Ciencia Latina
Revista Multidisciplinar

DOI: https://doi.org/10.37811/cl_rcm.v7i1.5259

Aplicaciones de los autómatas celulares en los procesos de marcado de agua digital

Francisco Lozada González
flozadag2100@alumno.ipn.mx
https://orcid.org/0000-0002-8130-3630
Instituto Politécnico Nacional – CDMX

Manuel Cedillo Hernández
mcedilloh@ipn.mx
http://orcid.org/0000-0002-9149-9841
Instituto Politécnico Nacional – CDMX

Pedro Guevara López
pguevara@ipn.mx
https://orcid.org/0000-0001-5373-1403
Instituto Politécnico Nacional – CDMX

RESUMEN

Los grandes avances de la tecnología hoy en día han ayudado a la comunicación y distribución de todo tipo de material digital de manera instantánea. Este es uno de los grandes beneficios de las tecnologías de la información y comunicación, donde también existen diversas amenazas de infracciones relacionadas al derecho de autor o Copyright, falsificaciones de contenido, plagios, por mencionar algunas. Al pasar de los años se han desarrollado diferentes algoritmos computacionales para coadyuvar a la protección de datos en archivos de textos, audio y video, respectivamente. En este artículo se presenta un análisis del estado del arte sobre el uso de autómatas celulares dentro del campo de procesamiento de imágenes digitales en conjunto con la técnica de Marcado de Agua Digital (Digital Watermarking).

Palabras clave: *autómata celular; procesamiento digital de imagen; marcado de agua digital; reglas de transición.*

Correspondencia: flozadag2100@alumno.ipn.mx
Artículo recibido 25 enero 2023 Aceptado para publicación: 25 febrero 2023
Conflictos de Interés: Ninguna que declarar

Cómo citar: Lozada González, F., Cedillo Hernández, M., & Guevara López, P. (2023). Aplicaciones de los autómatas celulares en los procesos de marcado de agua digital. Ciencia Latina Revista Científica Multidisciplinar, 7(1), 10882-10895. https://doi.org/10.37811/cl_rcm.v7i1.5259

Applications of cellular automata in digital watermarking processes

ABSTRACT

The great advances in technology today have helped the communication and distribution of all kinds of digital material information instantly. This is one of the great benefits of information and communication technologies, where there are also various threats of infringements, violations related to copyright, falsification of content, and plagiarism, to name a few, etc. Over the years, different computational algorithms and methods have been developed to help protect data in texts, audios and videos files, respectively. In this article, an analysis of the state of the art on the use of cellular automata within the field of digital image processing is presented in conjunction with the technique of, such as the use Digital Watermark algorithm etc.

Keywords: *cellular automaton; digital image processing; digital watermarking; transition rules.*

1. INTRODUCCIÓN

La protección de derechos de autor y la autenticación de propietario hoy en día se han vuelto de suma importancia dadas las ventajas tecnológicas que proporcionan las tecnologías de la información y comunicación, principalmente al compartir y distribuir archivos multimedia (texto, imagen, audio y video) en redes de comunicaciones ya sean locales o globales. Sin embargo, estas ventajas traen consigo amenazas constantes relacionadas con la infracción de derechos de autor, falsificaciones digitales, privacidad y plagio principalmente. . La protección de los derechos de autor y la autenticación de propietario han sido consideradas por los investigadores desde hace más de dos décadas. (Z. Jalil,2010)

En un contexto de imágenes digitales y , considerando como propósito principal la protección de derechos de autor y autenticación de propietario, el presente trabajo considera un análisis de los métodos más populares como demarcado de agua digital que involucran en sus diseños el uso de automátas celulares . (Manasi Jana,2022)

1.1Aplicaciones de Marca de agua

La técnica de marca de agua puede complementar incrustando señales secretas imperceptibles, una marca de agua, directamente en los datos originales de tal manera que siempre permanece presente. La marca de agua, por ejemplo, puede ser utilizado para los siguientes propósitos (G. C. Langelaar,2000):

- Protección de derechos de autor: Para la protección de la propiedad intelectual, el propietario de los datos puede incrustar una marca de agua que represente información de Copyright en sus datos.
- Toma de huellas dactilares: Para rastrear la fuente de las copias ilegales, el propietario puede utilizar una técnica de toma de huellas dactilares. En este caso, el propietario puede incrustar diferentes marcas de agua en las copias de los datos que se suministran a diferentes clientes.
- Protección de copias: La información almacenada en una marca de agua puede controlar directamente los dispositivos de grabación digital para la protección contra copias propósitos.
- Monitoreo de transmisiones: Mediante la incrustación de marcas de agua en anuncios comerciales, un seguimiento automatizado el sistema puede verificar si los anuncios se transmiten según lo contratado.

