Motivando el aprendizaje del Álgebra Lineal a través de sus aplicaciones: la división de secretos

Ángela Rojas Matas, [1] Alberto Cano Rojas

Dpto. de Matemáticas, Edificio Einstein, Campus de Rabanales, Universidad de Córdoba, Córdoba (14071)
Télefono 957 212145, Angela.Rojas@uco.es

[1] Becario FPU, Universidad de Córdoba,
i52caroa@uco.es

Resumen
Para motivar a nuestro alumnado planificamos realizar actividades académicas que hicieran uso de conceptos teóricos del Álgebra Lineal de una forma práctica, útil e interesante. En este trabajo se presenta una de estas actividades dedicada a la división de secretos: un secreto no estará en manos de una sola persona sino que sólo cuando se junten un número determinado de personas se podrá recuperar completamente dicho secreto. Por otro lado, la interpolación polinómica es un tema de indudable interés en Matemáticas y en Ingeniería. Resolver un problema de interpolación de este tipo conlleva el planteamiento y la resolución de sistemas de ecuaciones lineales. Veremos cómo aplicar estas ideas para conseguir la división de un secreto. En este trabajo veremos una experiencia desarrollada sobre este tema en clase de Álgebra Lineal en primer curso de Ingeniería Informática.

Palabras Clave: Motivación; Álgebra Lineal; División de secretos.

1. Introducción

Basta con analizar lo que se hace en nuestras universidades para comprobar que los programas, relaciones de problemas, etc. de Álgebra Lineal son bastante parecidos en cualquier titulación universitaria. La mayoría de las veces, la parte práctica de la asignatura se reduce a la clásica relación de problemas tan habituales en Matemáticas. Por supuesto, la relación de problemas debe formar parte de nuestro quehacer docente pero nosotros nos planteamos hacer además algo más. Por eso, quisimos hacer con nuestros alumnos de Álgebra Lineal, asignatura de primer curso de la titulación de Ingeniería Informática, una serie de actividades dedicadas a presentar aplicaciones reales útiles de la asignatura en temas de interés para un futuro ingeniero informático. Con esto pretendemos que los alumnos aprendan Álgebra Lineal sabiendo en qué temas relacionados con sus estudios se utilizan, para que así valoren más los conocimientos que están adquiriendo. Buscamos así atraer el interés del alumnado y fomentar la motivación ya que de esa forma mejoramos el proceso de enseñanza y aprendizaje de la asignatura.

El Álgebra Lineal es una parte de las Matemáticas que está adquiriendo una gran importancia en los últimos años. Así, por ejemplo, las imágenes digitales en escala de grises no son más que matrices donde cada elemento de la matriz coincide con el nivel de gris del píxel correspondiente. Si la imagen es una imagen en color RGB entonces cada elemento de la matriz será una terna (r, g, b) con la cantidad de rojo, verde y azul presentes en el color del píxel correspondiente (el color es una combinación de los tres colores primarios, Red Green Blue), en definitiva una imagen en color se corresponde con tres matrices. Por esta razón, en el procesamiento de imágenes digitales se utilizan muchas técnicas del cálculo matricial. Las imágenes han sido usadas en varias actividades académicas desarrolladas con nuestros alumnos de Álgebra Lineal.

Destacamos algunas de las aplicaciones del Álgebra Lineal al procesamiento de imágenes digitales que hemos realizado en nuestras clases o en algunas ocasiones realizadas por algunos alumnos como trabajos de la asignatura:

- La compresión JPEG de una imagen se implementa a través de un producto matricial con matrices ortogonales.
- La edición de imágenes para hacer un fotomontaje se puede llevar a cabo resolviendo un sistema lineal de ecuaciones [1].
- El coloreado de una imagen digital en escala de grises puede hacerse resolviendo también un sistema lineal de ecuaciones [2].
- El cifrado de una imagen digital puede también realizarse con el uso de técnicas matriciales [3, 4].
- La ocultación de mensajes secretos en una imagen digital (que se conoce por esteganografía digital) se puede conseguir también empleando métodos del Álgebra Lineal [5].
- Etc.

