# Traducciones de Paper Importantes

## A New Steganography Approach Using Sudoku With Digital Signature.

**ABSTRACT**

Steganography is a means of obscuring data where secret messages are hidden inside computer files such as images, sound files, videos and even executable files so that, no one except the sender and the receiver will suspect the existence of stealth information in it. Steganography may also involve the usage of cryptographywhere the message is first encrypted before it is concealed in another file. Generally, the messages appear to be something else such as an image, sound or video so that the transfer of secret data remains unsuspected. The main advantage of steganography over other methods such as cryptography is that, it will not arose suspicion even if the files fall in the hands of a third party. Thus steganography has an upper hand over cryptography as it involves both encryption and obscurity. This paper proposes a new approach on steganography using Sudoku puzzle with digital signature for providing authentication, integrity as well as non-repudiation.

**ABSTRACTO**

La Esteganografía es un medio de ocultar datos en mensajes secretos se ocultan dentro de los archivos de computadora, tales como imágenes, archivos de sonido, videos e incluso archivos ejecutables de manera que, nadie, excepto el remitente y el receptor serán sospechar la existencia de información de sigilo en el mismo. Esteganografía también puede implicar el uso de la criptografía en el que el mensaje es primero encriptado antes de que se oculta en otro archivo. En general, los mensajes parecen ser algo distinto, como una imagen, sonido o vídeo para que la transferencia de datos secreta permanece insospechada. La principal ventaja de la Esteganografía sobre otros métodos, como la criptografía es que, no se levantó sospechas, incluso si los archivos caen en manos de un tercero. Así Esteganografía tiene una ventaja sobre la criptografía, ya que implica el cifrado y la oscuridad. En este trabajo se propone un nuevo enfoque en la Esteganografía usando rompecabezas Sudoku con firma digital para proporcionar autenticación, integridad y no repudio.

**INTRODUCTION**

Steganography [7] is the art and science of invisible communication. This is accomplished through hiding in formation in other information, thus hiding the existence of the communicated in formation. Steganography differs from cryptography in the sense that, cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. An image used to cover the secret message is called the cover\_image, the data to be embedded inside the Cover\_image is called the hidden\_data, and the key used to encrypt the message is called the stego\_key. The output of these three is called as the stego\_medium. ‘Sudoku’ [11] originally called Number Place, is a logic-based, combinatorial number-placement puzzle. The objective is to fill a 9×9 grid with digits so that each column, each row, and each of the nine 3×3 sub-grids that compose the grid (also called "boxes", "blocks", "regions", or "sub-squares") contains all of the digits from 1 to 9. The puzzle setter provides a partially completed grid, which for a well-posed puzzle has a unique solution. Completed puzzles are always a type of Latin square with an additional constraint on the contents of individual regions. For example, the same single integer may not appear twice in the same row, column or in any of the nine 3×3 sub regions of the 9x9 playing board.

**INTRODUCCION**

Esteganografía [7] es el arte y la ciencia de la comunicación invisible. Esto se logra a través de esconder la formación en otra información, ocultando así la existencia del comunicado en formación. Esteganografía difiere de la criptografía en el sentido de que, la criptografía se centra en mantener el contenido de un mensaje secreto, Esteganografía se centra en mantener la existencia de un mensaje secreto. La imagen que se utiliza para cubrir el mensaje secreto se llama el **Cover Image**, los datos que se incrustan dentro del **Cover Image** se llama el **Hidden Data**, y la clave utilizada para cifrar el mensaje se llama la clave **Stego**. La salida de estos tres se llama como el medio stego. 'Sudoku' [11] originalmente llamado Number Place, es una combinatoria rompecabezas-colocación basadas en la lógica. El objetivo es rellenar una cuadrícula de 9 × 9 con los dígitos de manera que cada columna, cada fila y cada una de las nueve de 3 × 3 sub-redes que componen la red (también llamadas "cajas", "bloques", "regiones" o "cuadrados sub") contiene todos los dígitos del 1 al 9. El colocador rompecabezas proporciona una cuadrícula parcialmente completado, lo que para un puzle bien planteado tiene una solución única. Rompecabezas completadas son siempre un tipo de cuadrado latino con una restricción adicional sobre el contenido de las distintas regiones. Por ejemplo, el mismo entero sola no puede aparecer dos veces en la misma fila, columna o en cualquiera de las subregiones y nueve 3 × 3 del tablero de 9x9 de juego.

