

H04K

SECRET COMMUNICATION; JAMMING OF COMMUNICATION

Definition statement

This place covers:

This subclass covers secret line and radiation transmission systems in which the signal is modified at the transmitting station in such a way that the information cannot be intelligibly received without corresponding modification at the receiving station.

The signal can be modified using, for example, frequency scrambling or scrambling by combination with a second signal.

This subclass also covers the jamming of communications and counter-measures against jamming or against surveillance.

Relationships with other classification places

Systems using reduced bandwidth or suppressed carrier techniques, or using sub-carriers or spread spectrum techniques are classified in [H04B](#). In particular, spread spectrum as counter-measure against jamming is classified in [H04K 3/00](#) whereas spread spectrum communication as such is classified in [H04B](#).

Analogue scrambling, jamming or counter-measures to achieve secure communication are classified in [H04K](#) whereas encryption of digital signals is classified in [H04L](#).

References

Application-oriented references

Examples of places where the subject matter of this place is covered when specially adapted, used for a particular purpose, or incorporated in a larger system:

Means for anti-jamming used in radar or analogous systems	G01S 7/36
Jamming means used in radar or analogous systems	G01S 7/38
Counter-measures or counter-counter-measures used in lidar or analogous systems	G01S 7/495
Counter-measures or counter-counter-measures used in sonar or analogous systems	G01S 7/537
Arrangements for the secret or secure communication of digital information, encryption of digital signals	H04L 9/00
Secrecy systems used in scanning, transmission or reproduction of documents	H04N 1/44
Analogue secrecy systems or analogue subscription systems for television	H04N 7/16

Informative references

Attention is drawn to the following places, which may be of interest for search:

Arrangements for protecting computers or computers systems	G06F 21/00
Ciphering or deciphering apparatus per se	G09C
Systems with reduced bandwidth or suppressed carrier	H04B 1/66 , H04B 1/68

Spread spectrum techniques	H04B 1/69
Photonic quantum communication	H04B 10/70
Protection from unauthorised access for optical transmission, e.g. eavesdrop protection	H04B 10/85
Transmission systems characterised by the use of a sub-carrier	H04B 14/08
Arrangements for preventing the taking of data from a data transmission channel without authorisation	H04L 12/22
Selective content distribution, e.g. interactive television, VOD	H04N 21/00

Glossary of terms

In this place, the following terms or expressions are used with the meaning indicated:

Secret communication	Secret line and radiation transmission systems, i.e., those in which the signal is modified at the transmitting station in such a way that the information cannot be intelligibly received without corresponding modification at the receiving station.
Jamming of communication	Apparatus, circuits or systems purposefully trying to interfere with the physical transmission and reception of communication.
Frequency scrambling	Transposing or inverting parts of the frequency band or by inverting the whole band
Follower jammer	Jammer adapted to determine and follow the frequency of a jamming target signal that uses frequency hopping techniques
Look-through mode	Operation mode wherein jamming and monitoring of the jamming target alternate
Reactive jammer	Jammer wherein jamming is activated only when a target has been detected
RCIED	Remote Controlled Improvised Explosive Device

Synonyms and Keywords

In patent documents, the following words/expressions are often used as synonyms:

- "confidential", "sensitive", "undercover", "private", "sneaky"
- "hidden", "scrambled", "blinded", "obscured", "obfuscated", "masked", "concealed", "covert", "coded"

H04K 1/00

Secret communication

Definition statement

This place covers:

Secret communication in the analogue domain for speech and non-speech data.

Relationships with other classification places

Secret communication in the analogue domain, or analogue scrambling, jamming or counter-measures are classified in [H01K 1/00](#) whereas transmission systems for the secret or secure communication of digital information are classified in [H04L](#), with details of encryption in the digital domain most likely classified in [H04L 9/00](#) and [H04L 12/00](#).

References

Informative references

Attention is drawn to the following places, which may be of interest for search:

Ciphering or deciphering apparatus per se	G09C
Systems with reduced bandwidth or suppressed carrier	H04B 1/66
Spread spectrum techniques in general	H04B 1/69
By using a sub-carrier	H04B 14/08
By multiplexing	H04J
Transmission systems for secret digital information, encryption of digital signals	H04L 9/00 , H04L 12/00
Secret or subscription television systems	H04N 7/16 , H04N 21/00

H04K 3/00

Jamming of communication; Counter-measures

Definition statement

This place covers:

"jamming", only when it means purposefully trying to interfere with the physical transmission and reception of communication.

Provided this condition is met, this group covers devices and methods for:

- jamming of communication, e.g. jamming by intentionally decreasing the signal to noise ratio, deceptive jamming ([H04K 3/65](#)), passive jamming ([H04K 3/68](#)), destructive jamming ([H04K 3/62](#));
- countermeasures against jamming ([H04K 3/20](#));
- countermeasures against undesired self-jamming resulting from jamming ([H04K 3/28](#));
- countermeasures against surveillance, interception or detection ([H04K 3/82](#));
- other electronic countermeasures using or against electromagnetic or acoustic waves ([H04K 3/00](#));
- signal detection techniques used in relation to jamming for interception and monitoring of the jamming target signal ([H04K 3/45](#));
- signal detection techniques used in relation to anti-jamming for jamming detection ([H04K 3/22](#));
- signal detection techniques used in relation to anti-surveillance for surveillance detection ([H04K 3/822](#))

In particular, this group covers:

