Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):28-38
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

PERSPECTIVE STEGANOGRAPHIC SOLUTIONS AND THEIR APPLICATION

S. Toliupa, A. Romanova

Taras Shevchenko National University of Kyiv, the Faculty of Information Technology, Information Security Management

ABSTRACT

Nowadays, as the role of information technologies in our lives is growing and growing with every passing minute, there is no question about the fact that information security measures are an issue of the highest importance. It would not be wrong to say that there is no 'zero-day threat' anymore; it is more like 'a threat of a zero second'. Every modern technology automatically causes several new vulnerabilities and threats to come to existence, which, on its part, makes security specialists work their best to counter such efforts. Thus, there are quite a lot of information security solutions at hand already.

Cryptography is doubtlessly one of the most effective, developed and approbated methods to be used when it comes to the protection of information resources. Nevertheless, it might be more effective to hide the communication channel itself instead of making unreadable the information within it. The practice of concealing data within text- or media-file is called *steganography* and has its roots deep in the history of the humankind.

A considerable number of steganographic methods are well-known and implemented in various steganosystems and applications. There are some methods of information concealment, though, that receive the attention not so much. The reasons of such lack of popularity can differ depending on specific solutions: their complexity for one, low cost-effectiveness of their realization for another. In any instance, they are either poorly described or are not widely used regardless of their perspectiveness.

The purpose of this article is to conduct an analysis and suggest possible practical use of steganographic solutions that are known and can be applied to a variety of information security systems, and yet lack either theoretical basis or practical application.

KEYWORDS: Stenography, cryptography, applications, security

STEGANOGRAPHY AS A MEANS OF HIDING INFORMATION

Basic terminology

Steganography is an art and science of storing and transferring secret messages within covert channels that are based on and created inside open channels in such a way that the cover data is perceived as if not having any embedded messages for its unplanned recipients. The general approaches are:

- Full concealment of the covert communication channel;
- Creating difficulties for detection, retrieval and modification of hidden messages conveyed within open data;

- Secret message camouflage inside the protocol [1, 2].

The main concepts are:

- Container *b* (also: carrier) is open data used to conceal secret information;
- Message *m* (also: payload) is secret information to be concealed;
- Key *k* is secret information that is known only to a legitimate user and defines a specific concealment algorithm;
- Empty container *c* (also: unmodified container) is a container devoid of any secret data; it is a sequence of l_c-long elements;
- Modified container *s* (also: package, steganogram) is the one that contains a secret message;
- Steganographic algorithm means two transforms, a direct $F: M \times B \times K \rightarrow B$ and an inverse one $F^{-1}: B \times K \rightarrow M$;
- Steganographic system (also: steganosystem) is a totality of messages, secret keys, containers and transforms that connect them [1, 3].

Steganography uses containers of different nature; the choice depends on the specific task. In case a digital sound file is used as a container the length of elements will be defined as the number of counts per time unit. If the container is a digital image file, then the sequence of elements will be obtained by vectorizing the image (transforming the array of pixels into a vector) [3].

Most steganography methods are based on two key principles:

- Human senses cannot distinguish slight changes in colour, shape and sound perception;
- Consequently, there are files that do not demand absolute preciseness and therefore can be modified without losing their functional value.

As a result, said methods imply allocation of insignificant fragments of the container and replacement of the information within them with information that needs to be hidden.

Finally, the process of encoded steganogram detection is called *steganoanalysis*.

The interest in steganographic solutions is undeniable. They may be used as an alternative for the cryptographic means of hiding information, in many cases more effectively. Furthermore, they serve as a powerful tool for digital and non-digital watermarking and authentication control. Finally, while the use of cryptosystems is legally regulated and limited to some point, there is no such restrictions in designing and distributing steganosystems in any country.

CLASSIFICATION OF STEGANOGRAPHIC METHODS

By the method of selecting a container one can distinguish non-alternative, selective and constructive methods of steganography [3].

Non-alternative methods imply the choice of the first possible container made in order to conceal a message. Selective methods imply that a covert message has to reproduce special statistical characteristics of the container noise. In constructive methods a container is generated by the steganosystem itself.

By the way of access to the secret information there are methods for stream and fixed containers.

By the type of organization there are methods for systematic and non-systematic containers. In the first ones bits of noise and of the container itself can be distinguished. In the latter ones they are impossible to specify.

By the concealment principle there are two main classes: methods of direct substitution and spectral methods. The first use container redundancy and replace the insignificant areas of the container with the bits of a secret message, while the second hide the data using the spectral representation of the elements in the environment where the concealed data is embedded (for example, coefficients of the arrays of Fourier transforms).