Sudoku types and classes [12]

* Polyomino A shape composed of equal sized, side-adjacent squares. Often used for sudokuregion variants. Polyominos are named by size: (5) pentomino, (6) hexomino, (7) heptomino, (8) octomino, and (9) nonomino.
* Du-sum-oh 5×5, 6×6, 7×7, 8×8 or 9×9 grid with irregular, polyomino, shaped regions and minimal number of clues.
* 9×9 Sudoku Classic 9×9 grid with nine 3×3 regions.

This scheme uses an 18x18 sudoku reference matrix as the key for embedding the secret message into the cover\_image.

Sudoku tipos y clases [12]

* Polyomino Una forma compuesta de, cuadrados adyacentes laterales de igual tamaño. A menudo se utiliza para variantes de la región sudoku. Poliominós se nombran por tamaño: (5) pentominó, (6) hexominó, (7) heptomino, (8) octomino, y (9) nonomino.
* Du-suma-oh 5 × 5, 6 × 6, 7 × 7, 8 × 8 o 9 × 9 cuadrícula con, polyomino, regiones en forma irregular y número mínimo de pistas.
* 9 × 9 Sudoku Clásico 9 × 9 cuadrícula con nueve 3 × 3 regiones.

Este esquema utiliza una matriz de referencia 18x18 sudoku como la clave para incrustar el mensaje secreto en la imagen de portada.

Before going to the deep description about this scheme, we have to know about how an image is represented. An image [13] is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. In a (8-bit) greyscale image each picture element has an assigned intensity that ranges from 0 to 255. A grey scale image is what people normally call a black and white image, but the name emphasizes that such an image will also include many shades of grey. A normal greyscale image has 8 bit color depth = 256 greyscales. A “true color” image has 24 bit color depth = 8 x 8 x 8 bits = 256 x 256 x 256 colors = ~16 million colors.This scheme uses a 24 bit cover\_image for hiding the secret message. In 24-bit RGB schemes, a single pixel is represented by 3 bytes. Each byte represents 8 bits of either red, green, or blue component information.

Antes de ir a la descripción profunda sobre este esquema, hay que saber acerca de cómo se representa una imagen. Una imagen [13] es una matriz o una matriz de píxeles cuadrados (elementos de imagen) dispuestos en columnas y filas. En la imagen en escala de grises a (8 bits) cada elemento de imagen tiene una intensidad asignada que va de 0 a 255. Una imagen en escala de grises es lo que la gente normalmente llaman una imagen en blanco y negro, pero el nombre hace hincapié en que una imagen así también incluirá muchos sombras de Grey. Una imagen en escala de grises normal tiene 8 bits de color de profundidad = 256 escalas de grises. Una imagen de "color verdadero" tiene 24 bits de profundidad de color = 8 x 8 x 8 bits = 256 x 256 x 256 colores = ~ una imagen de la portada de 24 bits esquema de 16 millones de colores. Esta utiliza para ocultar el mensaje secreto. En los esquemas de RGB de 24 bits, un solo píxel está representado por 3 bytes. Cada byte representa 8 bits de información, ya sea rojo, verde, o azul componente.

When transferring the message inside a cover image to the receiver, one of major problems we will be facing is about the authentication, data integrity and the non-repudiation. In order to know whether the transmitted message is tampered or not, from where it comes from, this paper uses Digital signature which solves the above.

A ‘Digital Signature’ [6] is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

Digital signatures [5] employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures can also provide non-repudiation [10], meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid.