En las clases prácticas de la asignatura, realizadas en un laboratorio con ordenadores, vimos cómo utilizar Matlab a nivel de usuario para llevar a cabo los cálculos habituales de una clase de Álgebra Lineal: cómo calcular rangos, determinantes, autovalores, etc. pero también vimos cómo usar Matlab como lenguaje de programación. Al ser una asignatura de segundo cuatrimestre, tenemos la ventaja de que ya han cursado una

asignatura de programación en el primer cuatrimestre y, por lo tanto, ya saben programar. Ya saben utilizar bucles, condicionales, etc. y sólo deben adaptarse a la sintaxis específica de Matlab. Vimos también cómo manipular imágenes en Matlab lo que nos iba a permitir trabajar con imágenes digitales en nuestras clases.

En este trabajo se presentará una de estas actividades dedicada a la división o reparto de secretos. Es un tema interesante para los alumnos y de indudable interés para ellos. Pero ¿en qué consiste la división de secretos? Respondemos a continuación a esta pregunta.

Existen ocasiones donde una información secreta no es deseable que esté en manos de una sola persona. Puede interesar que varias personas posean parte de dicha información y que sólo se consiga recuperar la información completa si se juntan varias de estas personas. Por ejemplo, el director de un banco puede interesarle que ningún empleado de la misma posea la clave que abre la caja fuerte. Por el contrario, puede repartir entre 5 empleados, por ejemplo, parte de la información, de forma que para conseguir la clave de la caja fuerte tengan que juntarse al menos 3 de los 5 empleados. Esta idea se conoce como esquema umbral (5,3).

El primer artículo sobre este tema fue publicado en 1976 por A. Shamir, un criptógrafo muy conocido [6]. En su artículo Shamir propone el uso de polinomios para llevar a cabo un esquema umbral para el reparto de un número secreto. Posteriormente se han publicado una gran cantidad de trabajos. Por ejemplo en el artículo de Thien [7] explica cómo aplicar el esquema de Shamir para compartir una imagen secreta. En el artículo de Parakh [8] se propone una variación del método de Shamir. Existen otros métodos de reparto de secretos [9, 10].

La división o reparto de secretos es un tema de gran interés en la actualidad ya que hay una gran cantidad de empresas con intereses comerciales a las que les viene muy bien, por temas de seguridad, disponer de métodos seguros de reparto de secretos. Basta con buscar documentación sobre el tema y se podrá comprobar la gran cantidad de artículos que se han publicado recientemente sobre este esto. Pero además, atrae mucho el interés del alumnado, con lo que conseguimos un mayor grado de motivación.

La organización del trabajo es como sigue: en la sección 2 se estudiará el método de Shamir, en la sección 3 se estudiará el método de Thien para compartir una imagen

secreta (no es más que el método de Shamir adaptado para imágenes), en la sección 4 se estudiará el método de Parekh y, por último, terminamos con la sección de conclusiones.

2. Esquema de Shamir

Como se ha comentado en la introducción, los esquemas de compartición de secretos, conocidos también como esquemas umbrales, son protocolos criptográficos para compartir un secreto entre un conjunto de participantes de modo que sólo cuando se junten un número especificado de participantes sea posible recuperar el secreto. En un esquema umbral (n,k) hay un total de n participantes y sólo al juntar como mínimo a k de ellos será posible recuperar el secreto. Vamos a describir a continuación el esquema de Shamir [6].