By purpose one can distinguish the methods for the data secret transmission or storage and methods for concealing data in digital objects in terms of copyright protection.
A special group is represented by methods that use characteristic file format properties:

- Reserved fields, which are usually filled with zeros and are not taken into account by the program;
- Special data formatting (the shift of words, sentences, paragraphs or selecting specific positions of characters);
- Erasing file identifier captions etc [3].

Popular steganographic solutions

In this section the brief overview of widely used steganographic solutions is presented.
Mostly, steganography uses the data concealment within digital images and audio files, less so video files and text. Electronic communications may also include hiding data inside of a transport layer (program or protocol) [4]. Digital media files are extremely suitable for steganography tasks, first and foremost due to their large size. The subtle changes in their structure are highly unlikely to be noticed by the unintended user.
Starting with non-digital methods, physical steganography technics cannot be omitted. They have been developing for centuries and include, for example, blinking one's eyes in Morse code to spell a secret message [5].
Another example is adding tiny yellow dots to each page while printing a document. They are not detectable by the bare eye and contain the model, serial number and timestamps. This information cannot be obtained from a computer file and is embedded in a printout using dot-matrix code. Such a technology is used by many brand color laser printers, such as Xerox and Hewlett-Packard for traceability reasons [6].

Methods of embedding data within an image container [2, 3]:

- Least Significant Bit method (LSB) (Sequential Insertion) is the most popular steganographic method. The least siginficant bit of each pixel is in fact a noise. If it is changed, the difference in the image will not be noticed by a human eye. Thus, these bits can be replaced with the bits of a secret message.
- LSB Psuedo Random Insertion. In contrast to the previous method, in which every changed data bit follows the next, this method uses pseudo random distribution of the secret message bits through the container. Thus, the interval between two bits is pseudo-randomly defined, which complicates both visual and statistical attacks, as well as extraction of all the hidden bits.
- LSB Pseudo Random Permutation. Not only the least significant bits are chosen pseudo randomly, but also the bits of a secret message are uniformly distributed through the container in a pseudo random sequence.
- Block hiding method. The container is split into disjoint blocks; for each of them a parity bit is calculated. One secret bit is concealed within one block. If the parity bit does not equal the respective secret bit, then one of the LSB in the block is inverted, so that the parity and the secret bits are the same.
- Palette permutation. Any colour palette consists of pairs of indexes. Each pixel of the image corresponds to a certain index in the table. The sequence of colours in the palette is not important, so it is possible to conceal a covert message by changing this sequence.
- Image Quantization. Interpixel correlation can be defined by a function Θ. We can calculate the difference ε_I between adjacent pixels c_i and c_{i+1} (or c_{i-1} and c_i) and set it as a function parameter: $\Delta_i = \Theta(c_i - c_{i+1})$, where Δ_I is a discrete approximation of the difference of signals $c_i - c_{i+1}$. As Δ_I is an integer and the difference $c_i - c_{i+1}$ is a real number, quantization errors $\delta_i = \Delta_i - \varepsilon_i$ occur. The information concealment is carried out by correcting the difference signal Δ_i.

- Kutter-Jordan-Bossen method. A human eye is the least sensitive to the blue colour. The method is based on the embedment of the secret message within the blue channel.
- Koch-Zhao (Relative DCT (Discrete Cosine Transform) values change method). Initial image is split into blocks of 8x8 pixels. As the result of applying DCT to every block a table of DCT coefficients is formed. Every secret bit is hidden in a separate block. Frequencies quantization causes some rate of distortion in the image, which is still not noticeable by the human eye.
- Benham-Memon-Yeo-Yeung method. Optimized version of the previous method. Firstly, only the most suitable blocks are used. Secondly, three DCT coefficients are selected instead of two, which decreases destortion in the container.
- Hsu-Wu method is an algorithm of a binary digital watermark embedment. The value of its pixels can only be “0” or “1”, so the direct observation of such an image is impossible, as “0” and ”1” intensities correspond with the black colour. The watermark can be created black-and-white and then the whole array can be divided by 255 to replace the intensity of white pixels with “1”.
- Fridrich method implies a cascade embedment in low- and high-frequency DCT coefficients.
- Spread-Spectrum method consits of three possible variants:
  - The used frequency band is much wider than needed. Signal/noise ratio is then quite low, which makes the signal unlikely detectable;
  - Spectrum is expanded by using a special independed (also: code) signal. The signal energy is distributed through all frequency bands, which makes the signal noise immune;
  - Restoration of the initial information is carried out by comparing the received signal and a synchronized copy of the code signal.
- Embedding pictures within video-files [5].