Al transferir el mensaje de una imagen de la cubierta interior hacia el receptor, uno de los principales problemas que estaremos enfrentando es acerca de la autenticación, integridad de datos y el no repudio. Con el fin de saber si es manipulado el mensaje transmitido o no, de dónde viene, este trabajo utiliza la firma digital que resuelve los anteriores.

Una 'Firma Digital' [6] es un esquema matemático para demostrar la autenticidad de un mensaje digital o documento. Una firma digital válida da una razón destinatario para creer que el mensaje fue creado por un remitente conocido, de tal manera que el remitente no puede negar haber enviado el mensaje (autenticación y el no repudio) y que el mensaje no se ha alterado en tránsito (integridad).

Las firmas digitales [5] emplean un tipo de criptografía asimétrica. Para los mensajes enviados a través de un canal no seguro, una firma digital adecuadamente implementado da la razón receptor a creer que el mensaje fue enviado por el remitente reclamado. Las firmas digitales también pueden proporcionar no repudio [10], lo que significa que el firmante no puede alegar con éxito que no firmaron un mensaje, mientras que también reclaman su clave privada se mantiene en secreto; Además, algunos esquemas de no repudio ofrecen un sello de tiempo para la firma digital, por lo que incluso si se expone la clave privada, la firma es válida.

**LITERATURE SURVEY**

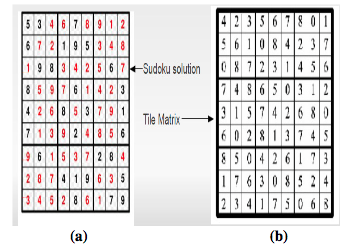
The first work on steganography using Sudoku puzzle was “An Information Hiding Scheme Using Sudoku” byC.C. Chang, Y.C. Chou and T.D. Kieu [2].

**Chang et al’s method [2]**

**Generating Reference matrix (M)**

1. A “tile” matrix T is constructed by subtracting every digit in a Sudoku puzzle by one.
2. The reference matrix, M is then consisting of an m×m tiling of copies of T, where m=|\_256/9\_|. figure 1
3. matrix M has to be truncated to 256×256.

This procedure is shown in the figure 1.



ENCUESTA LITERARIA

El primer trabajo sobre la Esteganografía usando rompecabezas Sudoku fue "un ocultamiento de información Esquema Usando Sudoku" byC.C. Chang, Y.C. Chou y T.D. Kieu [2].

El método de Chang et al [2]

Matriz de generación de Referencia (M)

1. Una matriz "baldosas" T se construye restando cada dígito en un rompecabezas Sudoku por uno.
2. La matriz de referencia, M es entonces que consta de un m × m mosaico de copias de T, donde m = | \_256 / 9\_ |. Figura 1
3. Matriz M tiene que ser truncado a 256 × 256.

**DATA EMBEDDING AND EXTRACTION**

1. Convert the secret bit stream into secret digits in the base-9 numeral system. S=s1 s2 s3....sn, where, n is the number of converted secret digits and sk є [0, 8], 1≤k≤n.
2. The cover image is partitioned into R non-overlapping blocks of size 1×2.

It has some drawbacks:

It is used for only 8-bit grayscale cover image, and the Size of the reference matrix M is designed to be 256× 256.

These limitations was modified later by Shetty et al [3]. In these methods, it was unable to find whether the cover\_image is modified or not. Later, “A Novel Steganographic Scheme using Sudoku”by Arnab Kumar Maji, Rajat Kumar Pal and Sudipta Roy [1], developed a technique in order to avoid the above drawbacks

**INCRUSTACION DE DATOS Y EXTRACCION**

1. Convertir el flujo de bits secreta en dígitos secretas en el sistema de numeración de base-9. S = S1 S2 S3 .... Sn, donde, n es el número de dígitos secretos convertidos y sk є [0, 8], 1≤k≤n.
2. La imagen de la portada se divide en R bloques no solapados de tamaño de 1 × 2.

Tiene algunos inconvenientes:

Sólo se utiliza imagen de la portada de escala de grises de 8 bits para, y el tamaño de la matriz de referencia M está diseñado para ser 256 × 256.