- **Autenticación de datos:** Las marcas frágiles se puede usar para comprobar la autenticidad de los datos.

Las técnicas de marcado de agua no solo se utilizan con el propósito de protección. Otras aplicaciones incluyen (G. C. Langelaar,2000):

- **Indexación**: indexación de correo de video, donde los comentarios pueden estar incrustado en contenido de video; indexación de películas y noticias, donde se puede insertar marcadores y comentarios que pueden ser utilizados por los motores de búsqueda.
- **Seguridad Medica:** incorporación de la fecha y el nombre del paciente en las imágenes médicas podría ser una medida de seguridad útil.
- **Ocultación de datos:** Se pueden utilizar técnicas de marca de agua para la transmisión de mensajes privados secretos. Desde varios gobiernos restringen el uso de servicios de encriptación, las personas pueden ocultar sus mensajes en otros datos.
- **Transparencia perceptiva:** En la mayoría de las aplicaciones, el algoritmo de marca de agua debe incrustar la marca de agua de manera que no afecte la calidad de los datos del host subyacente (G. C. Langelaar,2000).

Un procedimiento de incrustación de marca de agua es realmente imperceptible si los humanos no pueden distinguir los datos originales de los datos con la marca de agua insertada. Sin embargo, incluso a la modificación más pequeña de los datos originales puede resultar evidente cuando se comparan directamente con los datos con marca de agua. Dado que los usuarios de datos con marca de agua normalmente no tienen acceso a los datos originales, no pueden realizar esta comparación. Por lo tanto, puede ser suficiente que las modificaciones en los datos con marca de agua pasen desapercibidas siempre que los datos modificados no se comparen con los datos originales (G. C. Langelaar,2000).

1.2. Requerimientos de una marca de agua

Cada aplicación de marca de agua tiene sus propios requisitos específicos. Por lo tanto, no hay un conjunto de requisitos para cumplirse con todas las técnicas de marca de agua. Sin embargo, se pueden dar algunos requisitos para las aplicaciones antes mencionadas: (G. C. Langelaar,2000)

- Transparencia perceptiva: En la mayoría de las aplicaciones, el algoritmo de marca de agua debe incrustar la marca de agua tal que esto no afecte la calidad subyacente datos del anfitrión. Un procedimiento de marca de agua es verdaderamente imperceptible si los humanos no pueden distinguir el original de los datos con una marca de agua insertada.
- Carga útil de la marca de agua: la cantidad de información que se puede almacenar en una marca de agua depende de la aplicación. Para propósitos de protección contra copia, una carga útil de un bit suele ser suficiente.
- Robustez: una frágil marca de agua que tiene que demostrar la autenticidad de los datos del host no tiene que ser robusta contra técnicas de procesamiento o alteraciones intencionales de los datos del host, ya que la falta de detección de la marca de agua demuestra que los datos del host han sido modificados y ya no están autorizados.
- Seguridad: La seguridad de las técnicas de marca de agua puede interpretarse de la misma manera que la seguridad en técnicas de cifrado. De ahí una marca de agua La técnica es realmente segura su se conocen los algoritmos exactos. Para incrustar y extraer las marcas de agua no ayudar a una parte no autorizada a detectar la presencia de la marca de agua o quitarla.