Audio steganography [3]:

- LSB-method for audio-files is the same as for images, but working with the audio-file format. It causes considerable destortions in the container.
- Phase coding method implies the substitution of the initial sound segment phase with the reference phase, which is the data to be concealed. Phases of adjacent segments are agreed to preserve the difference phase between them.
- Echo-signal use. Data is embedded in the container by injecting an echo-signal in it. Three echo-signal parameters are changed: initial amplitude, attenuation and shear rate. The echo-signal is perceived only as an additional resonance [7].

Linguistic steganography [3]:

- Random interval methods. Changing the number of spaces in the end of the text string does not cause significant changes in the meaning of the sentence. What is more, an average reader is unlikely to detect insignificant space modifications:
  - Changing the interval between sentences. One or two additional spaces are added after the sentence. This method requires that a file of a considerable size is used to embed a small number of secret bits in. In addition, most text editors automatically change redundant punctuation and spaces, which may ruin the concealed data;
  - Changing the number of spaces in the end of text lines. Spaces are added according to the secret bit to be hidden. Two spaces encode one bit a line, four spaces – two bits etcetera. Compared to the previous method, the bigger amount of information can be embedded.
  - Changing the number of spaces between words in a flattened text. When the text is width aligned, spaces between words are not of the same length and some of them can be used to hide data.
- Making the text of the same colour as the background [5];
- Using similarly looking Unicode and ASCII characters [4, 8];

- Using non-printable Unicode characters [8];
- Creating a pattern of deliberate errors and/or marked corrections [4].

Format steganography:

- BMP:

o Appending data to the end of the file implies an artificial expansion of the final image sector;

o Palette permutation.

- JPEG:

o Appending data to the end of the file. Using the standart sysem of markers to append information after them, which will cause a program to ignore the secret message;

o Using collateral data. Data is preliminarily camouflaged as collateral information (Scan Index, Title Index etc), which is mostly ignored by programs, and then injected after specific identifiers.

o Using commentary markers is similar to the previous method, but works with commentary fields.

Some other methods:

- Converting a file so that it has the statistical characteristics of another one [4];
- Injection of delays to packets that are sent over the netwotk from the keyboard [5];
- Blog-steganography. Secret data is added as commentary pin boards on social networks[5].

Finally, there are different software applications that use the methods of steganographic concealment mentioned above:

- Using LSB-method: OutGuess, JSTEG, JPHS, Hide-and-Seek, Steganos, Steghide, DC-Stegano;
- Using the palette permutation: Gifshuffle;
- JPEG format: OutGuess, JSTEG, JPHS;
- GIF format: Gifshuffle, Hide-and-Seek;
- BMP format: Steganos, Steghide;
- PCX format: DC-Stegano;
- LSB-method in audio-files: Invisible secrets, Hide4PGP, Steghide, StegoWav, Steghan, S-Tools;
- Using parity of quantization of frequency coefficients: MP3Stego;
- Using incorrect frames in a compressed stream: UnderMP3Cover [9].

Perspective steganographic solutions and their application

Internet of Things and cyber-physical systems

A cyber-physical system is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. Examples of CPS are autonomous automobile systems, medical monitoring, smart grids, automatic pilot avionics etc [10].

The Internet of Things (IoT) is the network of physical devices, vehicles and other items embedded with electronics, sensors, software and network connectivity, which enable them to collect and exchange data. It is more or less an instance of a class of cyber-physical systems [11]. The network steganography uses communication protocols' control elements and their functionality to hide information inside [12]. The modifications can be carried out either over a single network protocol (applied to the Protocol Data Unit, the time relations between PDUs or both) or to several protocols at the same time (inter-protocol steganography). Such network steganography methods can be applied to the systems mentioned above, too. The IoT is believed to be a phenomenon that will expand its influence greatly within the next few years. As a perspective network instance it requires thorough attention of steganography specialists.

Information circulates within it the same or the fairly similar way as in any other system. Thus, optimal and the most suitable methods of hiding data in communication protocols should be developed specifically for the IoT.
What is more, as the items within the IoT possess a vast variety of sensors and software, they can be used to conceal data in. For example, covert messages can be stored in unused registers of the CPS/IoT components or in the states of their actuators [12].

