unnecessary place; you also cannot smoke where it is not supposed to. It is not only because of the culture of the city. Any of your offenses will be recorded by one of the millions of surveillance cameras installed on the streets of this beautiful city. Moreover, last year a system of sensors was introduced here, which allow tracking the movements of each person in the city, the activity of the residents to count the average density of the crowd. This process is monitored by several private companies selected by the state, but everyone says that the system can be trusted. But what will happen if all this data will be in the wrong hands?

Let's move to the project, which is almost not heard. The sensors do not react to your fingerprints or even to your face, like the newest iPhone. They react to human DNA. The main reason of this development is safety. Imagine, that at the time of detection of your offender, all inputs and outputs will automatically be closed for him; he will simply be detained and punished. Moreover, payment for something using DNA will be also possible. All you need is to touch the sensor. Thus, all criminality in the world can be reduced practically to zero. But the question arises: what if this data falls into the wrong hands?

Although we know well that in our world there is nothing permanent and perfect. Imagine that you simply lose all money from your account. Or, that someone knows absolutely everything about you: starting from a favorite kind of flakes and ending with a personal life. However, information leakage is not the only problem of such systems. Much greater problems are processing and storage of all these data streams. Imagine that in the same Singapore there are 2 cameras for one person (as average). This is about 11 million cameras, the information from which you need to store. For all this, there are simply huge servers created. They perform thousands of operations per second. It is not known what will happen then, but even with the current development of technologies, we will not be able to store the amount of data from all these sensors that will be needed to create a network tied to DNA. Also, all these cameras and sensors require a source of energy. For example, one standard camera consumes 3 watts, then multiply by 11 million and the numbers will shock you. For modern scales this may be a bit. But just think how many resources are required to produce this energy. And the last problem is just the creation of such sensors. This is a rather expensive process. But in fact, all this money will pay off the possibility to control people.

It seems to us that all these systems may become our fast future. Another question, how quickly will people invent the technologies that allow all these things to be done? And that we still choose: personal life or illusory security.

Scientific supervisor: Babii H.V.,
Senior Lecturer

UDC 004.056.55 (043.2)

Ivanova O.A.
National Aviation University, Kyiv

PRACTICAL APPLICATION OF STEGANOGRAPHY

Steganography is the science of hidden data transmission. It is a combination of methods and tools for their implementation, which make it possible to hide the fact that information exists in one or another environment.

Modern conditions for the development of computer technology and information technology put forward certain requirements for the preservation of confidential information. The most common means of protecting are the usage of cryptographic methods. However, their use with the transport of storage media, or transmission in local networks and the Internet are not always possible. In such cases steganographic methods become relevant.

The principle of steganography is the hiding of one mass of information in the other which has been widely used. Computer files (images, sound and video files, etc.) have areas in which it is possible to record hidden information.

Today, steganography technologies are actively used to solve the following main tasks:

- protecting confidential information from unauthorized access;
- copyright protection for certain types of intellectual property;
- overcoming systems for monitoring and managing network resources;
- camouflage software;
- creating hidden channels of information leakage from the legitimate user.

The use of steganographic system is the most effective for solving the problem of protecting confidential information. For example, by replacing the lower digits in bytes, it is possibly to hide messages in photos, videos and audio containers and, the changes will not be obvious to the user. The main requirement for the container is its size, which is several times larger than the size of the embedded data.

In addition to stealthy messaging, steganography is one of the most promising directions for authenticating and labeling copyrighted products in order to protect copyrights of digital objects from pirated copying. Computer graphics, audio products, literary works (including programs) are marked with a special label that remain invisible to the eye, but is recognized by special software. The label contains hidden information that confirms authorship. As to the implemented information, data can be used about the author, the date and place of creation of the product, the numbers of documents confirming authorship, the priority date, etc. The basic requirements for digital watermarks are reliability and resistance to distortion.

Quite often steganography methods are used for camouflaging software. Cases where the use of the programs by unregistered users are undesirable, it can be camouflaged as a standard universal software products (for example, text editors) or hidden in multimedia files (for example, in the sound of computer games).

Like any other tools, steganographic methods require careful treatment, as they can be used both for protection and for illegal purposes. Recently steganography has been used in the following malicious programs and cyber espionage:

- Microcin (AKA six little monkeys);
- NetTraveler;
- Zberp;
- Enfal (its new loader called Zero.T);
- Shamoon;
- KinS;
- ZeusVM;
- Triton (Fibbit).

Finally, the steganographic approach is used to create a hidden channel for leakage of sensitive information from authorized users.

Concerning widespread use of steganography, progress in this area can fundamentally change existing approaches to the problem of information protection.

Scientific supervisor: Balatska N.I.,
PhD, Senior Lecturer

UDC 629.76/.78:001.12/.18 (043.2)

Ivliev V.O.
National Aviation University, Kyiv

SPACE X'S ROCKET CONCEPTS – STEP FORWARD IN AERONAUTICAL ENGINEERING

Some say, that in Space X wage per year is not high comparing with other aerospace companies and the president of the company Gwynn Shotwell confirmed this rumor, but still, people prefer this job instead of the rest of the options. Let's try to find out the reason along with a story of the success of this truly legendary company.

In 2002, someone, named Elon Musk created the company, with lots of perspectives and ambitious planes about human on the Red Planet – Mars. Who might have thought, that in 2018, the SpaceX company would launch the spacecraft with the biggest number of engines ever made. But still, success did not always accompany the SpaceX.

In 2006 they initiated a launch of their 1st rocket – Falcon 1, which ended with failure. This result only gave further motivation for development. In the meantime, NASA monitors the results of all SpaceX's researches concerning engines and rocket concepts. In 2008 the 1st successful launch of the Falcon with payload delivery to the orbit was performed. It was one of the first big steps for the company. The same year NASA signs a profitable contract with SpaceX within Commercial Resupply Services for supplying the International Space Station. It provides such important thing as financing.

Engines used in these launches were originally made by SpaceX engineers and called "Merlin". Basically, it's a simple liquid propellant engine, with kerosene and liquid oxygen as a working body, but it has one important feature – this engine, and driving unit itself can be used multiple times. We'll return to this later. There're lots of configurations of this engine, depending on the purpose and kind of rocket. Also, for more ambitious planes, SpaceX is working on a brand new type of the engine – they call it "Raptor".The 1st testing of this engine ended successfully. Practically, this beast can develop thrust equal to 1 Meganewton. If they succeed, "Raptor" will become the most powerful rocket engine ever made.

Falcon Heavy –a rocket, with the biggest number of engines ever made was launched on 6th of February, this year. Whole world had crossed their fingers for success. The cost of launching is worth about 90 million dollars. The next rocket, which may be compared with the Falcon Heavy by payload efficiency is Delta Heavy IV (owner – United Launch Alliance) – 350 million dollars. The rocket consists of 3 Falcon9 1st stages, which make up 27 engines. Tesla Roadster, Elon Musk's own car of was used as a test payload. In case of a failure of some system, the rocket would crash into the ocean, or with the worst scenario – explode at the launching pad.

The aim of the SpaceX – is to settle the humans on Mars. Current technologies do not allow people to realize the flight today. During a space flight the human loses 2% of his bones mass per month. Also, calf muscles lose up to 13% of the volume during 6 months.