RPNS: 2067 | ISSN: 1817-9088
Volumen 21 (2024)
N° 2 (abril - junio)

Original **Recibido: 30/12/2023** | **Aceptado: 27/03/2024**

Aplicación de las marcas de agua en las informaciones digitales en instituciones deportivas

Application of watermarks in digital information in sports institutions

Alicia María Centurión Fajardo. Licenciado en Matemática. Master en Ciencias. Profesor Auxiliar. Universidad de Granma. Bayamo. Cuba. [acenturionfajardo@gmail.com]

Anier Soria Lorente. Licenciado en Matemática. Doctor en Ciencias. Profesor Titular. Universidad de Granma. Bayamo. Cuba. [asorial@udg.co.cu]

Carlos Felipe Gómez Jiménez. Licenciado en Educación. Especialidad Matemática y Física. Master en Ciencias. Ministerio de Educación de la República Dominicana. Técnico Distrito 13-02. Guayubín. República Dominicana. [cafe20001@gmail.com]

Resumen

En la actualidad, la seguridad de la información es una preocupación constante para todos los usuarios de la red, y los piratas informáticos constituyen una amenaza para dicha seguridad, lo que constituye un asunto de máxima importancia, evidenciando la necesidad de alcanzar una protección adecuada de la información, para evitar su uso, modificación, grabación o destrucción por usuarios no autorizados, o personas mal intencionadas, especialmente las que inciden de manera directa en la toma de decisiones, es incuestionable que el campo de las nuevas tecnologías de la información y las comunicaciones proporciona un espacio apropiado, posibilitando una seguridad de las informaciones digitales en las instituciones deportivas de Cuba. El trabajo se realizó en la Universidad de Granma, donde se aplicaron las marcas de agua, se utilizaron siete informaciones del período agosto - diciembre del 2023. Para el procesamiento de la información digital se utilizó el software PolyMarking versión 1. La aplicación de las marcas de agua permitió proteger las informaciones digitales en las instituciones deportivas, al transitar por los diferentes canales de

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. https://olimpia.udg.co.cu

la red, muchos de ellos confidenciales evitando los errores en manipulación de dichas informaciones, los ataques cibernéticos y las usurpaciones de identidad.

Palabras clave: Marcas de agua; informaciones digitales; software PolyMarking.

Abstract

Nowadays, the information security is a constant concern for all network users, and hackers constitute a threat to said security, which is a matter of utmost importance, evidencing the need to achieve adequate protection of information, to prevent its use, modification, recording or destruction by unauthorized users or ill-intentioned people, especially those that directly affect decision making, it is unquestionable that the field of new information and communications technologies provides a appropriate space, enabling security of digital information in Cuban sports institutions. The work was carried out at the University of Granma, where the watermarks were applied, to achieve this seven informations from the period September - December 2023 were used. PolyMarking version 1 software was used to process the digital accounting information. The application of watermarks made it possible to protect digital information in the sports institutions, when traveling through the different channels of the network, many of them confidential, avoiding errors in the manipulation of said information, cyber attacks and identity theft.

Keywords: Watermarks, digital information; PolyMarkin software

Introducción

En la actualidad, la seguridad de la información es una preocupación constante por todos los usuarios de la red, y los piratas informáticos constituyen una amenaza para dicha seguridad, por ello las TIC (Las Tecnologías de la Información y la Comunicación) tienen una importancia trascendental, ya que permite el fácil acceso a la información y a una comunicación eficiente, rápida y clara (Alvarado, 2022).

Lo anterior es un asunto de máxima importancia, por lo que existe la necesidad de alcanzar, una protección adecuada de la información, para evitar su uso, modificación, grabación o destrucción por

usuarios no autorizados, o personas mal intencionadas (Soria, Mecías, Pérez, & Rodríguez, 2014; Soria & Berres, 2017), especialmente las que inciden de manera directa en la toma de decisiones. Esta protección, está dirigida a hacer mínima la posibilidad de que pueda ser alterada o manipulada, conservando por el tiempo necesario su valor de uso para el cual ha sido destinada. De modo que reviste especial trascendencia trabajar con el propósito de lograr, cada día con mayor eficiencia, la implementación de los métodos y procedimientos que garanticen la protección de la información, con elevados índices de invulnerabilidad (Centurión, Soria & Moreno, 2019).

Es incuestionable que el campo de las nuevas tecnologías de la información y las comunicaciones, proporciona un espacio apropiado para perfeccionar los sistemas institucionales de gestión documental, que posibiliten una seguridad de la información, como demandan hoy en día las informaciones tramitadas en las Instituciones deportivas de Cuba, evitando alteración de la información, errores intencionados o no intencionados, que permitan que estas sean seguras.