THE USE OF STREAM CONTAINERS

As mentioned above, by the type of access to the data one can distinguish fixed and stream containers [3]. All the methods mentioned in Chapter 2.3 use the first ones to conceal information in. Such a container is a constant pre-defined sequence of bits that are displayed before a steganographer all at once. To the contrary, a *stream container* is a sequence of bits that are continuously changing, as in a phone conversation. A message is embedded in real time so that the final size of the container is never known beforehand. The intervals between the embedded bits are generated by a pseudorandom sequence (PRS) generator and uniformly distributed between readouts [3].
There is hardly a couple of scientific works devoted to this type of steganography, let alone examples of its real-life practical implementation. Despite any reasons, it can be successfully applied as an efficient means of information security. There is a number of solutions for encrypted secure real-time communication. However, what if we could, for example, make a confidential phone conversation not only indecipherable but also seem to be an innocent chat? A stenographic telephone set-top box could be a solution. The same concerns video-conferences. An extraneous observer would only see an average conversation not having any access to the real audio, video or any other embedded data.
The unpopularity of the stream-container steganography can be explained by defining major issues concerning its use. First and foremost, it is never known whether the size of the container will be enough to conceal the whole message as the length of the first (and likely of the latter, as well) is undefined. The same property creates and advantage as one carrier file can be capacious enough to contain several messages. In any case, the secret data has to be somehow synchronized with the container, thus one of the biggest questions is how to define the beginning and the end of the embedded sequence within the container. The problem becomes more serious concerning video communication. The solution would be of extreme complexity, as we would need to synchronize the image-image stream (both open and covert), the sound-sound stream and image and sound respectively.
The solution may lie in using special built-in libraries. They would consist of structured groups of words of the same length, which would in ideal case possess pronunciation similarities. Such groups should then be grouped in semantic dictionaries, so that they would form simple, but logically and semantically structured sentences. The linguistic means for this are well-developed and are similar to those of forming synonymic dictionaries and machine translation applications. The words and sentences could then be synchronized with the container using synchronization bits, package headers and/or other means of dividing encapsulated data; the covert message can be embedded after them and be synchronized using the initial properties of the container.
The possible situations with video communication would be more complex. If only the content of a given conversation is confidential, then the issue is just to steganographically encrypt the sound and synchronize it with the real video image. On the other hand, if the identities of conversation participants are also a secret, then other methods should be provided. It is not necessary for a steganographic solution to be all-purpose. It is possible to design a system consisting of a cryptographic and a steganographic modules and providing different scenarios according to the situation.

The biggest remaining problem is a significant delay which is unacceptable in real-time conversations. Then again, there are numerous solutions in cryptography in this field, that can be adapted to the task.

SEMANTIC AND SYNTACTIC METHODS

These two classes of methods belong to steganography with text containers. Instead of using digital format features, they work with the language itself. It is an advantage in comparison to the first type. As an average reader may not be aware of the covert message existing in an open text, a text editor may automatically change the number of spaces or conduct other actions that would ruin embedded data [3]. In fact, any reformatting will lead to the same result.

Syntactic and semantic methods, though, do not use the presentation of text, but work with the text itself. The first type uses the fact that in most languages there are some optional rules of punctuation and grammar forms. Any given language sticks to specific rules, but is still not so solid of a structure, which presents a great number of linguistic possibilities. For example, in the Ukrainian language a colon and a dash can replace each other in some cases. This can be used to encode bit of secret message: “0” for one punctuation mark and “1” for the other one. A more complicated method could be using grammatical similarities in different sentence constructions, such as changing the sequence of some words.

An example of semantic steganography is using the table of synonyms to encode the secret bits. If there are two of them, say, ‘however’ and ‘but’, then again one of them can mean “0” and the other “1”. If there are more synonyms, possibly context ones, then 4 words can encode 2 bits, 6 words 3 bits of information etcetera. The average data transfer speed when using these methods is several bits per kilobyte [3].

The main problems with such linguistic methods are obvious. First of all, they are very language-dependent. Secondly, they require large amounts of initial text as a container, which is not exactly effective. Finally, even if some punctuation rules are ambiguous, their deliberate and controversial usage can be detected by a censor/editor.

It could be wise to suggest the usage of more complex methods of language-based steganography. Every language can be analyzed to create special tables of syntactic correspondence. For example, for the English language and other Germanic languages the use of active and passive voice, as well as of complex object and complex subject is optional. Sentences can be easily and naturally transformed using equivalent constructions, that most likely will not raise suspicion. The advantages of such solution are numerous. One of them is high resistance to various attacks (they are here similar to one-time pads). Another is that the concealment capacity is much higher than that of basic semantic methods. The only question is an algorithm of selecting initial text material. It is likely the best option is to create special libraries of texts, sorted by the topic. This way many fields of interest may be covered so that the covert message is not detected.

A creation of a multi-purpose linguistic steganography complex is suggested. It will doubtlessly require linguistic work of high quality and profoundness. An optimal approach is to be found to, if possible, reduce the language-dependency of each solution. In other case, such an application will have to be designed according to a separate language or, at least, a group of languages with the same paradigm. Thus, the task at hand is to group the languages within each family by the similar tendencies in grammar usage. The next step is to create tables of correspondence for grammatical constructions and stylistic expressions that can be interchanged. Finally, text material libraries are required to provide unobtrusive containers with as much options described in the tables as possible.

STEGANOANALYSIS

Methodological base of steganographic analysis also require some further enhancement:

1) