Hiding in Skype

Computer science isn't just about using language, sometimes it's about losing it. Sometimes people want to send messages so secret that no one even knows the messages exist. A great place to lose language is inside a conversation.

Cryptography is the science of making messages unreadable. Spymasters have used secret codes for a thousand years or more. Now cryptography is a part of everyday life. It's used by the banks every time you use a cashpoint and by online shops when you buy something over the Internet. It's used by businesses that don't want their industrial secrets revealed and by celebrities who want to be sure that tabloid hackers can't read their texts.

Who called who?

Cryptography stops messages being read, but sometimes just knowing that people are having a conversation can reveal too much. Knowing a football star is exchanging hundreds of texts with his teammate's girlfriend suggests something is going on, for example. Similarly, the American CIA chief David Petraeus, whose downfall made international news, might have kept his secret and his job if the emails from his lover had been hidden. David Bowie kept his 2013 comeback single Where Are We Now? a surprise until the moment it was released. The dramatic surprise helped make the single a hit. But the secret could have been spoiled months before if music journalists had noticed Bowie having more conversations with his record label.

Sending messages gets hairy

That's where steganography comes in – the science of hiding messages so no one even knows they exist. Invisible ink is one form of steganography. It was used, for example, by the French resistance in World War II. Steganography has taken more bizarre forms over the years though – an Ancient Greek slave had a message tattooed on his shaven head warning of Persian invasion plans. Once his hair had grown back he delivered it unnoticed.

Digital communication opens up new ways to hide messages. Computers store information using a code of 0s and 1s. Each 1 or 0 is called a bit. Steganography is then about finding places to hide those bits. A team of Polish researchers led by Wojciech Mazurczyk have now found a way to hide them in a Skype conversation.

When you use Skype to make a phone call, the program converts the sounds you make to a long series of bits. They are sent over the Internet and converted back to sound at the other end. At the same time, bits stream back from the person you are talking to, containing the sound of their voice. Data transmitted over the Internet isn't sent all in one go, though. It's broken into packets: a bit like taking your conversation and tweeting it one line at a time.