Supongamos que el secreto es un número S que el dueño del banco quiere proporcionar a sus empleados y que es la clave de la caja blindada. Para ello, construirá un polinomio $P(x) = S + a_1 x + \cdots + a_{k-1} x^{k-1}$ de grado $k-1$ donde los coeficientes se eligen al azar, salvo el término independiente que se hace coincidir con el número secreto S. Después el dueño del banco elige unos valores para $x_1, x_2, \ldots, x_n$ y a continuación calcula:

$$P(x_1) = p_1,\ P(x_2) = p_2, \ldots,\ P(x_n) = p_n$$

Al empleado número 1 se le proporciona el par (x_1, p_1), al empleado número 2 se le proporciona el par (x_2, p_2) y así sucesivamente.

Cuando se junten al menos k de ellos tendremos datos suficientes para averiguar el polinomio $P(x)$, es decir, sus k coeficientes, planteando y resolviendo el sistema lineal correspondiente. Después bastará con evaluar el polinomio en cero para obtener el secreto ya que: $S = P(0)$.

Supongamos que la clave secreta es $s = 1234$ y que vamos a hacer un esquema umbral (6, 3). El distribuidor del secreto escogerá dos números cualesquiera, que indicaremos a_1 y a_2, con los que construirá el polinomio de segundo grado: $P(x) = s + a_1 x + a_2 x^2$

Supongamos que $a_1 = 166$ y que $a_2 = 94$, entonces:

$$P(x) = S + a_1 x + a_2 x^2 = 1234 + 166x + 94x^2$$

Calculamos 6 puntos cualesquiera del polinomio del polinomio, por ejemplo:

(1, 1494), (3, 2578), (4, 3402), (6, 5614), (8, 8578), (11, 14434). Estos datos se suelen llamar "sombras" en los esquemas de reparto de secretos.

El distribuidor reparte estos puntos entre sus seis empleados de confianza. Sólo cuando se junten al menos tres de ellos tendremos datos suficientes para poder construir el polinomio $P(x)$. Una vez construido el polinomio será fácil recuperar el secreto s ya que: $s = P(0)$

Supongamos que al empleado nº 1 se le da el primer punto, al empleado nº 2 el segundo punto, y así en adelante. Como el polinomio desconocido tiene 3 coeficientes a determinar harán falta un mínimo de tres puntos para poder determinarlo. Si se juntan tres o más sí que podrán reconstruir el polinomio.

Por ejemplo, supongamos que se juntan los empleados 2, 5 y 6. El sistema a resolver sería:

$$\left.\begin{array}{l} S + 3a_1 + 9a_2 = 2578 \\ S + 8a_1 + 64a_2 = 8578 \\ S + 11a_1 + 121a_2 = 14434 \end{array}\right\}$$

En el sistema anterior aparece el famoso determinante de Vandermonde:

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = (b-a)(c-a)(c-b) = (8-3)(11-3)(11-8)$$

Este determinante es no nulo, por lo tanto, el sistema es compatible determinado y podremos resolverlo, hallando el valor de S. La idea de Shamir es sencilla, el secreto se hace coincidir con el término independiente del polinomio y el grado del polinomio depende del número mínimo de empleados que deben juntarse para poder obtenerlo.

Para un esquema (6, 3) como el anterior, el polinomio debía ser de grado 2, para que el polinomio a determinar tenga 3 incógnitas y hagan falta como mínimo 3 puntos para poder determinarlo.

En [6] se modifica el método anterior para cuando interese trabajar con congruencias módulo p, siendo p un número primo. El secreto S es un número entre 0 y $p-1$. A continuación el dueño del banco, que desea llevar a cabo un esquema umbral (n,k), construiría un polinomio de grado $k-1$ donde el término independiente se hace coincidir con el secreto y el resto de coeficientes del polinomio se elegirán aleatoriamente (números entre 0 y $p-1$). A continuación se razona como antes, sólo que ahora se trabaja con congruencias módulo p. La ventaja de trabajar con un número p primo es que cualquier número no nulo tendrá inverso en esa aritmética y eso nos vamos a permitir realizar correctamente los cálculos.

