CPC COOPERATIVE PATENT CLASSIFICATION

H04K SECRET COMMUNICATION; JAMMING OF COMMUNICATION

NOTE

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** (ciphering or deciphering apparatus per se G09C; systems with reduced bandwidth or suppressed carrier H04B 1/66; spread spectrum techniques H04B 1/69; by using a sub-carrier H04B 14/08; by multiplexing H04J; transmission systems for secret digital information H04L 9/00; secret or subscription television systems H04N 7/16, H04N 21/00)

1/003 . {by varying carrier frequency at or within predetermined or random intervals, e.g. wobbling (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 {(selective content distribution involving video stream encryption H04N 21/2347, H04N 21/4408; selective content distribution involving multiplex stream encryption)}

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 of 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** (counter-measures used in radar or analogous systems G01S 7/00; {in radar G01S 7/36, G01S 7/38; in lidar G01S 7/495; in sonar G01S 7/537})

NOTES

1. {This group 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:
   a. jamming of communication:
      i. jamming by intentionally decreasing the signal to noise ratio
      ii. deceptive jamming
      iii. passive jamming
      iv. destructive jamming
   b. countermeasures against jamming
   c. countermeasures against undesired self-jamming resulting from jamming
   d. countermeasures against surveillance, interception or detection
   e. other electronic countermeasures using or against electromagnetic or acoustic waves
   f. signal detection techniques used in relation to
      i. jamming: for interception and monitoring of the jamming target signal
      ii. anti-jamming: for jamming detection,
      iii. anti-surveillance: for surveillance detection
   g. jamming for testing or assessing countermeasures
   h. jamming used to prevent:
      – cellular phone communication
         i. in a vehicle during motion
         ii. in particular areas, including prisons, hospitals, planes, petrol stations, theatres
         iii. to trigger RCIEDs - reception of positioning data using GPS
      – wireless communication in ad hoc networks or in sensor networks
      – exchange of data between wirelessly connected devices or device units, on Bluetooth, infrared or near field links
      – unauthorized access to network, service or information, including:
         i. access to a WLAN network
         ii. access to information stored in contactless carriers, including RFID carriers
      – transmission of an alarm, against burglary or vehicle theft
      – remote control of devices
      – surveillance
         i. of speech in meeting rooms
         ii. of electromagnetic emissions from a computer screen
      – interception or detection of a wirelessly transmitted signal }

2. {In this group, the following acronyms are used:
   GPS = global positioning system
   RCIED = remote controlled improvised explosive device
   RFID = radio frequency identification
   WLAN= wireless local area network }

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}

3/68 . . {using passive jamming, e.g. by shielding or reflection (shielding of apparatus or components against electric or magnetic field H05K 9/00)}

3/80 . {Jamming or countermeasure characterized by its function}

3/82 . . {related to preventing surveillance, interception or detection}

3/822 . . . {by detecting the presence of a surveillance, interception or detection}

3/825 . . . {by jamming}

3/827 . . . {using characteristics of target signal or of transmission (as countermeasure against jamming H04K 3/25), e.g. using direct sequence spread spectrum or fast frequency hopping (spread spectrum techniques H04B 1/69)}

3/84 . . {related to preventing electromagnetic interference in petrol station, hospital, plane or cinema}

3/86 . . {related to preventing deceptive jamming or unauthorized interrogation or access, e.g. WLAN access or RFID reading (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)}

3/88 . . {related to allowing or preventing alarm transmission}

3/90 . . {related to allowing or preventing navigation or positioning, e.g. GPS}

3/92 . . {related to allowing or preventing remote control}

3/94 . . {related to allowing or preventing testing or assessing}

2203/00 {Jamming of communication; Countermeasures}

2203/10 . {Jamming or countermeasure used for a particular application}

2203/12 . . {for acoustic communication}

2203/14 . . {for the transfer of light or images, e.g. for video-surveillance, for television or from a computer screen}

2203/16 . . {for telephony}

2203/18 . . {for wireless local area networks or WLAN}

2203/20 . . {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)}

2203/22 . . {for communication related to vehicles}

2203/24 . . {for communication related to weapons}

2203/30 . {Jamming or countermeasure characterized by the infrastructure components}

2203/32 . . {including a particular configuration of antennas}

2203/34 . . {involving multiple cooperating jammers}

2203/36 . . {including means for exchanging jamming data between transmitter and receiver, e.g. in forward or backward direction}