1.3. Autómatas celulares

Los autómatas celulares (AC) son un modelo discreto de computación que podría usarse para resolver cualquier tarea computacional. Los AC se utilizan ampliamente en diferentes aplicaciones, como la generación de imágenes, música, generación de números aleatorios, reconocimiento de patrones, algoritmos de enrutamiento y juegos. La aplicación de los CA en el área de procesamiento de imágenes digitales incluye la mejora de imágenes, compresión, encriptación y marca de agua. (Abu Dalhoum,2016)

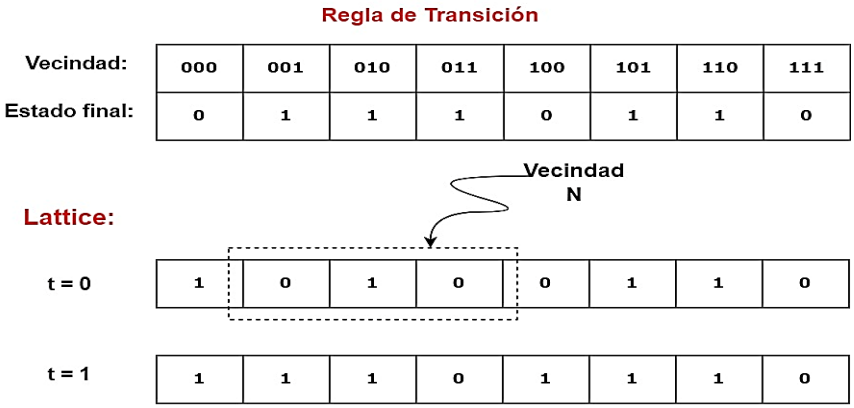
Los AC son un sistema dinámico en los que el tiempo, espacio y los valores de las variables de estado, son discretos. Están formados por un gran número de células(nodos) en una dimensión *d* siempre con interacciones locales. (C. r. Wei,2010)

Cada célula se encuentra en un determinado estado-espacio. Su valor de estado en el tiempo *t*+1 se programa de acuerdo con un parcial definido, y se sincroniza de acuerdo con la regla de la función de vecindad en el tiempo *t*. (C. r. Wei,2010) (véase figura 1)

Para definir una AC es necesario definir otros elementos que lo integran, tales como:

- **Lattice** (Células) regular de *N* máquinas de estado finito idénticas, llamadas células, que cubre el espacio n-dimensión; cada una de las células cuenta con patrones idénticos y conexiones locales con otras células.
- **Estado**, que puede ser asignado a cada célula.
- **Regla de transición**, que especifica la evolución en el tiempo de los estados.
- **Vecindad**; las interacciones locales que toda célula tiene es con células que pertenecen solo a su vecindad.

Figura 1. *Modelo propuesto por Wolfram(1983)*

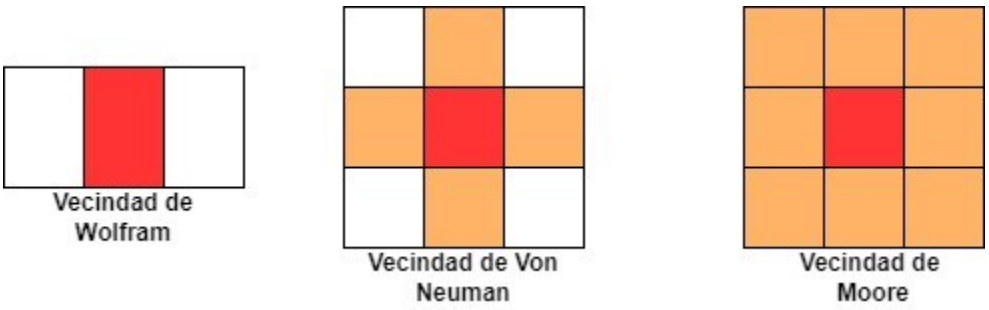


El comportamiento de los AC a menudo se ilustra utilizando "diagramas de espacio tiempo" en lo que la configuración de estados en el retículo d-dimensional se traza como una función del tiempo.

En los casos de AC de estado binario en los que los valores posibles, 1 o 0, la regla de la AC se muestra a menudo como una tabla de reglas que enumera cada posible vecindario junto con su bit de salida, el valor de actualización para el estado y el número de vecindarios posibles.

Las 256 AC unidimensionales *k*=2, *r*=1 se denominan AC elementales (ACE).