Nuestros alumnos de Álgebra Lineal ya conocen la aritmética modular que han estudiado en la asignatura de Matemática Discreta que cursan simultáneamente a la asignatura de Álgebra Lineal. Por lo tanto, no hay ningún problema en trabajar con congruencias módulo p en lugar de trabajar con la aritmética habitual.

3. Esquema de Thien

La idea de Shamir, pensada inicialmente para compartir un número secreto, se puede adaptar para compartir una imagen secreta: método de Thien [7]. En la Figura 1 se muestra la imagen que se desea compartir utilizando un esquema umbral como el de Shamir. Se trata de una imagen en escala de grises donde el nivel de gris de un píxel varía entre 0 (correspondiente al negro) y 255 (correspondiente al blanco). Esto requiere usar 1 byte por píxel. Esta escala de grises es muy habitual en las imágenes que se usan por Internet. Todos los valores de gris de esta imagen, que en principio podrían estar entre 0 y 255, resultan que están por debajo de 251, así que no hay problema en trabajar con congruencias módulo $p=251$ que es un número primo.

Figura 1. *Imagen secreta*

Supongamos que deseamos aplicar un esquema (3, 2). En este caso, para cada nivel de gris de la imagen secreta se razona como se expuso anteriormente: se formará un polinomio de grado 1 con coeficientes aleatorios, haciendo coincidir el término independiente con el secreto (nivel de gris del píxel). Los valores de $P(x_1) \pmod p$, $P(x_2) \pmod p$ y $P(x_3) \pmod p$ serán los niveles de gris del píxel correspondiente en cada una de las sombras que daremos a los participantes. La sombra de cada participante será una imagen del mismo tamaño que la imagen original pero que ahora tendrá aspecto pseudoleatorio. En la Figura 2 se muestran las tres sombras obtenidas en este ejemplo.

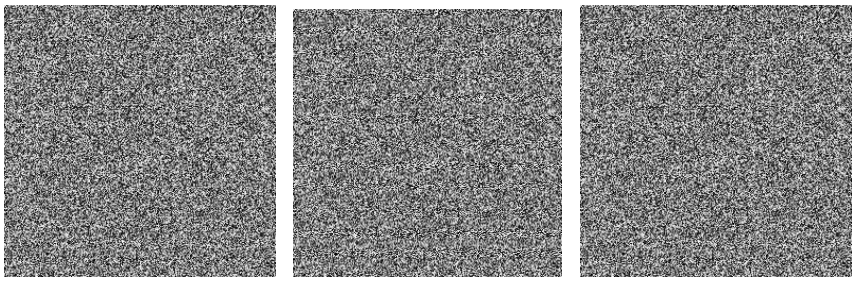

Figura 2. *Sombras para cada uno de los participantes*

Bastará con que se reúnan dos de los tres participantes para poder recuperar la imagen secreta de la Figura 1.

4. Esquema de Parakh

Vamos a tratar en esta sección otro esquema de reparto de secretos propuesto por Parakh [8]. Es una variación de la idea de Shamir. Explicamos el método con un esquema (4, 4).

Supongamos que deseamos compartir varios números secretos s_0, s_1, s_2 y s_3, por ejemplo. Averiguamos el polinomio interpolador que pasa por los puntos $(0, s_0), (1, s_1), (2, s_2), (3, s_3)$ que indicaremos por $P(x)$, que será en este caso un polinomio de grado 3. Evaluamos el polinomio en 4 puntos distintos de la forma:

$$D_1 = P(4), D_2 = P(5), D_3 = P(6), D_4 = P(7)$$

Damos al primer participante el punto $(4, D_1)$, al segundo el punto $(5, D_2)$, etc.

Está claro que cuando se junten los 4 participantes, tendrán cuatro puntos para averiguar el polinomio que pasa por ellos, es decir, el polinomio interpolador $P(x)$.

Después bastará con evaluar dicho polinomio en 0, 1, 2 y 3 para obtener los tres números secretos.

La idea se representa en la Figura 3. Los primeros 4 puntos sirven para averiguar el polinomio interpolador y los 4 puntos siguientes nos permiten averiguar las 4 sombras.

