Cifrado Parcial de Bit-Streams de video utilizando Mapas Caóticos Acoplados

Marcos Daniel Calderón Calderón
Maestría en Ciencias de la Computación
Centro de Investigación en Matemáticas (CIMAT)
Guanajuato , Gto.
marcos.calderon@cimat.mx

***Resumen*—Debido a la instraestructura que se a creado para lograr una comunicación eficiente, han surgido nuevas tecnologías para lograr dica comunicación. Una de ellas: servicios de video streaming sobre IP presenta diversos retos que se pueden investigar: calidad, requerimientos en tiempo real y seguridad. Se propone un esquema novedoso para la transmisión de streams de bits de una manera segura y rápida. Ésta se basa en en difusión de errores y tener un segmento de tamaño variable. La difusión de los datos cifrados y los mecanismos de mezclado están basados en operaciones aleatorias utilizando generadores de números peseudoaleatorios computacionalmente seguros. El esquema es ubicuo a los usuarios finales y puede ser desplegado en cuelquier nodo de la red. Este también involucra bit streams comprimidos si requerir una decodificación. BLA BLA, FALTA ALGO.**

I. Introducción.

A causa de los recientes desarrollos en el cambo de comunicaciones multimedia, aplicaciones tales como Voz sobre IP (VoIP), conferencias por video, aprendizaje electrónico y TV/HDTV son ahora parte de la vida diaria. Actualemtne, casi todas las personas están involucradas en una red de información donde se pueden hacer negocios el línea, y tener acceso a noticias, cuentas de banco desde la oficina o el hogar. Estas comodidades digitales tienen algunos riesgos inherentes: las redes de comunicación son vulnerables a ataques. Es necesario diseñar sistemas rápidos o seguros. De cualquier manera, en el caso de datos multimedia, la seguridad demanda

II. Esquema propuesto.

El proceso de cifrado comienza justo después de el proceso de empaquetado, en el cual, los fragmentos del video (VLC bitstream) varían de 300 bytes a 1400 bytes, dependiendo de las propiedades de transmisión del medio. Nuestro esquema propuesto cifra los bitstreams VLC codificados realizando las siguientes operaciones dinámicas sobre cada paquete RTP: random bits flipping and segment shuffling.La posición de los bitsa ser flipped, localizaciones de los segmentos a ser suffled, y el tamaño de segmento depene de un generador de números aleatorios seguro. El esquema propuesto está formado de los siguientes componenetes:

- Generador de números pseudoaleatorios seguro basado en mapas caóticos acoplados.
- Bit flipping.
- Segment Shuffling.

II-A. Secure random number generator based on chaotic maps.

La seguridad del esquema propuesto a diferentes ataques depende principalmente de la robustez del PRNG. Este esquema puede trabajar con cualquier PRNG siempre que la semilla no pueda ser determinada por una secuencia generada que se haya roto. Los actuales PRNG no son buenos candidatos para ser utilizados en este esquema debido a su dependencia sobre la semilla de longitud fija, así como la falta de flexibilidad para controlar dinámicamente la seguridad del sistema. Desarrollamos uno PRNG novedoso basado en una red de N mapas caóticos discretos que interactúan de una manera dinámica como un sistema pero mantenienso su propia identidad (el uso de sólo un mapa no da suficiente seguridad al sistema). Sistemas Dinámicos Caóticos (DCS) tienen muchas de las propiedades que se necesitan en Criptografía: el más importante es sensibilidad a los parámetros, sensibilidad a las condiciones iniciales y trayectorias impredecibles. Las primeras dos propiedades están relacionadas con la difusión, y la última con el fenómeno de confusión entendíéndolo en la nomenclatura criptográfica.

La confusión está destinada a hacer que la relación entre el texto cifrado y el texto plano se estadísticamente independiente, mientras que la difusión está destinada a extender la influencia de un sólo dígito del texto plano sobre múchos dígitos de texto cifrados para esconder la estructura estadísrica de el texto plano. Estas propiedades han sido la base para desarrollar seguridad analógica y sistemas digitales de comunicación.