Figura 2. *Tipos de Vecindades en Autómatas Celulares.Jana, Manasi(2021)*



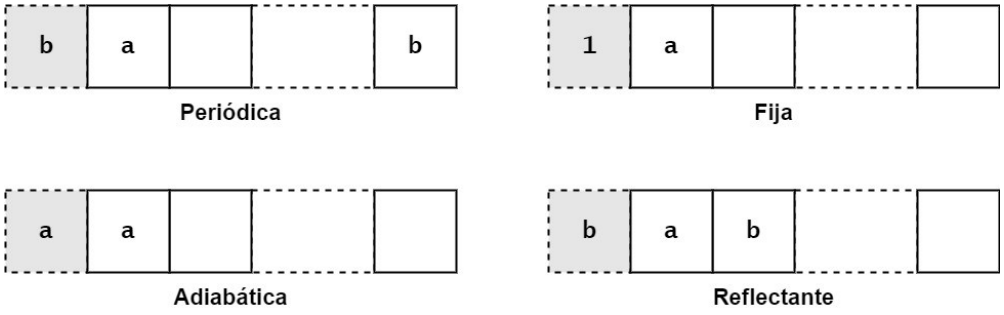
La definición de lattice por sí misma permite considerar lattices de tamaño infinito, pero en la práctica de esta implementación resulta imposible, es por eso por lo que los AC

son representados como sistemas de espacios finitos, a estas condiciones que permiten limitar el espacio de operación del AC las llamamos condiciones de frontera:

Los tipos de condiciones de frontera se manejan de cuatro formas (Chopard B.,1998):

- Periódica: Esta condición permite tomar el espacio que utilizamos para representar el AC de manera continua, uniendo los extremos del espacio de acción, en el caso de un AC 1-dimensional el espacio de acción queda representado como un anillo y para una AC 2-dimecional, el espacio se curva para formar un toroide
- Fija: Esta condición de frontera completa la vecindad con células virtuales con un valor preasignado
- Adiabática: Condición de frontera obtenida por la duplicación del valor de la célula cercana a la célula virtual
- Reflectante: Obtenida de copiar el valor de otros vecinos de la célula virtual.

Figura 3. *Tipos de Condiciones de frontera en Autómatas Celulares 1-Dimension. (Chopard, B.,2009)*



2. METODOLOGÍA

Para este artículo se revisarán algunas de las aplicaciones en algoritmos de marca de agua utilizando autómatas celulares:

2.1Marca de agua de imágenes médicas sin pérdidas basado en una diferencia significativa del coeficiente de transformación de autómatas celulares

De acuerdo con (Tzuo-Yau Fan,2019) propone un esquema para la aplicación de marca de agua sin perdidas proponiendo dos esquemas de construcción para generar Ownership Share Image (OSI) y extracción de marca de agua. En la fase de construcción OSI, se utiliza una clave secreta para obtener la marca de agua codificada y el código mediante el método Bose–Chaudhuri–Hocquenghem (BCH) codifica la marca de agua cifrada en la información de verificación. A continuación, la imagen medica se submuestrea en cuatro subimágenes y se eligen aleatoriamente dos subimágenes y se

obtienen dos anchos de banda de baja frecuencia usando transformación de Autómatas Celulares (TAC). Los dos anchos de banda de baja frecuencia se pueden utilizar para obtener características importantes de la imagen médica, que luego se utilizan para generar el Maste Share Image (MSI) (A. Morales-Ortega,2022).

Donde la información de verificación, MSI, puede utilizarse como imagen de protección para generar la OSI y verificar imágenes médicas, la OSI requiere el registro de tercero.(Figura 4) En la fase de extracción de la marca de agua de las imágenes médicas sospechosas es necesario generar nuevamente la MSI(Figura 5). Por último, la OSI y la MSI se combinan para obtener la información de verificación. El código BCH descifra la información de verificación a la marca de agua codificada, y la clave secreta se utiliza para restaurar los valores de los pixeles a su posición original en la marca de agua, que se utiliza para verificar la imagen medica sospechosa. Véase figura 4