Es evidente que para la transmisión de datos a través de los diferentes canales se necesitan técnicas de encriptación fuertes con el objetivo de garantizar la seguridad deseada (Sena & Siva, 2016; Camacho, 2017; Centurión, Céspedes & Moreno, 2021).

En los últimos años han surgido distintos métodos para tratar de proporcionar protección a la información digital y salvaguardar los derechos de sus propietarios, entre los cuales se destaca el uso de marcas de agua digitales (España, 2003).

Para Orúe (2002), las marcas de agua digitales son elementos de seguridad, es un código de identificación que se inserta directamente en el contenido de un archivo multimedia (imagen, audio, video, texto), de manera que sea difícil de apreciar por el sistema perceptual humano, pero fácil de detectar usando un algoritmo dado y una clave, en un ordenador.

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. https://olimpia.udg.co.cu

A pesar de su uso en todo el mundo, no existe evidencia que se hayan empleado en las informaciones digitales en las instituciones deportivas, por ello es el interés de mostrar su aplicación a estos, para garantizar la seguridad de la información.

Las instituciones deportivas en Cuba se encargan de la gestión deportiva, la educación física y la recreación en Cuba, estas cuentan con informaciones digitales, además de varios departamentos donde se procesan dichas informaciones. Las informaciones que emanan de los diferentes departamentos, es en muchas ocasiones información cuantitativa expresada en unidades monetarias y/o descriptivas, y en otras ocasiones son informaciones relevantes cuyo objetivo esencial es ser útil en la toma de sus decisiones, por ello existe una vulnerabilidad marcada de dichas informaciones, principalmente entre las que se envían y se reciben.

El objetivo de este trabajo es aplicar soluciones informáticas utilizando las marcas de agua para el perfeccionamiento de la gestión documental en las informaciones digitales en las Instituciones deportivas.

Materiales y métodos

En este trabajo se utilizó el software PolyMarking versión 1, que es el resultado de varias investigaciones realizadas, desarrolladas por el Departamento de Tecnología de la Universidad de Granma de conjunto con el Departamento de Contabilidad y Finanzas, éste utiliza un algoritmo desarrollado recientemente por los departamentos mencionados anteriormente y la Universidad de Alcalá (Centurión-Fajardo, Lastra, & Soria-Lorente, 2023).

El software se hizo sobre un Framework Django para desarrollo Web y dentro de este se programó con JavaScripts, con Python 3.8.10, CSS y HTML.

El Polymarking se basa en dos marcas de agua, una frágil y una robusta, para proteger cualquier información digital.

La robusta se encarga de insertar de manera invisible en el dominio de la frecuencia de la imagen, la

firma digital que va a ser a través de un QR que genera el mismo software.

La frágil inserta una imagen que también es invisible para poder detectar cualquier modificación realizada, garantizando su integridad, puesto que la marca depende de una clave y de funciones HASH, que al hacer cualquier cambio por pequeño que sea es detectado, indicando no solo que es auténtico, sino que parte del documento fue modificado.

Para el análisis experimental se recogieron 7 informaciones digitales correspondientes al periodo agosto - diciembre del 2023 en la Universidad de Granma, a todas las informaciones digitales se le aplicaron las marcas de agua, comprobando su autenticidad.

Métodos de investigación utilizados:

Método universal

Materialismo dialéctico: se llevó a cabo como base metodológica de todas las ciencias, teniendo en cuenta el estudio de las informaciones la toma de decisiones, a partir de la investigación realizada.

Métodos Teóricos:

Histórico-Lógico: se utilizó en el análisis de los antecedentes de las marcas de agua y de las informaciones digitales, para el perfeccionamiento de la información documental, de manera que permita estudiar las particularidades de este proceso.

Análisis y síntesis: se empleó en la construcción del fundamento teórico de la investigación, a través del análisis de las diferentes fuentes de información.

Inducción y deducción: se aplica el razonamiento a partir de generalizaciones, para mediante la deducción establecer los procesos lógicos sobre conceptos, valoraciones y análisis de la información; permitiendo arribar a las conclusiones.

Sistémico – estructural: se utiliza con el fin de organizar los cálculos y los estudios hechos para determinar la factibilidad de la investigación.

Métodos Empíricos:

Observación: como proceso riguroso que consiste en la percepción directa del objeto de estudio, conocerlo de forma efectiva, para luego describir y analizar situaciones sobre la realidad estudiada en correspondencia con la realidad existente.