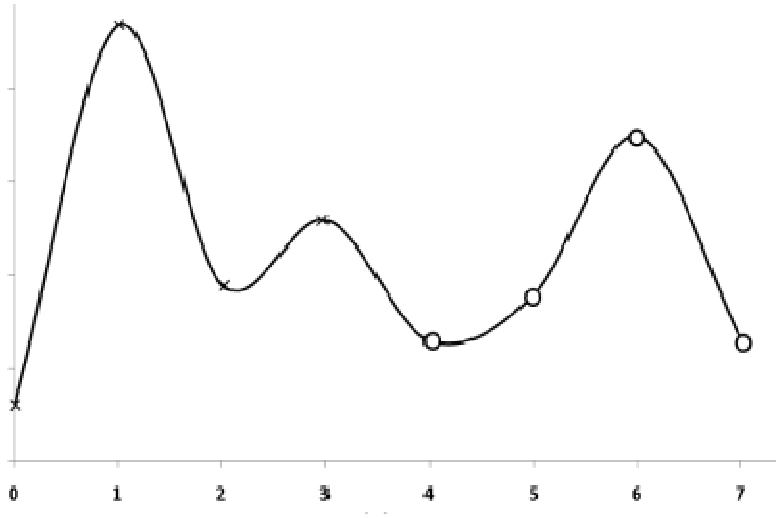

Figura 3. *Idea del método*

En la Figura 4 se muestran algunos de los polinomios que pasan por los tres últimos puntos (es decir, cuando se juntan los tres últimos participantes). En este caso, hay infinitos polinomios interpoladores de grado 3 que pasan por esos tres puntos y seremos incapaces de saber cuál es el verdadero polinomio interpolador y, por lo tanto, no podremos saber los números secretos.

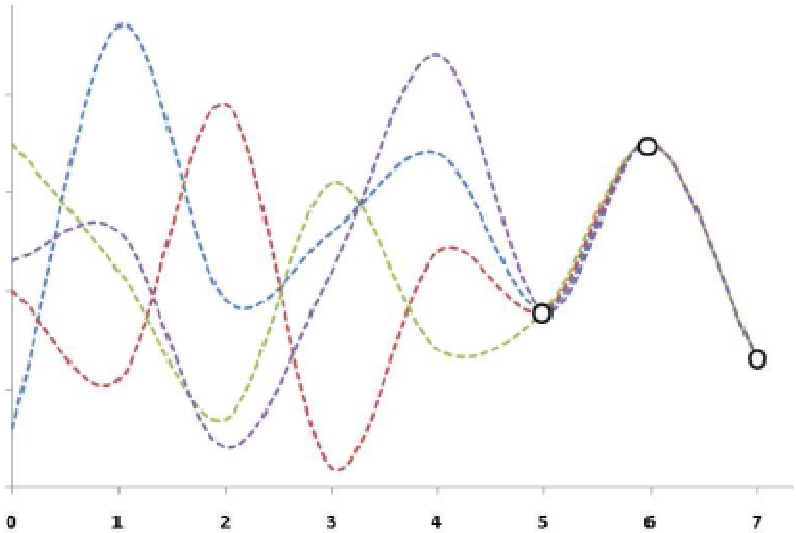

Figura 4. **Si se juntan 3 de los participantes**

Por ejemplo, si los números secretos fueran 7, 12, 31 y 82. El polinomio interpolador $P(x)$ que pasa por los puntos (0, 7), (1, 12), (2, 31), (3, 82) sería:

$$P(x) = 3x^3 - 2x^2 + 4x + 7$$

Después evaluamos el polinomio en 4, 5, 6 y 7 obteniendo 183, 352, 607 y 966 que serían las sombras de los 4 participantes.

En lo que sigue vamos a presentar una actividad desarrollada con nuestros alumnos en la que el secreto a dividir o repartir es un mensaje secreto.