Estas limitaciones se modificó más tarde por Shetty et al [3]. En estos métodos, que era incapaz de encontrar si la imagen de la portada es modificado o no. Más tarde, “A Novel Steganographic Scheme using Sudoku” por Arnab Kumar Maji, Rajat Kumar Pal y Sudipta Roy [1], desarrolló una técnica para evitar los inconvenientes anteriores

**Arnab Method**

The main goal of this method was to deliver the message integrity. An 8x8 Sudoku puzzle is used to check whether that there is any modifications in the cover\_image and an 18x18 reference matrix used as the key.[1]

**Embedding an 8x8 sudoku matrix into the cover image**

The cover image is divided into 64 blocks and each block consists of 3 pixel groups. Solved Sudoku values are embedded inside the LSB of the B (Blue) components of the each pixel groups.

**Embedding message inside the cover image**

Initially an 18x18 sudoku reference matrix is taken. Then convert the message into base-9 format. Find out the base-9 value in the reference matrix and depending upon it, update the values of R and G components of each pixel group.

**Check the integrity of the cover image**

For that, we need to send the 8x8 sudoku instance to the receiver. The receiver now solves the Sudoku puzzle and stores it. Then the receiver divides the cover image and takes out the last bit of each pixel group and kept it in an 8x8 matrix. If the solved sudoku puzzle is equivalent to the values kept inside the 8x8 matrix, then the integrity is maintained. Otherwise, the image has been modified. But, this method also has certain limitations.

1. This method only provides the message integrity.
2. This doesn’t provide any authentication and non-repudiation.

**Método Arnab**

El objetivo principal de este método consistía en entregar la integridad del mensaje. Un 8x8 Sudoku rompecabezas se utiliza para comprobar si que hay alguna modificación en la imagen de portada y una matriz de 18x18 de referencia utilizados como clave. [1]

**Incorporación de una matriz sudoku 8x8 en la imagen de portada**

La imagen de la portada se divide en 64 bloques y cada bloque consta de 3 grupos de píxeles. Valores Sudoku resueltos están incrustados dentro de los del B (azul) los componentes de los grupos de cada píxel LSB.

**Incorporación de mensaje de la imagen de la portada interior**

Inicialmente se toma una matriz de referencia 18x18 sudoku. A continuación, convertir el mensaje en formato de base-9. Averiguar el valor base-9 en la matriz de referencia y dependiendo de ella, actualizar los valores de R y componentes g de cada grupo de píxeles.

**Compruebe la integridad de la imagen de la portada**

Por eso, tenemos que enviar la instancia sudoku 8x8 al receptor. El receptor ahora resuelve el rompecabezas Sudoku y lo almacena. Entonces el receptor divide la imagen de la portada y saca el último bit de cada grupo de píxeles y lo mantuvo en una matriz de 8x8. Si el rompecabezas sudoku resuelto es equivalente a los valores guardados dentro de la matriz de 8x8, a continuación, se mantenga la integridad. De lo contrario, la imagen ha sido modificado. Pero, este método también tiene ciertas limitaciones.

1. Este método sólo proporciona la integridad del mensaje.
2. Esto no proporciona ninguna autenticación y el no repudio.

**PROPOSED SYSTEM**

As explained in the earlier sections, authentication, non-repudiation and integrity are the major factors to be take care of while sending the data inside a cover\_image. This scheme uses the digital signature for providing the above factors.This approach uses a 24 bit colored image to hide the data, an 18x18 reference matrix as the key and the digital signature which is embedded inside the cover\_image.

**Embedding the digital signature inside the cover\_image**

The procedure below describes how the digital signature is embedded inside a cover\_image.

**Generating the private and public keys**

For embedding the digital signature inside a cover\_image, first of all the sender will create asymmetric key pairs of size 128 bits using RSA algorithm or Elgamal algorithm. Public key of the sender will be visible to all who wishes to communicate with him. And his private key will not be revealed to all and it is kept as secret [4].