Figura 4. *Diagrama de flujo en fase de construcción de OSI. Jana, Manasi(2021)*

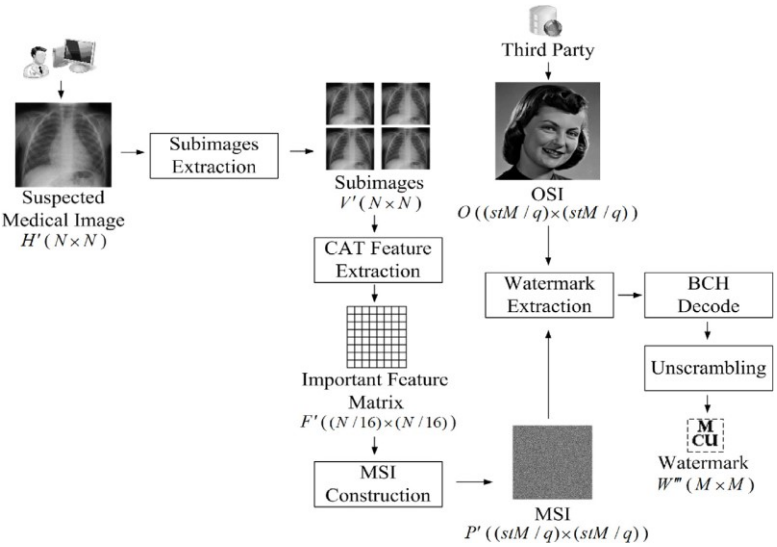
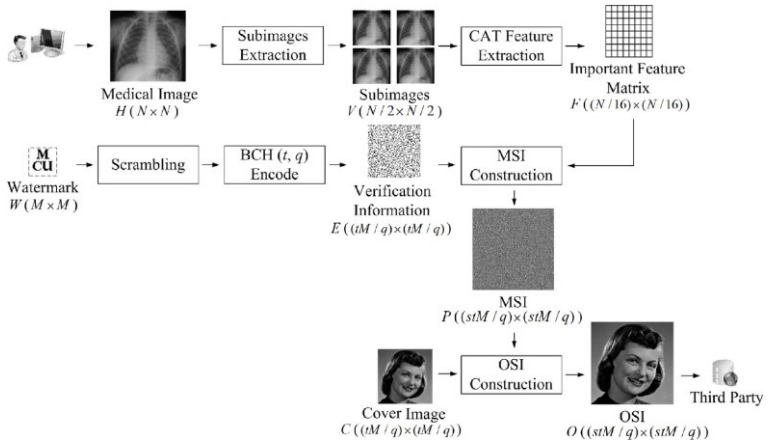


Figura 5. Fase de Extracción de Marca de Agua. Jana, Manasi(2021)



Dentro de la propuesta de (Tzuo-Yau Fan,2019) las imágenes médicas con Watermarking basado en la diferencia significativa de Autómatas Celulares para la protección de los derechos de autor. Con el fin de dar a el método propuesto suficiente seguridad y robustez, los pixeles de la marca de agua se mezclan primero antes de la implementación y se obtiene la información de verificación con capacidad de garantizar la integridad de los datos a través de la codificación de códigos BCH.

El uso de los autómatas celulares dentro de la propuesta al considerar dos su imágenes de manera aleatorias y someterlas a un autómata celular de 2D,para obtener 2 anchos de banda de baja frecuencia, por lo que dichas bandas son utilizadas como característica importante de las imágenes médicas. Véase figura 5

Figura 5*. Aplicación de automata celular dentro de 10890rocesso em generacion de OSI*

