UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

I+D INVESTIGACIÓN Y DESARROLLO

El código Hamming en la cuarta revolución industrial

The Hamming code in the fourth industrial revolution

Andrés Fabian Laguna Garzón[1], Brayan David Ruiz Rubiano[2], Iván Alejandro List Cabanzo[3], Duvan Leonardo Chávez Buitrago[4]

Para citar este articulo: A. F. Laguna Garzón, B. D. Ruiz Rubiano, I. A. List Cabanzo, D. L. Chávez Buitrago, "El código Hamming en la cuarta revolución industrial". *Revista Vínculos*, vol. 17, no. 2, pp. 104-111, julio-diciembre, 2020. https://doi.org/10.14483/2322939X.15133

Recibido: 13-10-2020 / Aprobado: 20-11-2020

Resumen

En este artículo se describe el código Haming, como método de detección y corrección de errores en las comunicaciones y almacenamiento de datos. En donde se presenta una breve historia del código Hamming, verificación de paridad y códigos de redundancia, luego se menciona el funcionamiento básico del código Hamming y adicionalmente se describen de forma general otros métodos de corrección de errores. Finalmente se presentan algunas aplicaciones del código Hammig en el marco de la cuarta revolución industrial, en la que se encuentran: Internet de las Cosas, Redes de Sensores, Códigos QR, Estenografía y Reconocimiento de patrones.

Palabras clave: Corrección de Errores, Código Hamming, IoT, distancia de Hamming.

Abstract

This paper describes Haming code as a method of detecting and correcting errors in communications and data storage. A brief history of the Hamming code, parity verification and redundancy codes is presented, then the basic operation of the Hamming code is mentioned and other error correction methods are described in general. Finally, some applications of the Hammig code are presented within the framework of the fourth industrial revolution, in which they are found: Internet of Things, Sensor Networks, QR Codes, Stenography and Pattern Recognition.

Keywords: Error Correction, Hamming Code, IoT, Hamming Distance.

[1] Ingeniería en Telemática, Tecnólogo en Sistematización de datos, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Colombia, Bogotá. Correo electrónico: aflagunag@correo.udistrital.edu.co

[2] Ingeniería en Telemática, Tecnólogo en Sistematización de datos, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Colombia, Bogotá. Correo electrónico: bdruizr@correo.udistrital.edu.co

[3] Ingeniería en Telemática, Tecnólogo en Sistematización de datos, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Colombia, Bogotá. Correo electrónico: ialistc@correo.udistrital.edu.co

[4] Ingeniería en Telemática, Tecnólogo en Sistematización de datos, Universidad Distrital Francisco José de Caldas Facultad Tecnológica, Colombia, Bogotá. Correo electrónico: dlchavezb@correo.udistrital.edu.co

1. Introducción

Actualmente, los códigos de Hamming son primordiales en la teoría de la codificación y tienen una gran cantidad de aplicaciones prácticas. En concreto, los códigos correctores de errores tienen un papel esencial en la vida cotidiana y son usados por múltiples dispositivos de red en la capa de enlace de datos del modelo OSI, memorias, comunicaciones vía satélite incluso Biosensores. En un sistema de transmisión de datos la información es muy vulnerable y propensa a errores. Los métodos de detección de errores permiten conocer si hubo o no un error en la cadena de datos recibidos, pero no están en condiciones de subsanar dichos errores. Entonces, cuando se detecta un error por medio de un método de detección de errores, la manera de reparar la información es que el receptor pida una retransmisión de la información.

Por medio del código de corrección de errores de Hamming es posible no solo detectar, sino también enmendar los errores ocurridos sobre la cadena de información en el receptor. La detección y corrección de errores en un sistema de transmisión de información depende de la inclusión de redundancia sobre la cadena de transmisión, es decir, a los datos se les añade información que permite dar una pequeña descripción de los mismos datos. La cantidad de errores a detectar o corregir en un sistema con código de Hamming depende de la distancia de Hamming “d”.

