Techóriások gyűjtik az ötleteket a deepfake elleni harchoz

A Facebook és a Microsoft hat egyetemmel közösen meghirdette a Deepfake Detection Challenge-t: hatékony deepfake-felismerő technológiákat keresnek.

Hat egyetemmel közösen hirdetett versenyt a Facebook és a Microsoft kutatóknak, cégeknek, hogy olyan technológiákat dolgozzanak ki, melyekkel egyértelműen fel lehet ismerni a mesterséges intelligencia segítségével meghamisított videókat.

Széles összefogásra építenek

Bár a videók manipulálására alkalmas szoftverekkel már a 90-es években is kísérleteztek, a technológia mostanra ért kritikus fázisba. Az utóbbi években vészesen szaporodnak az olyan hamis tartalmak, melyek megtévesztésig hasonlítanak valós videókra, képekre, hangfelvételekre. A nagy tartalomszolgáltató és -megosztó oldalak ugyan tettek látványos bejelentéseket, hogy kitiltják a deepfake tartalmakat szolgáltatásaikból, csakhogy lassan lehetetlen lesz eldönteni, hogy mi hamisított és mi nem.

A Facebook technológiai igazgatója, *Mike Schroepfer* blogbejegyzésében a Deepfake Detection Challenge társadalmi célját hangsúlyozza. Ezért vontak be a Microsofttal széles körből támogatókat: a hat egyetem (Cornell Tech, MIT, Oxford, Berkeley, Marylandi Egyetem, College Park, Albany Egyetem) mellett civil szervezeteket is, például a WITNESS emberi jogi szervezetet. Utóbbi meghívása nem véletlen, hiszen a szervezet épp videókkal, fényképekkel küzd az emberi jogok megsértése ellen, így elemi érdeke, hogy egy videóról ki lehessen deríteni, hogy azt utólag manipulálták-e.

Mint Schroepfer írja, eredménytáblával, támogatásokkal és díjakkal is szeretnék ösztönözni a vállalkozó kedvűeket az új módszerek felkutatására. Arról azonban nem ír, hogy konkrétan mennyit kívánnak a projekt támogatására fordítani. A Deepfake Detection Challenge felügyeletére létrehoztak egy új irányító testületet is a két cég, valamint az egyetemek és a társadalmi szervezetek képviselőiből.

A társadalomra és a gazdaságra is veszélyes

A hamisítást lehetővé tevő, mesterséges intelligencián alapuló eszközök elképesztő ütemben fejlődnek. Lapunk is foglalkozott a Zao arccserélő app esetével, amely lényegében mindenkinek elérhetővé teszi a videomanipulálást. Az ilyen eszközök végképp kontrollálhatatlanná teszik a folyamatot, aminek beláthatatlanok a következményei. Ha csak a társadalmi hatását nézzük, választások manipulálására épp úgy alkalmasak, mint a közvélemény bármilyen célú befolyásolására.

Emellett vannak konkrét gazdasági kárai is. A The Wall Street Journal a közelmúltban adott hírt egy olyan esetről, hogy manipulált telefonhívással csaltak ki egy angol energetikai cégtől több százezer eurót. A hívó hangját ugyanis úgy sikerült manipulálni, hogy az angol cég vezetője azt hitte, a német anyavállalat vezérigazgatójától kapott szóbeli utasítást a pénz azonnali átutalásra. (Az már csak egy érdekes mellékszál, hogy egy magyar cég számlájára kellett utalnia a pénzt.)

Nem is ez volt az első ilyen eset. A Symantec pár hónapja azt állította a BBC-nek, hogy többször is találkoztak olyan incidenssel, amikor pénzügyi igazgatókat mesterséges intelligenciával manipulált telefonhívással vettek rá arra, hogy pénz utaljanak csalók számlájára. *Hugh Thompson,* a biztonsági cég technológiai igazgatója akkor még azt is megkockáztatta, hogy a csalók által használt modell valószínűleg közel tökéletes lehet. A hamisított hang előállításához szükséges hangmintákat manapság nem nehéz beszerezni, hiszen a megcélzott vezetők gyakran tartanak előadásokat, amiknek a felvétele aztán felkerül a YouTube-ra vagy a vállalat nyilvános weblapjára, de a pénzügyi gyorsjelentéseknél szokásos konferenciahívások felvételei is elérhetők nyilvánosan.

Az már más kérdés, hogy komoly aggályokat vethet fel egy vállalat belső folyamataival kapcsolatban az, ha egy alkalmazott a vezér egyetlen telefonhívására hajlandó elutalni akár általa nem ismert számlára is nagyobb összegeket.

Forrás: https://bitport.hu/a-bigtechek-gyujtik-az-otleteket-a-deepfake-elleni-harchoz

Válogatta: Fonyó Istvánné