Supongamos que el mensaje fuera: "BLANCO" y que usamos el siguiente alfabeto compuesto de 31 caracteres (incluye 27 letras, el punto, los símbolos de interrogación y el espacio en blanco indicado por *).

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

q	r	s	t	u	v	w	x	y	z	.	¿	?	*
17	18	19	20	21	22	23	24	25	26	27	28	29	30

Vamos a hacer un esquema (4, 3). Cogemos el mensaje en grupos de tres letras. A cada grupo de tres letras se le aplican las ideas anteriores.

- Primeras tres letras "BLA": se corresponden con {1, 11, 0}. Interpolamos por (0, 1), (1, 11), (2, 0) obteniendo el polinomio interpolador y después evaluamos dicho polinomio en 3, 4, 5 y 6 obteniendo -32, -85, -159, -254.
- Siguientes tres letras "NCO": se corresponden con {13, 2, 15}. Interpolamos por (0, 13), (1, 2), (2, 15) obteniendo el polinomio interpolador y después evaluamos dicho polinomio en 3, 4, 5 y 6 obteniendo 52, 113, 198, 307.
- Al participante 1 se le proporcionan los datos {-32, 52}, al participante 2 los datos {-85, 113,}, al participante 3 {-159, 198}, al participante 4 {-254, 307}.

Supongamos que se reúnen los tres primeros participantes, entonces:

- Con los puntos (3, -32), (4, -85), (5, -159) obtienen el polinomio interpolador que después evaluarán en 0, 1 y 2, obteniendo 1, 11, 0 que se corresponden con las letras "BLA".
- Repetirán la acción anterior obteniendo el resto del mensaje "NCO".
- Juntando las dos partes se recuperará el mensaje completo.

Las ideas anteriores se pueden aplicar en $\mathbb{Z}_{31}$. Ahora las operaciones se realizarán módulo 31. El proceso es el mismo que describimos anteriormente sólo que las sombras de los participantes serían:

Participante 1: {-32, 52} mod 31={30,21}="*U"

Participante 2: {-85, 113} mod 31={8, 20}="IT"

Participante 3: {-159, 198} mod 31={27, 12}="•M"

Participante 4: {-32, 52} mod 31={25,28}="Y¿"

Al trabajar en módulo 31, cualquier número entero se convertirá en el resto de la división entera de dicho número entre 31, es decir, se convertirá en un número entre 0 y 30 que se puede hacer corresponder con un carácter del alfabeto. De esta forma, las sombras que reciben cada uno de los participantes son mensajes de texto también.

La forma de recuperar el mensaje secreto es idéntica a la forma descrita anteriormente sólo que ahora deberemos trabajar en $\mathbb{Z}_{31}$. Así para recuperar las tres primeras letras del mensaje oculto con los tres primeros participantes deberemos averiguar el polinomio interpolador que pasa por los puntos (3, 30), (4, 8) y (5, 27) trabajando módulo 31.

Por supuesto, también podemos aplicar este método de reparto de secretos a una imagen digital de una forma muy intuitiva. También podríamos adaptarlo fácilmente para compartir un fichero de audio.

5. Conclusiones

Hemos intentado trabajar dentro de la asignatura de Álgebra Lineal de una forma diferente de la habitual en clase de Matemáticas. No sólo nos íbamos a dedicar a las clásicas sesiones de teoría y problemas en el aula sino que además se introducirían aplicaciones útiles de los contenidos matemáticos estudiados en la asignatura a temas

de interés para el alumnado. De esta forma perseguíamos motivar más a nuestros en el proceso de enseñanza-aprendizaje. Hemos procurado abordar temas actuales y cuya relevancia para un ingeniero técnico informático fuera indiscutible. Creemos que el resultado ha sido globalmente satisfactorio. En este trabajo se ha explicado en qué consiste una de las actividades realizadas en clase: el reparto o división de secretos.

