cryptographic properties, such as higher information entropy and lower correlation coefficients than CBC. In future work, the new block cipher encryption mode will be utilized in an image encryption scheme for the SERSU on multiple highways.



(a) Highway(main application)

(b) Penguin

(c) Lena

Fig. 2: Various image used in encryption mode experimentation with original picture (left column), CBC (center column) and ECBC (right column). It should be noted that no block cipher encryption/decryption algorithms were used, only modes were tested with initialization vectors and original images.

References

[1] A. Al-Dweik, R. Muresan, M. Mayhew and M. Lieberman, “IoT-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems”, *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2017.

[2] L. Yang, “Comprehensive visibility indicator algorithm for adaptable speed limit control in intelligent transportation systems”, M.A.Sc. thesis, University of Guelph, 2018.

[3] T. Hue, T. Hoang and S. Assad, “Design and implementation of a Chaotic Cipher block chaining mode for image encryption”, *2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, 2013.

[4] R. Guesmi, M. Farah, A. Kachouri and M. Samet, “A novel design of Chaos based S-Boxes using genetic algorithm techniques”, *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, 2014.

[5] J. Fridrich, “Image encryption based on chaotic maps”, *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation. 1997*

[6] N. Thein, H. Nugroho, T. Adji and I. Mustika, “Comparative Performance Study on Ordinary and Chaos Image Encryption Schemes”, *2017 International Conference on Advanced Computing and Applications (ACOMP)*, 2017.

[7] G. Jakimoski and L. Kocarev, “Chaos and cryptography: block encryption ciphers based on chaotic maps”, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 2, pp. 163-169, 2001.

[8] E. Yavuz, R. Yazc, M. Kasapba and E. Yama, “A chaos-based image encryption algorithm with simple logical functions”, *Computers & Electrical Engineering*, vol. 54, pp. 471-483, 2016.

[9] W. Yu and J. Cao, “Cryptography based on delayed chaotic neural networks”, *Physics Letters A*, vol. 356, no. 4-5, pp. 333-338, 2006.

[10] Y. Abanda and A. Tiedeu, “Image encryption by chaos mixing”, *IET Image Processing*, vol. 10, no. 10, pp. 742-750, 2016.

[11] J. Fridrich, “Symmetric Ciphers Based on Two-Dimensional Chaotic Maps”, *International Journal of Bifurcation and Chaos*, vol. 08, no. 06, pp. 1259-1284, 1998.