2. Contexto e Historia

Antes de la aparición del código Hamming en 1950 propuesta por Richard Hamming [1], otros investigadores ya habían encontrado otros métodos para detectar errores, no con los beneficios o ventajas de Hamming, pero si jugaron un papel importante al proporcionar las bases e inicios de los futuros códigos y de sus mejoras. A continuación, se presentan los métodos más destacados y que fueron usados antes del código Hamming:

- **Paridad:** Se obtiene añadiendo a las palabras de un código de distancia mínima uno, un dígito que se denomina de paridad, es decir que se agrega un bit adicional a un cierto número de bits de datos denominado palabra código (generalmente 7 bits) cuyo valor (0 o 1) es tal que el número total de bits 1 es par. Para ser más claro, 1 si el número de bits en la palabra código es impar, 0 en caso contrario. [2]
- **Redundancia:** Consiste en enviar dos veces cada unidad de datos, de forma que el dispositivo receptor puede hacer una comparación bit a bit entre ambos datos y detectar si ha habido errores, para corregirlos con el mecanismo apropiado.[3]
  Existen cuatro tipos de cuatro de comprobación de redundancia: verificación de redundancia vertical (VRC - corresponde a la verificación de paridad), verificación de redundancia longitudinal (LRC) y verificación de redundancia cíclica (CRC).
  LRC: no consiste en verificar la integridad de los datos mediante la representación de un carácter individual, sino en verificar la integridad del bit de paridad de un grupo de caracteres.
  CRC: consiste en la protección de los datos en bloques, denominados tramas. A cada trama se le asigna un segmento de datos denominado código de control (al que se denomina a veces FCS, secuencia de verificación de trama, en el caso de una secuencia de 32 bits, y que en ocasiones se identifica erróneamente como CRC).[2]

3. Codificación de Hamming

Los códigos Hamming son códigos lineales de bloque binarios que pueden corregir un error o detectar dos errores en una palabra de n bits. Sin embargo, no se distingue entre fallos de 2 bits y de un bit (para lo que se utiliza Hamming extendido).
Generalmente el código Hamming se representa en un valor (n, d), el valor (7, 4) representa a un mensaje que tiene cuatro bits de datos (d) y va a ser transmitido como una palabra de código de 7 bits con la adición de tres bits de control de error. A esto se le conoce como código Hamming (7, 4). Los tres bits que se agregan son

ISSN 1794-211X • e-ISSN 2322-939X • Vol 17, No 2 (julio-diciembre 2020). pp. 104-111. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

bits de paridad (P), donde se calcula la paridad de cada uno de los diferentes subconjuntos de los bits del mensaje [4].

Consideremos el mensaje en binario "0001" que se desea codificar con Hamming (7,4), en la tabla 1 se observa la posición de los bits, d para indicar los bits de datos y la p para indicar los bits de paridad. Los bits cuya posición es potencia de 2 es decir (1,2 y 4) corresponden a bit de paridad, y el resto de las posiciones (3, 5, 6, 7) corresponden a los bits de datos.

Para cada bit de paridad se debe comprobar unos determinados bits, dependiendo de la posición que ocupe y siguiendo las normas del siguiente ejemplo. Por ejemplo, la posición es 2, desde está misma posición se seleccionan 2, luego dejará 2 sin seleccionar, seleccionará los siguientes 2, para luego dejar los siguientes 2 sin seleccionar, y así hasta que se complete la longitud del mensaje. Del mismo modo para todas las posiciones que son potencias de dos.

Para realizar la comprobación se utiliza la compuerta XOR con los bits anteriormente seleccionados de acuerdo a la posición de la paridad, el resultado ira en la posición de la paridad, de esta manera es la codificación Hamming (7,4) el resultado se puede observar en la tabla1.

Tabla 1. Codificación Hamming (7,4) según paridad.

Posición de los bits/ Paridad	**P1**	**P2s**	**D1**	**P3**	**D2**	**D3**	**D4**
Bits			0		0	0	1
P1	1		0		0		1
P2		1	0		0	1	
P3				1	0	0	1
Mensaje Codificado	**1**	**1**	**0**	**1**	**0**	**0**	**1**

Fuente: elaboración propia.

4. Otros métodos de Corrección de Errores

A lo largo de los años el campo de aplicación de los códigos de corrección de errores ha ampliado considerablemente logrando así que más matemáticos y científicos se interesen en investigar algoritmos cada vez más eficientes. De esta manera a continuación se presenta de forma paralela tres diferentes códigos detectores de errores; códigos BCH, Reed-Solomon y convolucionales.