Técnicas, tales como:

Revisión documental: se utilizó en la revisión de las informaciones generadas y de su seguridad al enviarlo de forma digital.

Método de la Ciencia:

Estadístico-matemático: en el procedimiento de marcas de agua se aplicó de la Estadística Descriptiva, los diagramas de barras y gráfica circular (gráfico de pastel) y de la Estadística Inferencial, los coeficientes de correlación.

Para este trabajó se utilizaron, además:

- Microsoft Word 2010 (Como editor de texto).
- Microsoft Excel 2010 (Como procesador y tabulador)

Análisis y discusión de los resultados

Los algoritmos utilizados para la incrustación y extracción se muestran a continuación:

Figura 1

Algorithm 1 Embedding Algorithm

Input: Cover image $\mathcal{C}$, robust watermark $\{\omega_i \in \{0,1\} : i = 1, 2, \ldots\}$, key κ, x_0, μ.
Output: Watermarked image $\mathcal{W}$
Fragile watermark: $\upsilon \leftarrow$ **sha256**$(\kappa)[:16]$
$\{\hat{\omega}_i\} \leftarrow$ scrambled watermark by the piecewise linear chaotic map (x_0, μ)
Divide $\mathcal{C}$ into non-overlapping blocks of 8×8 bytes
for each $\mathcal{C}^{(k,8)} \in \mathcal{C}$ **do**
  $\mathcal{M} \leftarrow \mathcal{A}\,\mathcal{C}^{(k,8)}\mathcal{A}^t$: according to (26)
  $\nu^k \leftarrow \mathscr{Z}(\mathcal{M})$: Apply the zigzag scan [52, Section 4.3]
  $\overline{\nu}^k_{28} \leftarrow \nu^k_{28}$ watermark bit $\hat{\omega}_k$ is embedded in the selected coefficient ν^k_{28} by using Dither Modulation, [28, Section 5.3]
  $\overline{\mathcal{M}} \leftarrow \mathscr{Z}^{-1}(\overline{\nu}^k)$ [52, Section 4.3]
  $\overline{\mathcal{W}}^{(k,8)} \leftarrow \mathcal{A}^t\,\overline{\mathcal{M}}\,\mathcal{A}$: According to (28)
end for
for each $\overline{\mathcal{W}}^{(k,8)} \in \overline{\mathcal{W}}$ **do**
  $\varsigma \leftarrow \mathscr{Z}(\overline{\mathcal{W}}^{(k,8)})$: Apply the zigzag scan
  LSB$(\varsigma[:16]) \leftarrow \upsilon$: according to [52, Section 4.3]
  $\mathcal{W}^{(k,8)} \leftarrow \mathscr{Z}^{-1}(\varsigma)$: According to [52, Section 4.3]
end for
return $\mathcal{W}$

Algoritmo de Incrustación. Fuente (Centurión-Fajardo, Lastra, & Soria-Lorente, 2023)

Figura 2

Algorithm 2 Extracting Algorithm

Input: Watermarked image $\mathcal{W}$, key κ, x_0, μ.
Output: Robust watermark $\{\omega_i \in \{0,1\} : i = 1, 2, \ldots\}$ and tamper detection
Divide $\mathcal{W}$ into non-overlapping blocks of 8×8 bytes
for each $\mathcal{C}^{(k,8)} \in \mathcal{C}$ **do**
  $\mathcal{M} \leftarrow \mathcal{A}\mathcal{C}^{(k,8)}\mathcal{A}^t$: according to (26)
  $\nu^k \leftarrow \mathscr{Z}(\mathcal{M})$: Apply the zigzag scan
  $\omega_k \leftarrow$ watermark bit is extracted from the selected coefficient ν^k_{28} by using Dither Modulation.
end for
for each $\overline{\mathcal{W}}^{(k,8)} \in \overline{\mathcal{W}}$ **do**
  $\varsigma \leftarrow \mathscr{Z}(\overline{\mathcal{W}}^{(k,8)})$: Apply the zigzag scan
  $\upsilon \leftarrow$ **LSB**$(\varsigma[:16])$ **fragile watermark**
  if $\upsilon \neq$ **sha256**$(\kappa)[:16]$ **then**
    $\mathcal{W}$ is not authentic; break
  end if
end for

Algoritmo de extracción Fuente (Centurión-Fajardo, Lastra, & Soria-Lorente, 2023)

Aplicación de las marcas de agua en las informaciones digitales de las Instituciones deportivas

Proceso de inserción de las marcas de agua (frágil y robusta) – versión 1:

1.- Inicialmente el emisor inserta su clave privada en el software, la cual es única e intransferible, comprobándose la aceptación por parte del emisor.