- jamming for testing or assessing countermeasures ([H04K 3/94](#));
- jamming used to prevent cellular phone communication ([H04K 2203/16](#)), e.g. in a vehicle during motion ([H04K 3/415](#)), in particular areas, including prisons, hospitals, planes, petrol stations, theatres ([H04K 3/84](#)), and to trigger RCIEDs ([H04K 3/92](#) and [H04K 2203/24](#));
- jamming used to prevent reception of positioning data using GPS ([H04K 3/90](#));
- jamming used to prevent wireless communication in ad hoc networks or in sensor networks ([H04K 2203/18](#));
- jamming used to prevent exchange of data between wirelessly connected devices or device units, on Bluetooth®, infrared or near field links;
- jamming used to prevent unauthorized access to network, service or information ([H04K 3/86](#)), including access to a WLAN network ([H04K 2203/18](#)) and access to information stored in contactless carriers, including RFID carriers ([H04K 2203/20](#));
- jamming used to prevent transmission of an alarm against burglary or vehicle theft ([H04K 3/88](#));

Definition statement

- jamming used to prevent remote control of devices ([H04K 3/92](#));
- jamming used to prevent surveillance ([H04K 3/82](#)), e.g. of speech in meeting rooms ([H04K 2203/12](#)), of electromagnetic emissions from a computer screen [H04K 2203/14](#));
- jamming used to prevent interception or detection of a wirelessly transmitted signal ([H04K 3/825](#)).

Relationships with other classification places

[H04K 3/00](#) and [H04B](#)

Terminology

Jamming should be understood as meaning "intentional disturbance".

Interference should be understood as meaning "unintentional disturbance".

Anti-jamming

Jamming and anti-jamming techniques are covered by [H04K 3/00](#) and lower.

Anti-interference techniques are covered by [H04B](#).

Cancellation of "self-jamming"

- intentional self-jamming (e.g. self-jamming of receiver to counter interference; self-jamming of transmitter to counter surveillance): [H04K](#);
- undesired self-jamming caused by transmitting: [H04B 1/525](#);
- undesired self-jamming caused by transmitting a jamming signal intentionally: [H04B 1/525](#) and [H04K 3/28](#);

[H04K 3/00](#) and [H04K 1/00](#)

If the intentional self-jamming signal is known by the transmitter and the receiver of the jammed signal (and can therefore be regarded as a shared secret): [H04K 1/00](#)

Other cases of intentional self-jamming: [H04K 3/00](#)

References**Application-oriented references**

Examples of places where the subject matter of this place is covered when specially adapted, used for a particular purpose, or incorporated in a larger system:

Counter-measures used in radar or analogous systems	G01S 7/00
Counter-measures used in radar	G01S 7/36 , G01S 7/38
Counter-measures used in lidar	G01S 7/495
Counter-measures used in sonar	G01S 7/537

Informative references

Attention is drawn to the following places, which may be of interest for search:

Secret communication	H04K 1/00
Vehicle anti-theft relating to remote keyless entry	B60R 25/00
Vehicle anti-theft alarm transmission	B60R 25/102
Weapons	F41
Defence devices	F41H 11/00

Radars and GPS	G01S
Counter-measures used in radar or analogous systems	G01S 7/00
Remote keyless entry	G07C 9/00
Alarm and surveillance	G08B
Acoustics	G10K
Aerials	H01Q
Gain control	H03G 3/00
Automatic frequency control	H03J 7/00
Electric pulse generators	H03K 3/00
Transmission	H04B
Reducing, in transceivers, leakage of transmitter signal into the receiver	H04B 1/525
Spread spectrum techniques	H04B 1/69 - H04B 1/719
Suppression or limitation of noise or interference	H04B 15/00 , H04B 1/10
Monitoring or testing of receivers for locating or positioning the transmitter	H04B 17/27
Measuring or estimating channel quality parameters	H04B 17/309
Flow control or congestion control packet switching networks	H04L 47/135
Network architectures or network communication protocols for network security for supporting lawful interception, monitoring or retaining of communications or communication related information	H04L 63/30
Handfree telephone for vehicles	H04M 1/6075
Television systems	H04N 7/00
Wireless communications networks	H04W
Wireless security	H04W 12/00
Cognitive radio	H04W 16/14 , H04W 72/541
Wireless local area networks (WLAN)	H04W 84/12
Self-organizing networks, ad-hoc networks and sensor networks	H04W 84/18
Shielding	H05K 9/00

Special rules of classification

A patent document should be classified in [H04K 3/20](#) when the countered signal disturbance is:

- intentional (whether offensive or defensive) or
- used in a military, security or confidentiality context.

Glossary of terms

In this place, the following terms or expressions are used with the meaning indicated:

Jamming of communication	Purposefully trying to interfere with the physical transmission or reception of communication
Self-jamming resulting from jamming	Undesired interference, caused by a jamming device, to the communication of the jamming device itself or of a friendly device, and resulting from intentionally interfering with the communication of adversary devices

Follower jammer	Jammer adapted to determine and follow the frequency of a jamming target signal that uses frequency hopping techniques
Look-through mode	Operation mode wherein jamming and monitoring of the jamming target alternate
Reactive jammer	Jammer wherein jamming is activated only when a target has been detected

Synonyms and Keywords

In patent documents, the following abbreviations are often used:

(F)FH	(Fast) Frequency Hopping
GPS	Global Positioning System
NFC	Near Field Communication
RCIED	Remote Controlled Improvised Explosive Device
RFID	Radio Frequency IDentification
WLAN	Wireless Local Area Network

H04K 2203/20

for contactless carriers, e.g. RFID carriers

References

Informative references

Attention is drawn to the following places, which may be of interest for search:

Arrangements for sensing record carriers including arrangements for protecting the interrogation against piracy attacks	G06K 7/10257
Means for preventing undesired reading or writing from or onto record carriers by hindering electromagnetic reading or writing	G06K 19/07318