Hemos procurado atender también a la diversidad de nuestro alumnado: algunos de nuestros alumnos viene más motivados y otros menos, como todos los profesores sabemos. Pensando en el alumnado menos motivado hemos incluido en nuestras clases las típicas relaciones de problemas y no los hemos "obligado" a realizar este tipo de actividades académicas más difíciles pero mucho más interesantes. Sin embargo, también hemos pensado en los alumnos más motivados, a los que sí que se les puede presentar este tipo de actividades más complejas. Por ejemplo, el tema de reparto de secretos ha sido presentado a nuestros alumnos a través de diversos ejercicios con un grado creciente de dificultad:

- Todos los alumnos deberán conocer de qué va el tema de reparto de secretos.
- Todos los alumnos deberán resolver el problema del reparto de secretos en un caso sencillo con lápiz y papel, sin usar ordenador.
- Todos los alumnos deberán usar Matlab a nivel de usuario y comprobar los resultados obtenidos en el apartado anterior (comprobando las soluciones de los sistemas de ecuaciones, etc.)
- Sólo los alumnos que lo deseen podrán realizar el reparto de secretos adaptado a una imagen digital usando Matlab (una actividad más complicada que las anteriores).

Sólo un número reducido de nuestros alumnos ha abordado este tipo de actividades opcionales más complejas. Sin embargo, ha merecido la pena porque estos alumnos sí que se han mostrado muy interesados en llevar a cabo este tipo de actividades. Concretamente en el curso pasado, el reparto de una imagen secreta fue resuelta por aproximadamente un 25% de los alumnos de los alumnos que asistieron regularmente a las clases prácticas.

Concluimos comentado que hemos conseguido elaborar un material que será válido para cursos posteriores y que, por supuesto, seguiremos ampliando y mejorando. Las

actividades están diseñadas para su uso por alumnos de Ingeniería Informática pero también se pueden aprovechar para otras titulaciones, sobre todo para otras ingenierías. Esperamos que el material expuesto en este trabajo pueda ser de interés para otro profesorado que imparte también esta asignatura.

6. Referencias

1. P. Pérez, M. Gangnet, M. Blake, "Poisson Image Editing", *ACM Transactions on Graphics* , vol. 22, nº 3, pp. 313-318, (2003).

2. A. Levin, "Colorization using optimization", *ACM Transactions on Graphics*, vol. 23, nº 3, Proceedings of ACM SIGGRAPH 2004, pp. 689-604, (2004).

3. S. Liping, Q. Zheng, L. Huan, Q. Jun, L. Bo, "Scrambling Matrix Generation Algorithm for High Dimensional Image Scrambling Transformation", *IEEE Conference on Industrial Electronics and Applications*, ICIEA 2008, 1707-1712, (2008).

4. B. Acharya, S. K. Panigraphy, S. K. Patra, G. Panda, " Image encryption with advanced Hill Cipher algorithm", *International Journal of Recent Trends in Engineering*, Vol. 1, No. 1,pp. 663-667, (2009).

5. N. Provos, "Hide and Seek: An Introduction to Steganography", *IEEE Security & Privacy. IEEE Computer Society*, pp. 32-44, (2003).

6. A. Shamir, "How share a secret", *Communications of the ACM*, 22 (11), pp. 612-613, (1976).

7. C. C. Thien and J. C. Lin, "Secret image sharing", *Computer and Graphics*, 26 (5), pp. 765-770, (2002).

8. A. Parakh, K. Subhash, "Space efficient secret sharing", *Information Sciences*, 181(2), pp. 335-341, (2011).

9. A. Martín del Rey, "A matrix-based secret sharing schemes for images", *Lectures and Notes in Computer Sciences*, 5197, pp. 635-642, (2008).

10. C. C. Chang, P. Y. Lin, Z. H. Wang, M. C. Li, "A Sudoku-based secret image sharing scheme with reversibility", *Journal of Communications*, vol. 5, nº 1, pp. 5-11, (2010).