Figura 3

Introducción de la clave. Fuente: Elaboración propia.

2.- Luego debe ir a la sección de prueba de autenticidad, aquí comienza el proceso de autenticación de la

fuente emisora.

3.- Posteriormente carga la información que será autenticada.

Si el documento antes de ser validado por el sistema es modificado, no es detectado como erróneo; pero sí identifica la fuente que lo emitió, garantizando seguridad para el receptor.

4.- Autentica el documento. Suministra una firma digital, la cual representa la marca de agua robusta que será insertada para verificar que la fuente emisora es genuina, ésta se inserta de manera invisible en el dominio de la frecuencia de la imagen, en forma de un código QR que es generado por el mismo software mediante la firma digital, independientemente a ello, el software inserta una marca de agua frágil con el propósito de detectar cualquier modificación que se le haga a la información a partir de este momento. Toda la información queda registrada en una base de datos Postgres psql (base de datos profesional).

5.- Se realizan las evaluaciones y se muestra el resultado de la aplicación de las marcas de agua.

Test de imperceptibilidad (Se utilizó el demostrado en Centurión-Fajardo, Lastra, & Soria-Lorente, (2023)

El análisis experimental reveló los valores de PSNR (relación señal-ruido pico) y BER (bit error rate) de los polinomios tipo Charlier-Sobolev y tipo Meixner-Sobolev. Los resultados experimentales mostraron que los momentos propuestos permitieron obtener informaciones digitales con buena calidad, con valores de PSNR, entre 37 y 47.6 db, lo que está en correspondencia con los valores heurísticos de PSNR. El PSNR para evaluar el nivel de imperceptibilidad y distorsión, así como para medir la diferencia entre la cubierta y las informaciones digitales con marca de agua se muestra a continuación.

$$\text{PSNR}= 10\log_{10}\left(\frac{\Xi^2}{\text{MSE}}\right),$$

El PSNR está dado en unidades llamadas decibelios (dB) y el MSE está dado por el error cuadrático medio.

$$\text{MSE} = (\text{N}^2\rho)^{-1}\sum_{\gamma\in\tau}\|\text{C}(\gamma)-\text{W}(\gamma)\|^2.\,\text{C},\text{W}\in\{0,1,\ldots.,\Xi\},\text{y}\;\Xi=\max(\max(\text{C}),\max(\text{W})),$$

Donde C es la imagen de la cubierta y W representa la imagen con la marca de agua respectivamente, de tamaño $N^2\rho$.

Test de Robustez (Se utilizó el demostrado en Centurión-Fajardo, Lastra, & Soria-Lorente, (2023)

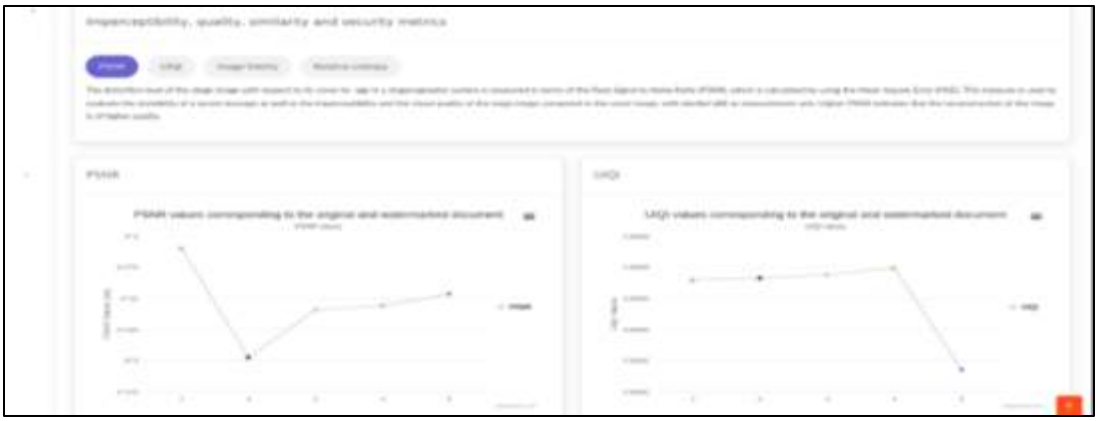
Los valores binarios formados incorrectamente de la imagen de la marca de agua determinan la solidez de los métodos en términos de tasa de error de bits BER (Bit Error Rate).

$$\mathrm{BER} = \frac{1}{L}\sum_{n=0}^{L-1}\begin{cases}1, & \bar{\omega}(n) \neq \omega(n),\\ 0, & \bar{\omega}(n) = \omega(n),\end{cases}$$

donde ω(n) y $\bar{\omega}$(n) son bits binarios (0 o 1) de C y W. Aquí, L representa el número de bits del esquema de marca de agua. Para evaluar la robustez, se aplicaron los siguientes ataques: Ruido de recorte, Ruido gaussiano, Laplace gaussiano, ruido de filtro mínimo y ruido de sal y pimienta, cuyos parámetros aparecen en (Centurión-Fajardo, Lastra, & Soria-Lorente, 2023)

A continuación se muestran los valores de PSRN y entropía relativa obtenidos en este trabajo.