- **BCH:** Hace referencia al conjunto de códigos cíclicos binarios basado en códigos Hamming que tienen capacidad de corregir errores múltiples, aunque tiempo después fueron generalizados para alfabetos en vez de binarios. Su nombre hace referencia a los tres autores R. C. Bose, A. Ray-Chaudhuri y A. Hocquenghem (BCH).
  Es considerado como uno de los mejores códigos longitudes de bloque moderadas, de hasta varias centenas o pocos miles de bits, por esta razón se han desarrollado para ellos algoritmos eficientes de decodificación, aunque es importante mencionar el problema que se presenta con longitudes de bloque significativamente grandes.
  Este error se refiere a que, en una codificación fija, la distancia no aumenta en proporción con la longitud, he de ahí que, en un bloque muy grande, la distancia estará por debajo de lo requerido [5].
- **Reed-Solomon (RD):** Es un esquema decodificación de bloque que puede corregir ráfagas de errores hasta un cierto límite determinado por la cantidad de redundancia 15 con que se diseñe el código. Aunque el procesado computacional de estos códigos es sumamente complejo, ha sido implementado en circuitos integrados en gran escala (VLSI) y en la actualidad se incluye en el hardware de sistemas a un costo relativamente bajo [6]. La definición más acertada para el conjunto de códigos Reed– Solomon es mediante la relación existente con los códigos BCH. Un código Reed–Solomon (RS) sobre el cuerpo q es un código BCH de longitud q – 1[5]

ISSN 1794-211X • e-ISSN 2322-939X • Vol 17, No 2 (julio-diciembre 2020). pp. 104-111. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

De esta forma la longitud de un código Reed-Solomon es el número de elementos no nulos del cuerpo base; y, naturalmente, q =/ 2, es decir, los códigos RS no son binarios, sistemáticos, cíclicos y lineales que operan sobre símbolos consistentes de varios bits y tienen buenas propiedades para la corrección de errores en grupo o ráfaga ya que la corrección se realiza a nivel de símbolo.

- **Convolucionales:** Se basa en principios muy diferentes a los de los códigos de bloque. En éstos, el proceso de detección y corrección de errores opera de forma continua sobre la secuencia de datos de entrada al codificador, a nivel de bit, o de bloques pequeños de datos. Una característica adicional que la distingue es que ésta opera únicamente sobre la información presente a la entrada del codificador, es decir, no tiene en cuenta la información pasada y, por tanto, no tiene memoria. [6]

5. Aplicaciones del Código Hamming

Principalmente el código Hamming y sus algoritmos derivados tienen aplicación en las comunicaciones digitales y en sistemas de almacenamiento de datos. A pesar de ser algoritmos longevos, en la actualidad son muy utilizados en distintos campos: Su flexibilidad y fácil implementación lo hace un candidato para implementarse en cualquier tecnología. A continuación, se describen algunas aplicaciones del Código Hamming.

5.1. Aplicaciones en IoT, Sistemas Embebidos y Electrónica

En tiempos de la industria 4.0 temas como el internet de las cosas (IoT – Internet of Things), redes de sensores y sistemas embebidos han tomado relevancia, por ese motivo se han desarrollado tecnologías a la medida de las necesidades que ha ido surgiendo. Uno de los retos que ha enfrentado el IoT es la eficiencia energética, el consumo de memoria y el ancho de banda en los dispositivos y sensores, ya que al ser dispositivos instalados en sitios remotos es necesario garantizar la vida útil de las baterías, el bajo consumo de memoria, procesamiento y ancho de banda al transmitir la información.

El software y los sistemas embebidos han evolucionado rápidamente en los últimos años, los conceptos de interconexión entre aparatos inteligentes, domótica y ciudades inteligentes son más comunes en la actualidad, estas tecnologías han permitido la comodidad y eficiencia en las tareas de las personas [7], sin embargo, estas áreas son muy conocidas por su falta de seguridad, la información que se transmite desde los distintos dispositivos puede ser interceptada y fácilmente legible para un delincuente informático, provocando resistencia a utilizar estos artefactos.

Existen varios ejemplos de la implementación del código Hamming en proyectos que involucran electrónica de bajo consumo como lo es por ejemplo lo muestran los autores [8], donde se presenta la implementación y aplicación de un código de Hamming (7,4) a un transmisor digital inalámbrico en una tarjeta de desarrollo con tecnología de lógica programable de tipo FPGA.