Commando tactics

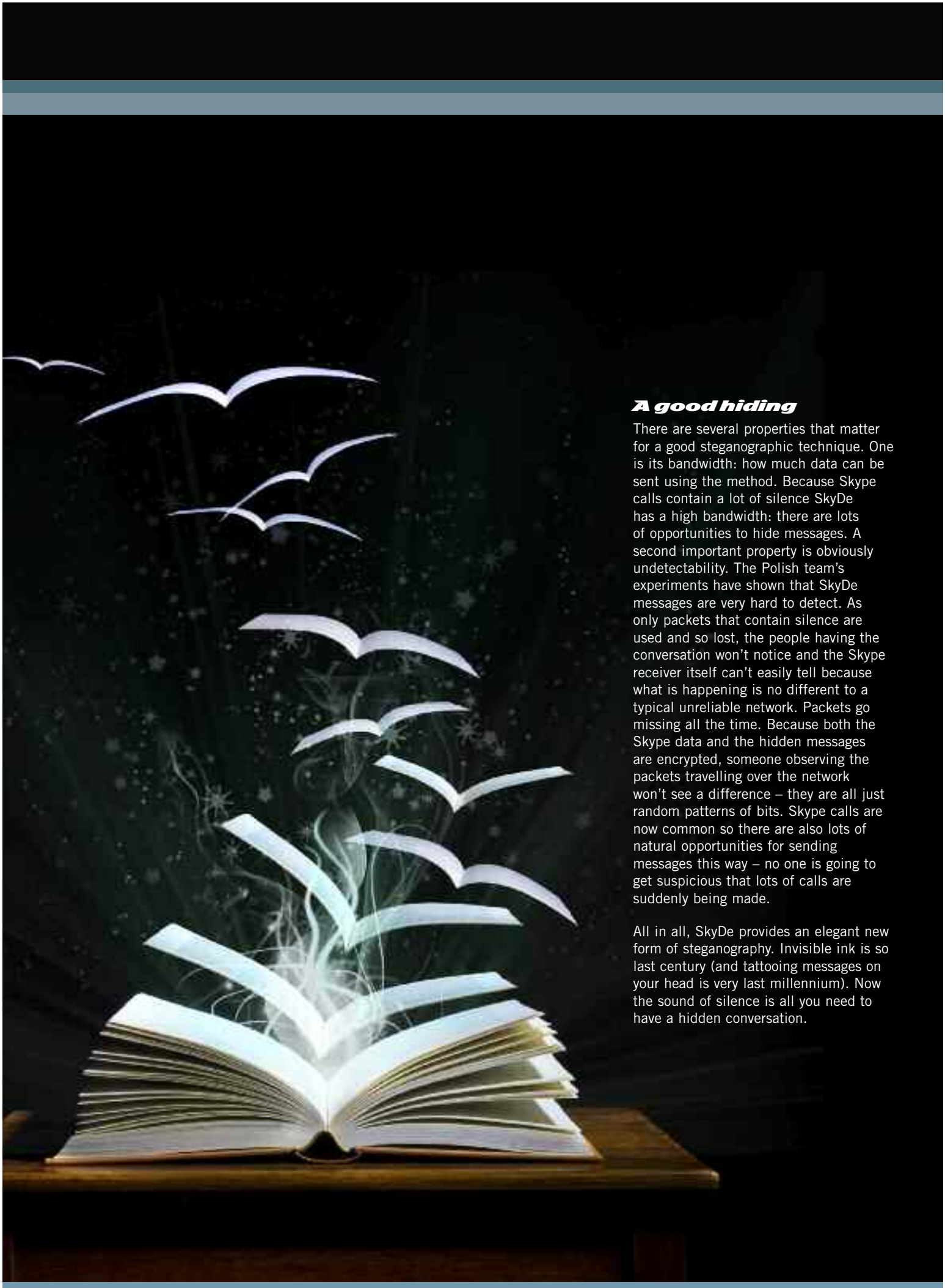
Why? Imagine you run a crack team of commandos who have to reach a target in enemy territory to blow it up – a stately home where all the enemy's generals are having a party. If all the commandos travel together in one army truck and something goes wrong along the way, probably no one will make it. The mission would be a disaster. If, on the other hand, the commandos each travel separately and meet once they arrive, the mission is much more likely to be successful. If a few are killed on the way the rest can still complete the mission.

Who'd have thought the sound of silence would be so useful

The same applies to a Skype call. Each packet contains a little bit of the full conversation and each makes its own way to the destination across the Internet. On arriving there, they reform into the full message. To allow this to happen, each packet includes some extra data that says, for example, what conversation it is part of, how big it is and also where it fits in the sequence. If some don't make it then the rest of the conversation can still be put back together without them. As long as not too much is missing, no one will notice.

The sound of silence

Skype does something special with its packets. The size of the packets changes depending on how much data needs to be transmitted. When someone is talking, each packet they send carries a lot of information. When that person is listening Skype sends shorter packets from their end, because they are only transmitting silence. The Polish team realised they could exploit this for steganography. Their program, SkyDe, intercepts Skype packets looking for short ones. When SkyDe finds those short packets, they are replaced with packets holding the data from the covert message. At the destination another copy of SkyDe intercepts them, extracts the hidden message and passes it on to the intended recipient. As far as Skype is concerned some packets just never arrive.



A good hiding

There are several properties that matter for a good steganographic technique. One is its bandwidth: how much data can be sent using the method. Because Skype calls contain a lot of silence SkyDe has a high bandwidth: there are lots of opportunities to hide messages. A second important property is obviously undetectability. The Polish team's experiments have shown that SkyDe messages are very hard to detect. As only packets that contain silence are used and so lost, the people having the conversation won't notice and the Skype receiver itself can't easily tell because what is happening is no different to a typical unreliable network. Packets go missing all the time. Because both the Skype data and the hidden messages are encrypted, someone observing the packets travelling over the network won't see a difference – they are all just random patterns of bits. Skype calls are now common so there are also lots of natural opportunities for sending messages this way – no one is going to get suspicious that lots of calls are suddenly being made.

All in all, SkyDe provides an elegant new form of steganography. Invisible ink is so last century (and tattooing messages on your head is very last millennium). Now the sound of silence is all you need to have a hidden conversation.