Figura 4



Valores de PSRN y Entropía Relativa. Fuente: Elaboración propia.

6.- Luego, el software genera un documento .zip por cada información incluida.

7.- El emisor debe enviar el documento .zip, por cualquier canal de comunicación (seguro o inseguro) al receptor.

Proceso de extracción:

Universidad de Granma. Bayamo MN, Cuba.
Carretera de Manzanillo Km 17 ½ Bayamo. Granma. Cuba.
C.P. 85100. https://olimpia.udg.co.cu

1.- El receptor debe ingresar al software a través de una contraseña privada única.

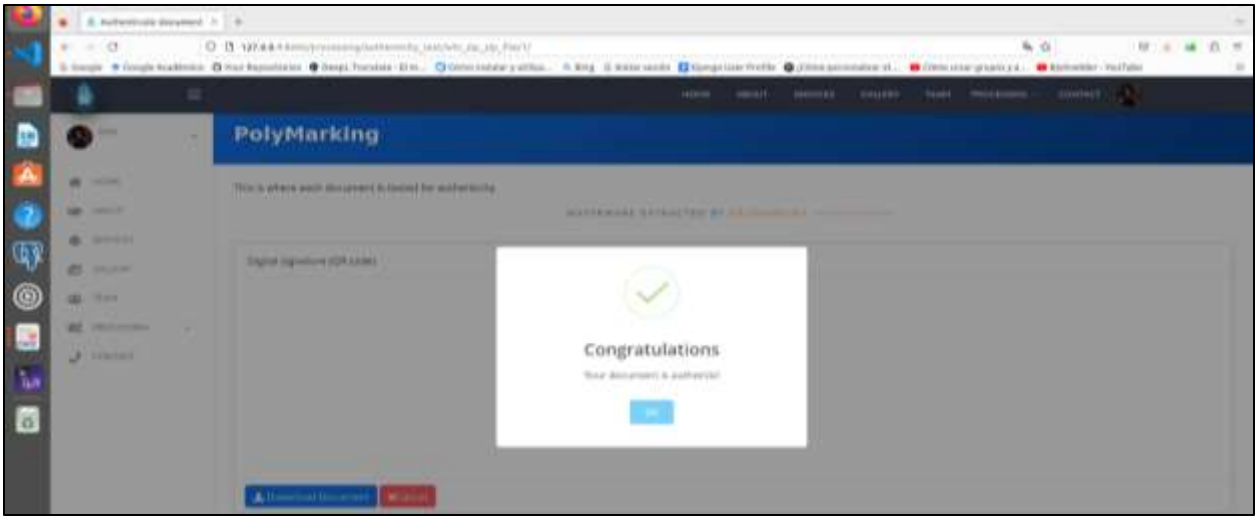
2.- Luego debe ir a la sección de prueba de autenticidad.

3.- Cargar los documentos .zip enviados por el emisor (uno a uno).

4.- Se muestran las informaciones cargadas por el sistema.

5.- El software realiza la prueba de autenticidad, indicando la fuente emisora, la autenticidad e integridad de las informaciones, lo cual puede ser verificado con un escáner de QR, que puede realizar desde una laptop hasta en un celular.