Como lo menciona Rubén Martínez, en su proyecto "Diseño e implementación de un control remoto seguro ante interceptación para puerta levadiza de garaje"[4], en el que expone un sistema de control para puertas de garaje donde consideró pertinente agregar una redundancia para asegurar la integridad y robustez de código en la comunicación, su sistema utiliza un protocolo de comunicación con mensajes de 8 bytes y 16 bytes de variable de inicialización, en este caso como el bloque de datos es pequeño, decidió implementar el código Hamming (7,4) debido a que encontró una eficiencia de 57.14%, que asegura integridad de la información frente a ruido, asumiendo que en el canal la probabilidad de error en un bit es menor a 0.5. Adicionalmente, optimizo el mencionado código Hamming empleando una matriz de entrelazado de 8x8 bits, lo cual permite corregir errores aleatorios y errores en ráfagas de hasta 8 bits. Con esta técnica se obtuvo código de un total de 48 bytes, los

ISSN 1794-211X • e-ISSN 2322-939X • Vol 17, No 2 (julio-diciembre 2020). pp. 104-111. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

cuales incluyen mensaje cifrado y redundancia, la eficiencia en este caso es del 50%.

También en otro proyecto[9] se implementa un sistema SCADA por sus siglas (Supervisory Control And Data Acquisition) que sirve para el monitoreo y control a nivel industrial, en este caso el sistema SCADA se realizó para el control de un robot tipo 3GDL (3 grados de Libertad) en que se desarrolló un método tolerante a fallas basado en el código Hamming (7,4) para el protocolo de comunicación industrial MODBUS, en donde después de analizar las diferentes técnicas de corrección de errores, se escogió el código haming por su sencillez de aplicación con respecto a otras técnicas y por la necesidad de corregir únicamente un bit en los datos que se intercambian entre maestro y esclavo.

Al usar el código de Hamming en este tipo de aplicaciones se evidencia la versatilidad del mismo en campos como la electrónica, sensores y microcontroladores

Nadie en 1950 podía haber predicho que se utilizaría el código Hamming para garantizar la fiabilidad de los datos a bordo de los nanosatélites. Así como lo muestra Caleb Hillier y Vipin Balyan [10], en el artículo "Error Detection and Correction On-Board Nanosatellites Using Hamming Codes", en este se analiza y compara diferentes tipos de codificaciones de Hamming, aplicado a la corrección de errores a bordo del nanosatélite ZA-cube 2 que utiliza dispositivos programables FPGA (Field-Programmable Gate Array).

En el artículo se demuestra mediante una simulación en el software MatLab que al hacer una optimización al código haming original, se obtuvo una versión más efectiva, esta fue Hamming [16, 11, 4], que es una versión del código Hamming (15, 11) extendida, el código mencionado garantiza la corrección de un solo error y la detección de un doble error.

El uso de este código ofrece un poco consumo de memoria y un tiempo de procesamiento muy pequeño, garantizando que el algoritmo consumirá una cantidad mínima de energía. De este modo Hamming se convierte en candidato ideal para la corrección de errores aplicaciones de estas características.

La gestión de claves segura y eficaz para la autenticación es un requisito previo a las operaciones de seguridad, en este contexto, se implementan protocolos de gestión de claves interactivos, si dos dispositivos requieren una comunicación segura se utilizará PMK (Pairwise Master Secret) para la generación te tiquetes además de autenticación y PFS (Perfect Forward Secrecy) que permite la administración de claves de sesión [11], la comunicación no sería posible sin una codificación adecuada, al utilizar estos protocolos existirá una conexión constante entre las máquinas involucradas, cualquier modificación o perdida de datos significaría un problema de integridad, es aquí donde la codificación Hamming crea una alternativa óptima para el transporte de paquetes de datos, dependiendo de la capacidad de procesamiento de los dispositivos conectados, se fija un tamaño de bits especifico junto a los bits de paridad y se realiza el proceso de codificación/decodificación añadiendo una capa de seguridad a la sesión.

El tema de consumo energético, en las redes de sensores inalámbricas es crucial, así lo mencionan los autores [12] en donde se estudia algunas estrategias para la implementación de sistemas correctores de errores en Redes de Sensores Inalámbricas. En el artículo da una perspectiva desde el punto de vista energético, por lo cual se analiza algunos modelos energéticos para encontrar el equilibrio entre consumo de energía y tasa de corrección de bits. El rendimiento de las técnicas de corrección de errores se evalúa sobre la base de modelos energéticos y criterios de optimización establecidos. El mismo código corrector de error no puede implementarse en todos los escenarios,

La evaluación de esta investigación arrojó que los códigos correctores de datos más eficientes a nivel de tasa de corrección, son óptimos para ser usados a nivel de extremo a extremo de toda la red de sensores, mientras que los códigos simples son mejores para el control de errores de nodo a nodo ya que consumen menos energía en su funcionamiento.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 17, No 2 (julio-diciembre 2020). pp. 104-111. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

En este caso en particular el código Hamming (7, 4) es el más eficiente desde el punto de vista energético para valores de tasa de error binario bajos. De este modo a pesar que el rendimiento del código Hamming es inferior a todos los códigos de corrección de errores observados, su sencillo decodificador consume menos energía y, por lo tanto, alarga la vida útil de las baterías en las redes de sensores inalámbricas.