Las actuales investigaciones en sistemas caóticos están enfocadas en dos principales cuestiones: Esquemas basados en perturbación y mapas caóticos basados en redes. Esquemas basados en perturbación transforman los ciclos estables caóticos en ciclos no estables sl perturbar una trayectoria. Una red de mapas caóticos o mapas acoplados utilizan un array de mapas caóticos que están relacionados por una transformación sobre alguna vecindad del array. En este trabajo, se utliza CML (Coupled Map Lattices) para desarrollar un PRNG que tiene las propiedad de robustez necesaria para el cifrado de datos. Y tiene buenos resultados para resistir ataques con texto plano conocido o diferencial.

El PRNG presentado se basa en una red de N mapas caóticos:

$$X_{i,j} = (1-\epsilon) f(X_{i,j-1} + \epsilon H(X_{N,j-1})) \qquad (1)$$

$$H(X_{i,j-1},...,X_{N,j-1}) = \sum_{i=1}^{N} w_i X_{i,j-1} \quad (2)$$

Los j estados en la red caótica representan la interacción pesada entre cada mapa individual $f(X_{i,j-1})$ (término local) y la función de acoplamiento H (puede ser un término de interacción lineal o no lineal) conpeso w_i, tales que $\sum_{i=1}^{N} w_i$, y $N \leq 8$. CUando el peso ϵ es débil (una magnitud pequeña), el sistema puede ser considerado como un mapa local perturbado por contribuciones de otros sitios, manteniendo así sus principales propiedades individuales. De otro modo, cuando ϵ es grande, el sistema alcansa un comportamiento asintótico colectivo (no deseado) caracterizado por ciclos caóticos periódicos e intermitentes (que es lo que se quiere evitar).

Por su simplicidad matemática, la selección para $f(X_{i,j})$ es el bien conocido mapa logístico representado por la siguiente expresión:

$$X_{i,j} = f(X_{i,j-1}) = \lambda X_{j-1}(1-X_{j-1}), \quad \lambda \in [1,4), \quad X \in (0,1) \quad (3)$$

Donde λ representa el parámetro caótico y X la variable de estado, Cuando λ se incremente de 1 a 4, el mapa experimenta una diplicaci[on del período caótico. En particular para $\lambda \geq 3{,}5699$ (conocido como el punto de acumulación), este presenta un comportamiento caótico, sin embargo hay muchas ventanas periódicas indeseables con cortos periodos que aparecen de manera abrupta. Una ventana muy conocida de poeriodo 3 aparece cuando $\lambda = 1 + \sqrt{8} = 3{,}828$. LOs puntos fijos ($f(X) = X$) también aparecen en $X = 0$ y em $X = (\lambda - 1)/\lambda$ los cuales definen un patron regular en el mapa log[istico. Para mantener la dinámica caótica adecuada en el mapa logístico, se evitan valores iniciales malos para X y para λ y asegurar el uso de al menos 8 mapas caóticos para incrementarel tamaño de ciclo. Es importante señalar que cualquier mapa caótico en la literatura puede ser utilizado como el sustituto de la ecuación caótica. La seguridad se basa en el propio régimen, en lugar del mapa caótico.

Como se mencionó antes, la principal razón para desarrollar un propio esquena PRNG es administrar la seguridad del sistema para crear una saeñal caótica libre de ciclos (lo más cercano posible) con la capacidad de manejar comunicaciones multimedia de términos grandes como VoIP y video streaming (este último puede durar desde minutos hasta horas). La seguridad es controlada al cambiar el número de mapas caóticos y aplicar perturbaciones de manera periódica al estado del sistema (variables, parámetros, funcion de acoplado, peso $epsilon$, ...). Adicionalmente, se incluyen datos de entrada previos (llamados texto plano) como una parte de la función de acoplamiento H para permitir difusión de la información sobre el texto cifrado de la siguiente manera:

$$H_j(X_{1,j},...,X_{N,j},P) = \sum_{i=1}^{N} w_l X_{l,j} + w_{N+1} P_j^{'} \quad (4)$$

$$P_j^{'} = \frac{\left(\sum_{i=1}^{M} P_{j-1,l}^{32}\right) \mod H_{j-1}^{'}}{H_{j-1}^{'}} \quad (5)$$