**Generating the digital signature**

The Sender, will hold a plain message which he want to transform it as the digital signature [9].The process is as follows:

* Hashing: Using any one of the hashing techniques such as SHA1, Message Digest 5 (MD5) etc. find the hash value of the message. The generated output is known as the message digest. This process ensures the message integrity.
* Encryption: message digest is then encrypted using private key of the sender using RSA algorithm [8]. It is used to sign the message digest. The original message can be recovered by decrypting the message signature using corresponding public key of sender. To obtain non-repudiation, signing is performed. Now we have created the digital signature. Next step is,
* Packing: The plain message, message signature and the public Key of the sender are packed together into a single packed unit.
* Encryption:The single packed unit of message which contains plain message and message signature along with the public key of the sender is encrypted using receipt’s public key by RSA algorithm to form signed and encrypted message.

The output of the last process (Encryption) can vary in size depending upon the hashing technique and encryption techniques used. And also it will be in hexadecimal format. Convert those hexadecimal values to binary values.

The next process is same as the “Block preparation” of the paper [1].

**SISTEMA PROPUESTO**

Como se explica en las secciones anteriores, la autenticación, no repudio y la integridad son los principales factores que cuidar al enviar los datos dentro de un cover\_image. Este esquema utiliza la firma digital para proporcionar el enfoque. La anterior utiliza una imagen en color de 24 bits para ocultar los datos, una matriz de 18x18 de referencia como la clave y la firma digital que se incrusta la imagen de la portada interior.

**Incorporación de la firma digital en el interior del cover\_image.**

El procedimiento siguiente describe cómo se encaja la firma digital dentro de un cover\_image.

**La generación de las claves privadas y públicas**

Para la incorporación de la firma digital dentro de un cover\_image, en primer lugar el remitente creará pares de claves asimétricas de tamaño de 128 bits utilizando el algoritmo RSA o algoritmo Elgamal. Clave pública del remitente será visible a todos los que desea comunicarse con él. Y su clave privada no se dará a conocer a todos y se mantiene como secreto [4].

**La generación de la firma digital**

El remitente, contendrá un mensaje sencillo que quieren transformarla como la firma digital [9] .

El proceso es el siguiente:

* Hashing: El uso de cualquiera de las técnicas de hashing como SHA1, Message Digest 5 (MD5), etc. encontrar el valor de hash del mensaje. La salida generada es conocido como el resumen del mensaje. Este proceso asegura la integridad del mensaje.
* Cifrado: resumen del mensaje se cifra con la clave privada del remitente utilizando RSA algoritmo [8]. Se utiliza para firmar el resumen del mensaje. El mensaje original puede ser recuperado por descifrar la firma del mensaje utilizando la clave pública del remitente correspondiente. Para obtener el no repudio, se lleva a cabo la firma. Ahora hemos creado la firma digital. El siguiente paso es:
* Embalaje: El mensaje sencillo, firma del mensaje y la clave pública del remitente se embalan juntos en una sola unidad de empaquetado.
* Cifrado: La unidad de empaquetado sencillo de mensaje que contiene el mensaje claro y mensaje de la firma junto con la clave pública del remitente se cifra utilizando la clave pública de la recepción por el algoritmo RSA para formar la firma y el mensaje cifrado.

La salida del último proceso (cifrado) puede variar en tamaño dependiendo de las técnicas de la técnica de hashing y de cifrado utilizadas. Y también será en formato hexadecimal. Convertir esos valores hexadecimales a valores binarios. El siguiente proceso es igual a la "preparación de bloques" del papel [1].

**Block preparation**

Divide the cover\_image into 64 blocks. Now Group 3 pixels in each block. Each pixel holds RGB (Red, Blue, and Green) components. These components holds 8 bit value each. Extract the B (Blue) components of each pixel. Now we take the encrypted value of the last process which is now in the binary format and embed each value one by one into the last 2 bits of the B (Blue) components of every pixel. Thus only 2 bits get changed [1].