Por lo tanto, es muy difícil elegir un código de corrección de errores óptimo para las comunicaciones en redes de sensores inalámbricas en el que se tengan en cuenta tanto el rendimiento como el consumo de energía.

5.2. Esteganografía

Una nueva técnica de esteganografía de imágenes con un esquema de incrustación adaptativa que combina los métodos de detección de bordes y códigos híbridos de Hamming para ocultar un mensaje secreto dentro de una ilustración. Se utiliza el algoritmo de detección de bordes de Canny para identificar el grado de nitidez de un bloque debido al funcionamiento del sistema visual del ser humano que es más sensible a las zonas lisas que a las zonas nítidas de la imagen; por tanto, incrustar información confidencial en la imagen de acuerdo con el grado de nitidez de las zonas de la imagen proporcionara una calidad visual superior a la imagen resultante del algoritmo Stego.

El volumen de datos incrustados en cada bloque depende de la nitidez del bloque, es decir, cuanto más nítido es el bloque, más datos se incrustan en él. Para incrustar un mensaje secreto en una imagen, se utilizan las regiones más nítidas, luego procede gradualmente a las regiones menos nítidas y así reduce significativamente la distorsión de la imagen generada por el algoritmo Stego, haciéndola imperceptible. [13]

5.3. Agregando una capa de seguridad a los códigos QR

Los códigos QR (Quick Response) son utilizados en distintos ámbitos debido a su gran capacidad de información, fuerte capacidad de corrección de errores y rápida velocidad de lectura. Sin embargo, la codificación pública del código QR hacen que sus contenidos sean inseguros, se presenta entonces como una solución a este problema, un nuevo tipo de código QR con información de tres capas que utiliza las características del código Hamming y el mecanismo de corrección de errores del código QR para proteger la información secreta. La información de primera capa, es decir, la información pública, puede ser decodificada por cualquier lector QR estándar. Se realiza la operación XOR sobre todas las acciones para obtener la información de la segunda capa y finalmente, los píxeles de la misma posición en todas las acciones se toman como un conjunto de códigos Hamming respectivamente, la información de la tercera capa se extrae mediante una operación de multiplicación de matriz. En comparación con otros esquemas relacionados, el esquema tiene una ventaja de contar con una alta eficiencia de integración de la información y una gran robustez frente a los ataques comunes de post procesamiento de imágenes. [14]

5.4 Comparación biométrica de iris

En la comparación de iris, la métrica más popular es la distancia Hamming, dado que en la etapa de comparación resulta tener mejor rendimiento, los subconjuntos Hamming de longitud adaptable basados en la densidad de los bits cubiertos, cada subconjunto es capaz de expandirse y unirse a las partes vecinas a la derecha o la izquierda, aumentando la precisión computacional de la distancia de Hamming y mejorando el rendimiento de las coincidencias encontradas del código del iris; resultado de una investigación realizada en el instituto de automatización de la academia China de ciencias (CASIA) muestra un rendimiento del 99,96% y una tasa de rechazo del 0,06% [15]

5.5 Reconocimiento de patrones

Para enfrentar el problema de escalabilidad en datos masivos, se aboga por una mayor distancia de los códigos binarios, ya que permite obtener datos exactos y al mismo tiempo comparte la ventaja de

ISSN 1794-211X • e-ISSN 2322-939X • Vol 17, No 2 (julio-diciembre 2020). pp. 104-111. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

almacenamiento eficiente, la distancia Hamming en estos códigos permite encapsular estos datos, realizar un hash sobre cada bit y finalmente analizarlos eficientemente sin temor a sesgos por errores de codificación. Con el método llamado Parametric Local Multiview Hamming metric (PLMH), que aprende la métrica multivista basada en un conjunto de funciones hash locales para adaptarse localmente a la estructura de datos de cada modalidad. Para equilibrar la localidad y la eficiencia computacional, se parametriza la matriz de proyección hash de cada instancia, con límite de error de aproximación garantizado, como una combinación lineal de proyecciones hash básicas asociadas con un pequeño conjunto de puntos de anclaje. La información de supervisión débil (información lateral) proporcionada por las restricciones de pares y trillizos se incorpora de manera coherente para lograr un hash semánticamente efectivo. Un algoritmo local de gradiente conjugado óptimo con rotaciones ortogonales está diseñado para aprender cada para cada bit, y los códigos generales de hash se guardan de manera secuencial para minimizar progresivamente el sesgo. Las evaluaciones experimentales de las tareas de recuperación de efectos cruzados demuestran que PLMH se desempeña de forma competitiva frente a los métodos más modernos.[16]

6. Conclusiones

El código Hamming muestra ser flexible para ser implementado en múltiples aplicaciones, además demuestra ser eficiente para resolver errores de un conjunto de bits siempre y cuando ese error solo sea uno por conjunto.