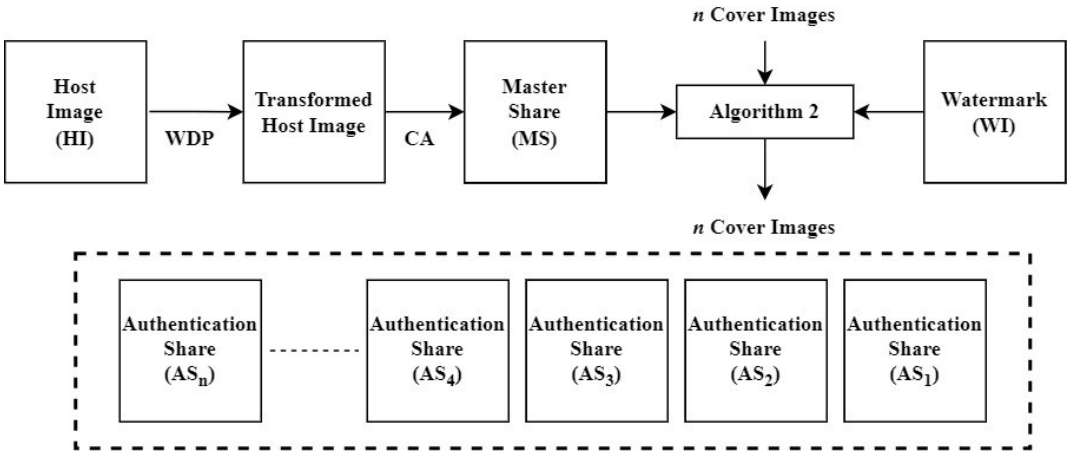
2.2Autenticación de imágenes basado en autómatas Celulares usando criptografía visual extendida

La novedad propuesta por Kukreja, S (Kukreja,S,2022) es donde la imagen original (host) no se modifica para incrustar la marca de agua, sino que las acciones de autenticación se construyen a partir de la imagen host utilizando Visual Cryptography (VC)(Olvera-Martinez,2022) para almacenar la información de la marca de agua. Esto hace el sistema imperceptible3 como no se requiere ningún proceso de ocultación de datos para ocultar estas acciones y los datos de autenticación en imágenes de portada, en su lugar se construyen acciones de autenticación significativas que se asemejan a las imágenes de portada. Esto reduce la complejidad del sistema. Los autómatas celulares dentro de la propuesta de (Kukreja,S,2022) son utilizados para crear el Master Share Image (MSI),aumentando aún mas la seguridad del sistema, ya que la nueva marca de

agua oculta en los Shares, no puede ser detectada o eliminada fácilmente por personas no autorizadas.

Las ventajas de utilizar autómatas celulares (AC) son que no se necesita *codebooks* para crear las acciones, no hay expansión de pixeles, ya que cada bit de la imagen host está representado por un bin en Master Share y nos es necesario almacenar la acción, ya que puede construirse a sí misma a partir de su estado inicial. El esquema de CV existente basado en CA utiliza una clave para generar la acción. Esta clave tiene que ser transmitida desde el emisor al receptor como información secundaria, lo que se supone un coste adicional de transmisión y también puede ser accedida por terceros atacantes. Mientras que en el esquema propuesto se considera como clave una representación binaria de la media de cada bloque, no hay necesidad de transmitir la clave como información secundaria. Puede ser construida por el emisor y el receptor individualmente a partir de su imagen anfitriona y recibida respectivamente. Esto reduce el coste de transmisión y mejora la seguridad.

Figura 6. *Diagrama de flujo en creacion de VC con Automatas celulares con R30 (Kukreja,S,2022)*