**Embedding hidden message**

As described earlier, the cover\_image is divided into 64 blocks with 3 pixel groups in it. Its B (Blue) component holds the digital signature, the public key of the sender and the plain message, in the encrypted form. Its other components, such as Red and Green holds the secret message. Digital signature is used to ensure the authentication, message integrity as well as the non-repudiation.

**Generation of 18x18 reference matrix**

Initially we take a 9x9 sudoku puzzle with some clues given, solve it. Now subtract 1 from each value of the puzzle. So that the value ranges from 0-8.Replicate the 9x9 sudoku puzzle into an 18x18 reference matrix in a square form. An example of 18x18 reference matrix generated from 9x9 sudoku puzzle is shown in the figure 2 and 3.

**La preparación de bloques**

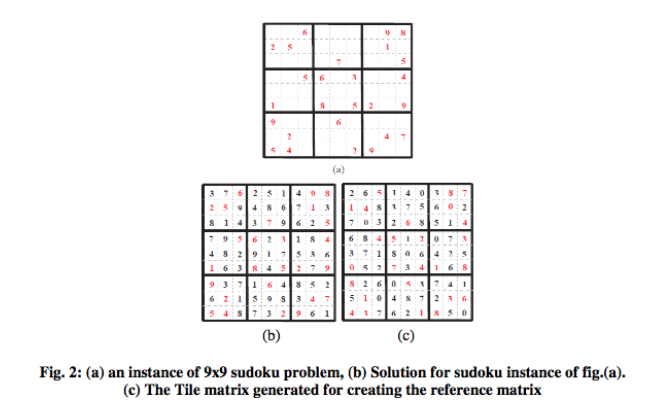
Dividir la imagen de portada en 64 bloques. Ahora Grupo 3 píxeles en cada bloque. Cada píxel contiene RGB (rojo, azul y verde) componentes. Estos componentes sostiene 8 valor de bits cada uno. Extraiga los componentes B (Azul) de cada píxel. Ahora tomamos el valor cifrado del último proceso que ahora está en el formato binario y integramos cada valor de uno a uno en los últimos 2 bits de la B (Azul) componentes de cada píxel. Por lo tanto sólo 2 bits se cambian [1].

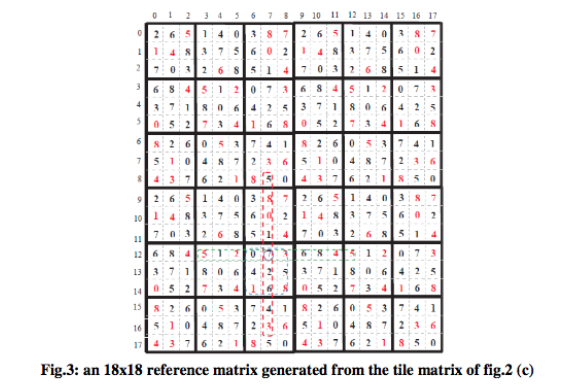
**Incorporación de mensaje oculto**

Como se describió anteriormente, la imagen del libro se divide en 64 bloques con 3 grupos de píxeles en el mismo. Su B (Azul) componente tiene la firma digital, la clave pública del remitente y el mensaje llano, en forma cifrada. Sus otros componentes, como el rojo y el verde sostiene el mensaje secreto. La firma digital se utiliza para asegurar la autenticación, la integridad del mensaje, así como el no repudio.

**Generación de matriz de referencia 18x18**

Inicialmente tomamos un rompecabezas sudoku 9x9 con algunas pistas dadas, resolverlo. Ahora resta 1 de cada valor del rompecabezas. Así que el valor oscila entre 0-8.Replicate el 9x9 rompecabezas sudoku en una matriz de referencia 18x18 en una forma cuadrada. Un ejemplo de matriz de referencia generada a partir de 18x18 rompecabezas sudoku 9x9 se muestra en la figura 2 y 3.

****



**Conversion of the secret message into base-9**

Take the all characters of secret message one by one, convert it into ASCII code (decimal) and then convert it again into base-9.This base-9 value will fall in the range from 0-8 which consist of 3 digits.