Figura 5



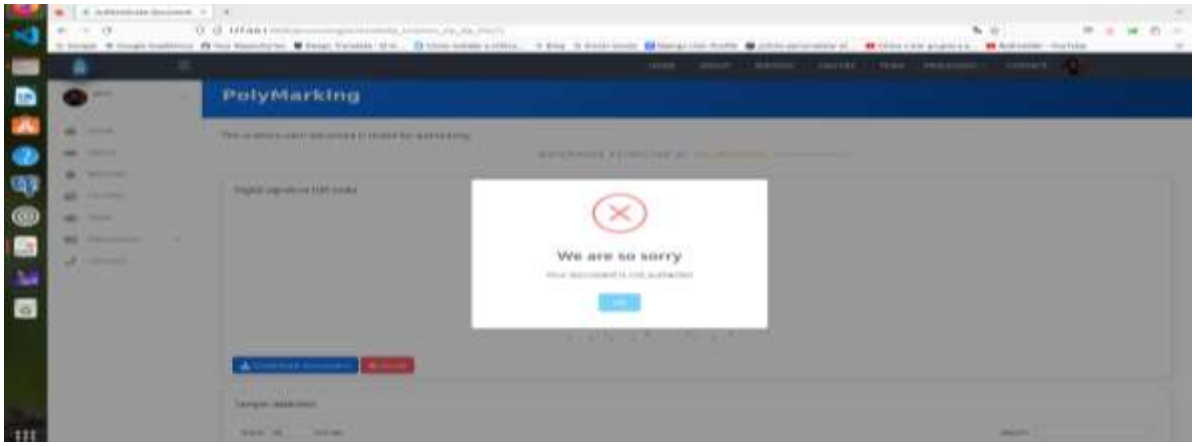
Se comprueba la autenticidad del documento. **Fuente: Elaboración propia.**

6.- Si el documento es original el software le inserta un código QR de autenticidad en la esquina izquierda superior de cada documento procesado.

7.- En caso de que el documento haya sido modificado el software es capaz de detectar la más mínima alteración, indicando donde se hizo, las páginas afectadas, así como los porcientos que representan los cambios realizados, mostrados a través de un diagrama de barra y de una gráfica circular (gráfico de pastel) el porciento global afectado (ver figuras de la 6 a la 9). En este paso se garantiza la autenticidad, integridad

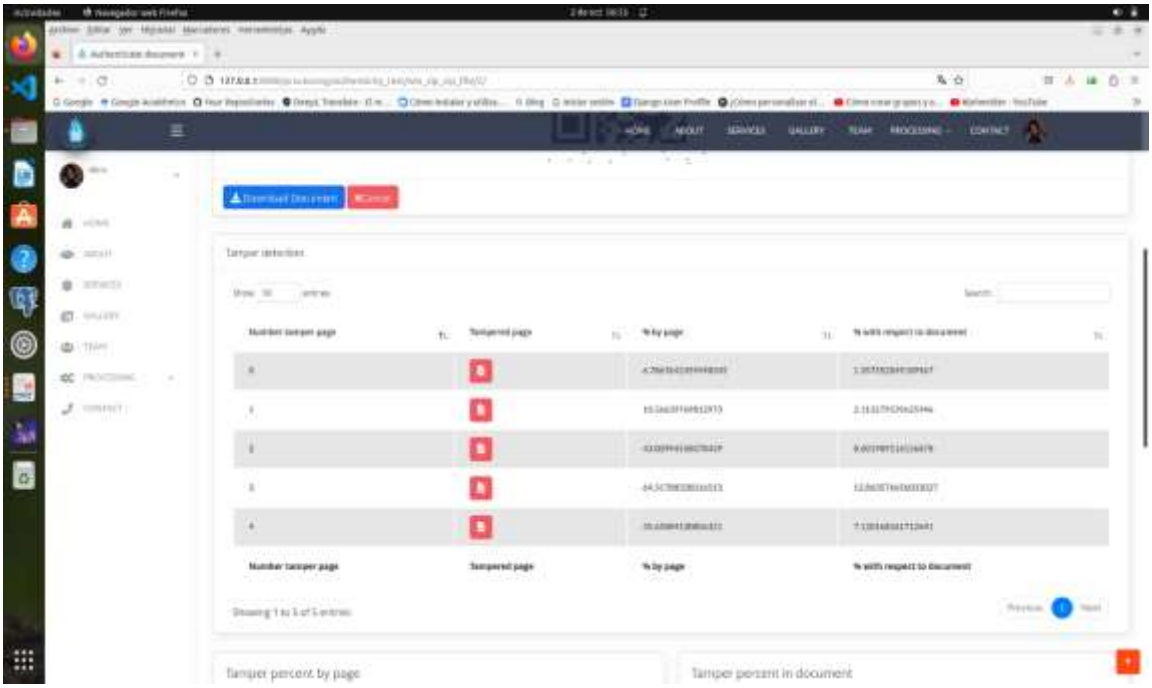
y originalidad de la información emitida.