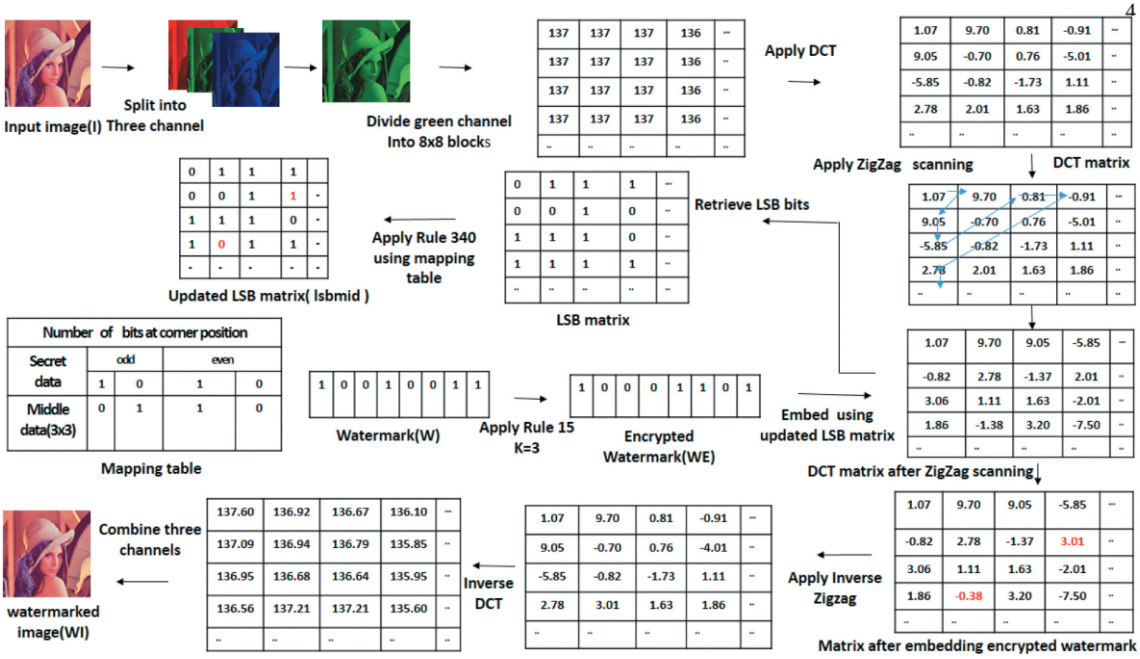


2.3 Marca de agua de imagen basado en DCT que utiliza autómatas celulares

En el esquema propuesto de marca de agua propuesto por (Jana, Manasi,2021), forma parte de una imagen de entrada en color I de (*M*x*N*) y una imagen de marca de agua *W*(*mxn*). Las imágenes se han dividido en tres canales de color: rojo, verde y azul. Cada canal se divide en (8x8) bloques nos superpuestos y se aplica la DCT a cada bloque. Antes de incrustarla, la marca de agua W se cifra mediante la regla CA-15 para hacerla más robusta. La imagen de marca de agua se incrusta en los coeficientes DCT de cada

bloque no solapado (8x8) en orden ZingZang. El bit de la imagen de marca de agua cifradas en el valor medio de los bloques superpuestos(3x3) de cada bloque no superpuesto utilizando la regla CA- 340, t la tabla de asignación. Se aplica la exploración inversa ZingZang inversa para obtener el componente modificado y por último DCT inversa para obtener la imagen con marca de agua que se envía al receptor

Figura 7*. Diagrama de procedimento de Extracción de datos propuesto por (Jana, Manasi,2021) usando DCT con Autómatas Celulares*



3. RESULTADOS Y DISCUSIÓN

Dentro de esta sección se presenta una evaluación de las diferentes aplicaciones, posibles dentro de las características del uso de marca agua. Donde puede ser visto como un prototipo de sistema dinámico, con ciertas condiciones iniciales y parámetros a considerar dentro del modelo en el que se encuentre trabajando, como es el uso de los diferentes tipos de vecindades, estados, y transformaciones en un tiempo t+1.

Con las comparaciones dentro de las aplicaciones analizadas, se observa un objetivo en común, que es cumplir los requerimientos de una Watermarking, como es generar mayor robustes en la ocultación de la información, con diferentes tipos de vecindades dentro de los algoritmos propuestos como fue el caso de la propuesta de Kukreja, S (Kukreja, S.,2020) al utilizar los autómatas celulares como medio de seguridad, obteniendo una llave como condición inicial que, al realizar el recorrido del autómata en

la Regla 30 en el Modelo de Von Neumann, es posible generar uno de los shares de la imagen que forman parte del MSI.

Dentro de las aplicaciones de se encuentran ventajas del uso de los autómatas celulares como fue el caso de Tzuo-Yau Fan(Tzuo-Yau Fan,2020) donde propone un método de autenticación de imágenes médicas haciendo uso de la regla 15, 134 del modelo de wólfram, donde se recalca un consumo de tiempo adicional en la creación del OSI al hacer en BCH donde el tiempo computacional es notablemente mayor que en otros esquemas, donde también se muestra la efectividad y excelencia de la marca de agua dando un equilibrio a la robustes del algoritmo.

Uno de los algoritmos propuestos por Jana, Manasi (Jana, Manasi, 2020) al hacer uso de los 3 canales de la imagen a color RGB, realiza una encriptación por DCT y complementa con el uso de autómatas celulares, los cueles le dan una mejor robustes en la incrustación de la marca de agua, con un bajo tiempo de ejecución. A demás, indica que el método propuesto es altamente robusto contra varios ataques.

