SECRET COMMUNICATION; JAMMING OF COMMUNICATION

In this subclass, the following expression is used with the meaning indicated:

- "secret communication" includes secret line and radiation transmission systems, i.e. those in which apparatus at the transmitting station modifies the signal in such a way that the information cannot be intelligibly received without corresponding modifying apparatus at the receiving station.

1/00 Secret communication

1/003 . (by varying carrier frequency at or within predetermined or random intervals (H04K 1/04 takes precedence))
1/006 . (by varying or inverting the phase, at periodic or random intervals)
1/02 . by adding a second signal to make the desired signal unintelligible
1/025 . . (using an analogue chaotic signal)
1/04 . by frequency scrambling, i.e. by transposing or inverting parts of the frequency band or by inverting the whole band
1/06 . by transmitting the information or elements thereof at unnatural speeds or in jumbled order or backwards
1/08 . by varying the polarisation of transmitted waves
1/10 . by using two signals transmitted simultaneously or successively

3/00 Jamming of communication; Counter-measures

3/20 . (Countermeasures against jamming (in radar G01S 7/36; interference suppression in receivers H04B 1/10))
3/22 . . (including jamming detection and monitoring)
3/222 . . . wherein jamming detection includes detecting the absence or impossibility of intelligible communication on at least one channel)
3/224 . . . (with countermeasures at transmission and/or reception of the jammed signal, e.g. stopping operation of transmitter or receiver, nulling or enhancing transmitted power in direction of or at frequency of jammer)
3/226 . . . . (Selection of non-jammed channel for communication (spectrum sharing arrangements H04W 16/14; selection of wireless resources by user or terminal H04W 72/02))
3/228 . . . . (Elimination in the received signal of jamming or of data corrupted by jamming (interference suppression in receivers H04B 1/10))
3/25 . . . (based on characteristics of target signal or of transmission (as countermeasure against surveillance H04K 3/827), e.g. using direct sequence spread spectrum or fast frequency hopping (spread spectrum techniques H04B 1/69))
3/255 . . . . (based on redundancy of transmitted data, transmission path or transmitting source)
3/28 . . . (with jamming and anti-jamming mechanisms both included in a same device or system, e.g. wherein anti-jamming includes prevention of undesired self-jamming resulting from jamming)
3/40 . . . (Jamming having variable characteristics)
3/41 . . . . (characterized by the control of the jamming activation or deactivation time (control of jamming activation and deactivation time only for the purpose of alternating between jamming mode and target monitoring mode H04K 3/45))
3/415 . . . . (based on motion status or velocity, e.g. for disabling use of mobile phones in a vehicle)
3/42 . . . (characterized by the control of the jamming frequency or wavelength)
3/43 . . . (characterized by the control of the jamming power, signal-to-noise ratio or geographic coverage area)
3/44 . . . (characterized by the control of the jamming waveform or modulation type)
3/45 . . . (characterized by including monitoring of the target or target signal, e.g. in reactive jammers or follower jammers for example by means of an alternation of jamming phases and monitoring phases, called "look-through mode")
3/46 . . . . (characterized in that the jamming signal is produced by retransmitting a received signal, after delay or processing)
3/60 . . . (Jamming involving special techniques)
3/62 . . . (by exposing communication, processing or storing systems to electromagnetic wave radiation, e.g. causing disturbance, disruption or damage of electronic circuits, or causing external injection of faults in the information)
3/65 . . . . (using deceptive jamming or spoofing, e.g. transmission of false signals for premature triggering of RCIED, for forced connection or disconnection to/from a network or for generation of dummy target signal)
Jamming or countermeasure used for a particular application

for acoustic communication

for the transfer of light or images, e.g. for video-surveillance, for television or from a computer screen

for telephony

for wireless local area networks or WLAN

for contactless carriers, e.g. RFID carriers (record carriers with integrated circuit chips including means for preventing undesired reading or writing from or to record carriers by hindering electromagnetic reading or writing G06K 19/07318; arrangements for sensing record carriers including arrangements for protecting the interrogation against piracy attacks G06K 7/10257)

for communication related to vehicles

for communication related to weapons

Jamming or countermeasure characterized by the infrastructure components

including a particular configuration of antennas

involving multiple cooperating jammers

including means for exchanging jamming data between transmitter and receiver, e.g. in forward or backward direction