Figura 6



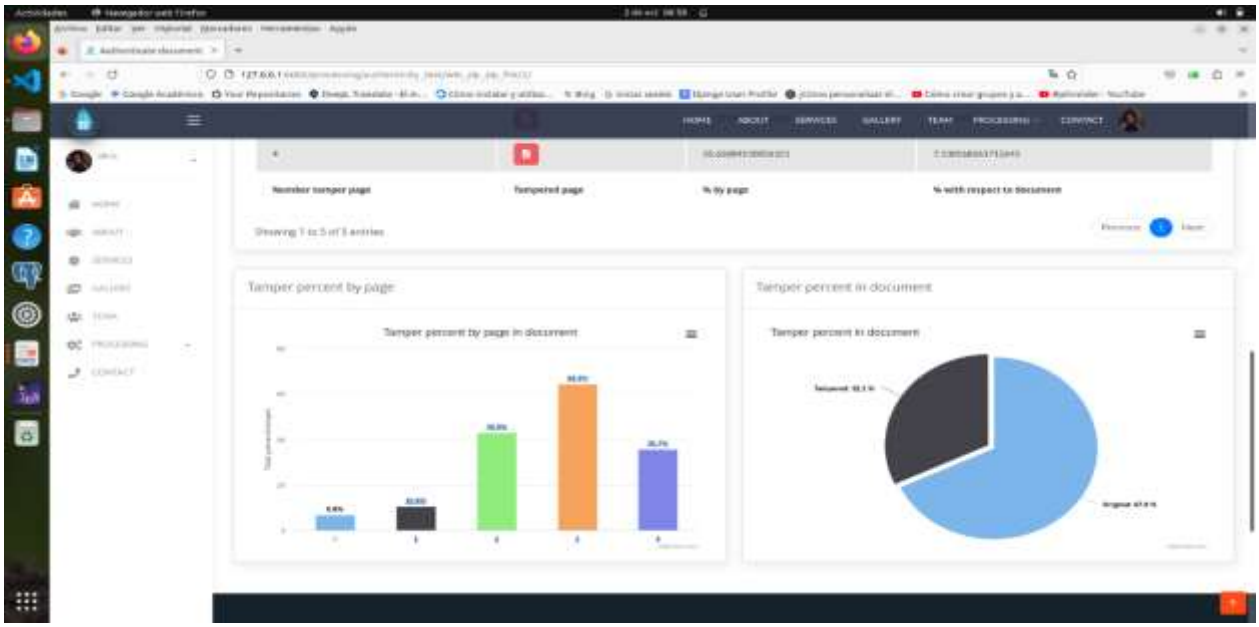
Mensaje recibido cuando un documento no es autentico. Fuente: Elaboración propia

Figura 7



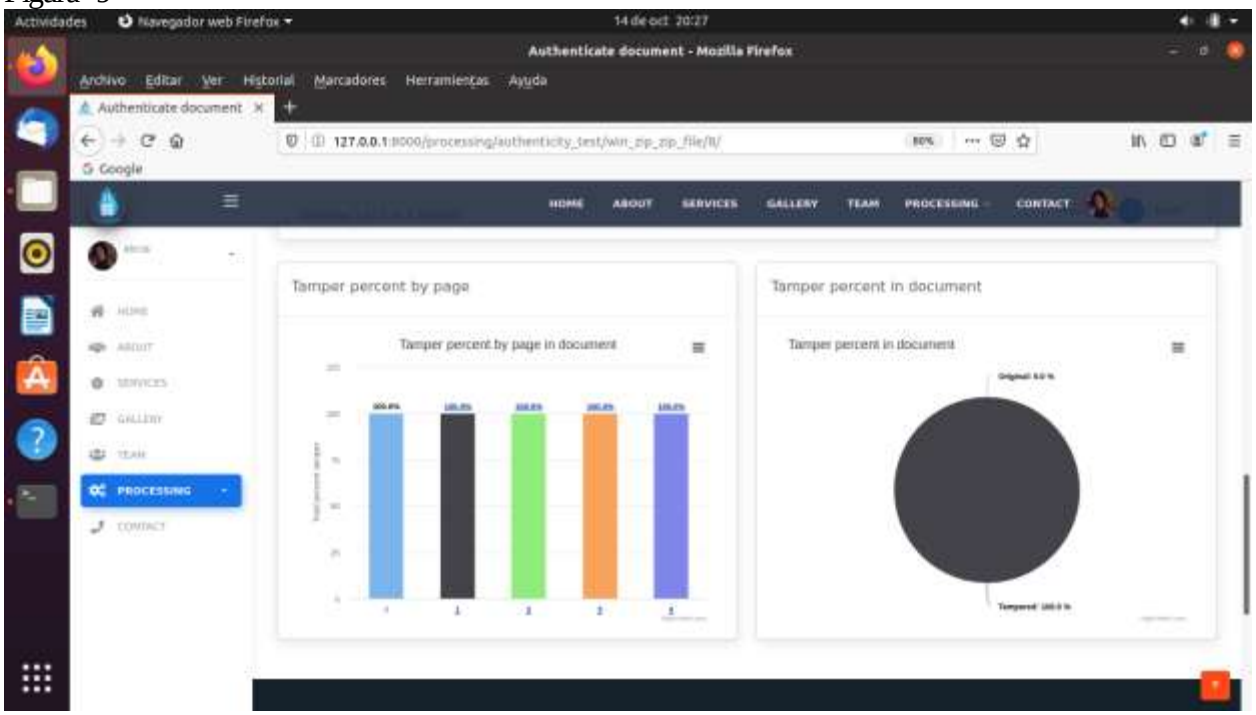
Detección de cambios, con números de paginas y porcientos modificados de cada una de ella. Fuente: Elaboración propia