4. CONCLUSIONES

El objetivo de este artículo es presentar las diferentes técnicas de protección de imágenes por medio de diferentes tipos de Marcas de Agua Digitales, en la implementación de diferentes propuestas y algoritmos, utilizando Autómatas Celulares, ya que estos aportan diferentes beneficios como es la robustes de la marca de agua, como también las mejoras en tiempos computaciones. Siendo punto importante para los investigadores y autores de los diferentes medios digitales.

LISTA DE REFERENCIAS

Jalil, Z., Mirza, A. M., & Iqbal, T. (2010). A zero-watermarking algorithm for text documents based on structural components. International Conference on Information and Emerging Technologies. https://doi.org/10.1109/iciet.2010.5625705.

Jana, M., & Jana, B. (2021). A new DCT based robust image watermarking scheme using cellular automata. Information Security Journal: A Global Perspective, 31(5), 527–543. https://doi.org/10.1080/19393555.2021.1956023.

Wei, C., Liu, J., & Liang, G. B. (2010). A DCT_SVD domain watermarking algorithm for digital image based on Moore-model cellular automata scrambling. International

Conference on Intelligent Computing. https://doi.org/10.1109/iciss.2010.5656731.

Dalhoum, A. L. A., Madain, A., & Hiary, H. (2016). Digital image scrambling based on elementary cellular automata. Multimedia Tools and Applications, 75(24), 17019–17034. https://doi.org/10.1007/s11042-015-2972-z

Chopard, B., & Droz, M. (1998, December 10). Cellular Automata Modeling of Physical Systems. https://doi.org/10.1017/cbo9780511549755.

Wolfram, S. (1982) Cellular automata as simple self-organizing systems. Caltech Preprint CALT,. submitted to Nature.

Wolfram, S. (1984). Cellular automata as models of complexity. Nature, 311(5985), 419–424. https://doi.org/10.1038/311419a0.

Wolfram, S. (1983). Statistical mechanics of cellular automata. Reviews of Modern Physics, 55(3), 601–644. https://doi.org/10.1103/revmodphys.55.601.

Juárez, G. J. (2000) Teoría del campo promedio en Autómatas Celulares Similares a TheGame of Life[Tesis de Maestría]. CINVESTAV, México,.

Langelaar, G. C., Setyawan, I., & Lagendijk, R. L. (2000). Watermarking digital image and video data. A state-of-the-art overview. IEEE Signal Processing Magazine, 17(5), 20–46. https://doi.org/10.1109/79.879337.

Mohanty, S. P., Sengupta, A., Guturu, P., & Kougianos, E. (2017). Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection. IEEE Consumer Electronics Magazine, 6(3), 83–91. https://doi.org/10.1109/mce.2017.2684980.

Fan, T., Chao, H., & Chieu, B. (2019, February 1). Lossless medical image watermarking method based on significant difference of cellular automata transform coefficient. Signal Processing-image Communication; Elsevier BV. https://doi.org/10.1016/j.image.2018.09.015

Kukreja, S., Kasana, G., & Kasana, S. S. (2019, January 1). Cellular Automata Based Image Authentication Scheme Using Extended Visual Cryptography. Computing and Informatics; Central Library of the Slovak Academy of Sciences. https://doi.org/10.31577/cai_2019_6_1272

Morales-Ortega, A., & Cedillo-Hernandez, M. (2022). Ownership Authentication and Tamper Detection in Digital Images via Zero-Watermarking. 2022 45th

International Conference on Telecommunications and Signal Processing (TSP). https://doi.org/10.1109/tsp55681.2022.9851253.

Olvera-Martinez, Luis Angel, Cedillo-Hernandez, Manuel, Diaz-Rodriguez, Carlos Adolfo, & Jimenez-Borgonio, Enrique Tonatiuh. (2022). Secure Exchange of Medical Images Via Extended Visual Cryptography. Revista mexicana de ingeniería biomédica, 43(2), 1275. Epub 31 de octubre de 2022.https://doi.org/10.17488/rmib.43.2.5