**Finding out the base-9 values in the reference matrix**

Select a pixel (p, x) where p and x are the random location of the pixel. Next, find the values:

X= (R%6)+6.

Y= (G%6)+6.

Where R and G are the Red and Green components of that pixel which is selected.

Now, find the cell (X,Y) in the 18x18 reference matrix .X is taken as the row number and Y is taken as the column number.

Now extract the values of the nine cells in the same row keeping (X,Y) as the middle of it and keep them in Pg. Similarly, extract the value of nine cells in the same column keeping (X,Y) as the middle of it and keep them in Pr. Next take the minigrid where the (X,Y) value belongs and store it in Pb.

Next, find the locations of (Xg,Yg) in Pg,(Xr,Yr) of Pr and (Xb,Yb) of Pb from the reference matrix. Find the deviations of (Xg,Yg), (Xr,Yr) and (Xb,Yb) from the location (X,Y).

**La conversión del mensaje secreto en la base 9**

Tome los todos los caracteres del mensaje secreto, uno por uno, convertirlo en código ASCII (decimal) y luego convertirlo de nuevo en base-9.Esta valor base-9 caerá en el rango de 0-8, que consta de 3 dígitos.

**Averiguar los valores de base-9 en la matriz de referencia**

Seleccionar un píxel (p, x), donde p y x son la ubicación aleatoria de píxel. A continuación, encontrar los valores:

X = (R%6)+6.

Y = (G%6)+6.

Donde R y G son los componentes verdes de ese píxel que se selecciona Rojo y Ahora, encontrar la célula (X, Y) en la matriz de 18x18 referencia se toma como el número de fila X e Y se toma como el número de columna.

Ahora extraer los valores de las celdas de nueve en el mismo mantenimiento de fila (X, Y) como el centro de la misma y mantenerlos en Pg. Del mismo modo, extraer el valor de nueve celdas de la misma el mantenimiento de la columna (X, Y) como el centro de la misma y mantenerlos en Pr. A continuación, tomar el mini rejilla donde el (X, Y) Valor pertenece y almacenarlo en Pb.

A continuación, encontrará la ubicación de (Xg, Yg) en PG, (Xr, Yb) de Pb y (Xb, Yb) de Pb de la matriz de referencia. Encuentra las desviaciones de (Xg, Yg), (Xr, Yr) y (Xb, Yb) de la ubicación (X, Y).

**Updating the R and G values of each pixel**

If (Xg,Yg) has the minimum deviation from the (X,Y) location then, Update R and G components of the pixel (p,x) as:

R=R-(X-Xg),

G=G-(Y-Yg)

B holds the digital signature as described earlier.

An example now shows how the above procedure works:

Selecting a random pixel location, we get X=12 and Y=7. The corresponding value of (12,7) is 7 which is marked inside a circle. Now, suppose that we want to encrypt the secret message starting with ‘A’. The ASCII code of A is 65.Then converting to base-9 code, it will be 027.Now, we are going to embed 0 in the first pixel. For that, what we do is that, take the values from Pg,Pr and Pb. The elements of Pg,Pr and Pb are located in the figure 3 respectively represented as green, red and blue. Find the presence of 0 in Pg, Pr, Pb. Then find the least deviation among them. We found that the least deviation is in Pg. Now change the values of R and G accordingly.

**La actualización de los valores de R y G de cada píxel**

Si (Xg, Yg) tiene la desviación mínima de la (X, Y) ubicación, entonces, los componentes de actualización de R y G del píxel (p, x) como:

R = R-(X-Xg),

G = G-(Y-Yg)

B tiene la firma digital como se describe anteriormente.