Figura 8



Detección de cambios, reflejados en Diagrama de Barra y Gráfico de Pastel. Fuente: Elaboración propia

Figura 9



Detección del 100% de cambios, reflejados en Diagrama de Barra y Gráfico de Pastel. Fuente: Elaboración propia

Las informaciones digitales pueden ser vulneradas en cualquier momento y por diferentes personas, al aplicar las marcas de agua le permite a la entidad una seguridad razonable al disminuir la vulnerabilidad, se pueden presentar casos que el receptor modifique alguna información tanto parcial como general y puede

ser modificado totalmente. También puede ocurrir que el emisor modifique la información antes de ser validada por el sistema, en este último caso al recibirlo el receptor lo valida como auténtico, no obstante, le garantiza la autenticidad de la fuente emisora, librando al receptor de cualquier responsabilidad.

Conclusiones

La aplicación de las marcas de agua permite proteger las informaciones digitales en las instituciones deportivas, al transitar por los diferentes canales de la red, muchos de ellos confidenciales, evitando los errores en manipulación de dichas informaciones, los ataques cibernéticos y las usurpaciones de identidad. Las marcas de agua permiten una seguridad razonable al disminuir la vulnerabilidad.

El Software Polymarking puede ser incluido en la docencia, y tiene aplicación para cualquier entidad estatal o no estatal, así como en la seguridad nacional.

Referencias Bibliográficas

Alvarado, L. (31 de julio de 2022). Qué son los TIC y cuál es su importancia. https://www.poli.edu.co/blog/poliverso/que-son-las-tic.

Camacho Bello, C. J. (2017). Marca de agua en imágenes de gran tamaño y video utilizando momentos ortogonales discretos clásicos, Tesis de Grado, Maestro en Computación Óptica. pp. 155, Unidad Politécnica de Tulancingo, México.

Centurión Fajardo, Alicia M., Soria Lorente, A. & Moreno Roque, E. (2019). Un algoritmo esteganográfico vinculado a los cuadrados mágicos. Revista REDEL. Revista Granmense de Desarrollo Local, 3. Número 4, octubre-diciembre, pp. 225-238. https://revistas.udg.co.cu/index.php/redel/article/view/1139.

Centurión Fajardo, Alicia M., Céspedes, Nancy, & Moreno, E. (2021). Una marca de agua frágil en el dominio de los momentos ortogonales de Krawtchouk. Revista Pensamiento Matemático, XI, Número 1,Abr 2, pp. 017−028.

Centurión-Fajardo, A. M., Lastra, A. & Soria-Lorente, A. (2023). Un esquema dual de creación de marca de agua basado en momentos ortogonales tipo Sobolev para la autenticación de documentos. arXiv preprint arXiv:2305.10112.

España Boquera, María Carmen. (2003). Aplicaciones y Servicios de Comunicaciones, Disponible en: http://www.google libros/. [Consulta: 6 de septiembre de 2023].

Orúe López, Amalia Beatriz. (2002). Marcas de agua en el mundo real, 2002. Disponible en: https://digital.csic.es/ bitstream/ 10261/8864/ 1/ Marcas_de_agua_en_el_mundo_real.pdf, [Consulta: 6 de septiembre de 2023].

Sena Reddy, M.I. & Siva Kumar, A.P. (2016). Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm, Procedia Computer Science, 85, pp. 62 – 69.

Soria, A., Mecías, R., Pérez, A., & Rodríguez, D. (2014). Algoritmo esteganográfico pseudo-asimétrico, Lecturas Matemáticas, 35 (2), pp. 183–196.

Soria, A., & Berres, S. A . (2017). secure steganographic algorithm based on frequency domain for the transmission of hidden information, Security and Communication Networks. g