A nivel de la Cuarta Revolución Industrial, el artículo nos muestra la posibilidad de optimizar recursos a la hora de implementar el código Hamming como método corrector de errores, en aplicaciones como Edge Computing, Redes de Sensores, IoT y Ciudades Inteligentes. Este tipo de análisis permite abrir nuevas vías para establecer un estándar de sistemas correctores de errores para las aplicaciones para tecnologías de la cuarta revolución industrial.

Referencias

[1] R. W. Hamming, “Error Detecting and Error Correcting Codes,” Bell System Technical Journal, vol. 29, no. 2, pp. 147–160, 1950.

[2] “Códigos detectores y correctores de error”. Fundamentos de la Informática. Departamento de Informática. Universidad de Vallalodid. 2009. [En línea]. Disponible en: https://www.infor.uva.es/~cevp/FI_I/fichs_pdf_teo/FI_I_Tema8_CodCorr.pdf

[3] “Detección y corrección de errores. Sistemas de Multiplexado”. En línea]. Disponible en: https://sites.google.com/site/sistemasdemultiplexado/home

[4] R. P. Alvarado Martínez, “Diseño e implementación de un control remoto seguro ante interceptación para puerta levadiza de garaje,” Nov. 2011. [En línea]. Disponible en: http://hdl.handle.net/20.500.12404/906

[5] C. López, M. Veiga, “Teoría de la Información y Codificación”. Universidad de Vigo, 2002.

[6] C. Vega, “Codificación de Canal”. Universidad de Cantabria, 2015.

[7] T. Chantem, N. Guan, and D. Liu, “Sustainable embedded software and systems,” Sustainable Computing: Informatics and Systems, vol. 22, pp. 152–154, 2019.

[8] L. Á. Reyes Cruz , J. C. Pedraza Ortega , J. M. Ramos Arreguín , G. Díaz Delgado, and S. Tovar Arriaga , “Diseño e Implementación de un Transmisor Digital Inalámbrico mediante Tecnología FPGA,” La Mecatrónica en México, vol. 04, no. 3, pp. 77–89, Sep. 2015.

[9] H. Torres Salamea, D. D. Toledo Torres, and P. D. Urgilés Cárdenas, “Diseño e implementación de un sistema SCADA mediante protocolo

ModBus con comunicación inalámbrica para el control de un robot," 2017.

[10] C. Hillier and V. Balyan, "Error Detection and Correction On-Board Nanosatellites Using Hamming Codes," Journal of Electrical and Computer Engineering, vol. 2019, pp. 1–15, 2019.

[11] L. Celia and Y. Cungang, "(WIP) Authenticated Key Management Protocols for Internet of Things," 2018 IEEE International Congress on Internet of Things (ICIOT), 2018.

[12] N.A. Alrajeh, U. Marwat, B. Shams, S. Saddam, H. Shah, "Error Correcting Codes in Wireless Sensor Networks: An Energy Perspective", Applied Mathematics & Information Sciences vol. 818, no. 2, pp. 809-818, 2015.

[13] C.-F. Lee, C.-C. Chang, X. Xie, K. Mao, and R.-H. Shi, "An adaptive high-fidelity steganographic scheme using edge detection and hybrid Hamming codes," Displays, vol. 53, pp. 30–39, 2018.

[14] S. Liu, Z. Fu, and B. Yu, "Rich QR Codes With Three-Layer Information Using Hamming Code," IEEE Access, vol. 7, pp. 78640–78651, 2019.

[15] A. B. Dehkordi and S. A. Abu-Bakar, "Iris code matching using adaptive Hamming distance," 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), 2015.

[16] D. Zhai, X. Liu, H. Chang, Y. Zhen, X. Chen, M. Guo, and W. Gao, "Parametric local multiview Hamming distance metric learning," Pattern Recognition, vol. 75, pp. 250–262, 2018.