Un ejemplo muestra ahora cómo funciona el procedimiento anterior:

Selección de la ubicación de píxeles aleatoria, obtenemos X = 12 e Y = 7. El valor correspondiente de (12,7) es 7 que está marcada dentro de un círculo. Ahora, supongamos que queremos cifrar el mensaje secreto que empiezan con 'A'. El código ASCII de A es 65. Entonces convertir basar-9 código, será 027. Ahora, vamos a integrar 0 en el primer píxel. Por eso, lo que hacemos es que, toma los valores de Pg, Pr y Pb. Los elementos de Pg, Pr y Pb se encuentran en la figura 3, respectivamente, representado como verde, rojo y azul. Encuentra la presencia de 0 en Pg, Pr, Pb. A continuación, busque la menor desviación entre ellos. Se encontró que la menor desviación está en Pg. Ahora cambiar los valores de R y G en consecuencia.

**Verification of the digital signature**

As described earlier, sender will send the cover\_image which holds the single packed unit of message that contain plain message and message signature along with the public of the sender which is encrypted using receipt’s public key to form signed and encrypted message to the receiver side. Now, at the receiver side, how the decryption and signing is done, is explained [4]:

Decryption: In this step, the received cover\_image is divided into 64 blocks and inside each block 3 pixel groups are created. Now, extract the last 2 bits of the B (Blue) components of each pixel of the cover\_image which consists of packed unit which is now in the binary value and also in encrypted form. Convert it from binary to hexadecimal in order to decrypt it

Unpack: Now, decrypt it using the receiver’s private key to form a packed unit of message containing plain message, the signature and the public key of the sender.

Hashing: In this Step, plain message which is obtained after decrypting and unpacking the received message is input to hash function that was used by the sender to compute message digest.

Decryption: In this step, the received message signature is decrypted by using the received public key of the sender. By decryption, message digest is obtained which was computed before the transmitting the message.

Comparison: At last in this step, message digest obtained after decrypting the received message signature and message digest, computed from the plain message is compared. If they match, then the authentication, integrity and non-repudiation is maintained; otherwise image has been changed or tampered by an intruder.

Signed and encrypted data or message can only be decrypted using the correct Private Key of the recipient thus ensuring the privacy. Hashing and Signature verification offer the integrity, authenticity and nonrepudiation.

**La verificación de la firma digital**

Como se describió anteriormente, el remitente envía la imagen de portada que mantiene la unidad de empaquetado sencillo de mensaje que contiene el mensaje claro y firma del mensaje junto con el público del remitente que está cifrada con la clave pública del destinatario para formulario firmado y el mensaje cifrado al lado del receptor. Ahora, en el lado del receptor, cómo se realiza el cifrado y la firma, se explica [4]:

Descifrado: En este paso, la imagen de portada recibido se divide en 64 bloques y dentro de cada píxel bloque 3 grupos son creados. Ahora, extraer los 2 últimos bits de la B (Azul) componentes de cada píxel de la imagen de la portada, que consiste en la unidad de empaquetado, que se encuentra ahora en el valor binario y también en forma encriptada. Convertirlo de binario a hexadecimal con el fin de descifrar

Desembalaje: Ahora, descifrarlo utilizando la clave privada del receptor para formar una unidad compacta de mensaje que contiene el mensaje sin formato, la firma y la clave pública del remitente.

Hashing: En este paso, el mensaje sencillo que se obtiene después de descifrar y descomprimir el mensaje recibido es la entrada a la función que fue utilizado por el emisor para calcular resumen del mensaje de hash.

Descifrado: En este paso, la firma del mensaje recibido se cifra mediante la clave pública recibida del remitente. Por descifrado, resumen del mensaje se obtiene que fue calculado antes de la transmisión del mensaje.

Comparación: Por fin en este paso, resumen de mensaje obtenida después de descifrar la firma recibida mensaje y resumen del mensaje, calculado a partir del mensaje de llanura se compara. Si coinciden, entonces se mantiene la autenticación, integridad y no repudio; de lo contrario la imagen se ha cambiado o alterado por un intruso.

Firmado y datos cifrados o mensaje sólo se pueden descifrar con la clave privada correcta del destinatario que garantiza la privacidad. Hashing y verificación de firmas ofrecen la integridad, autenticidad y no repudio.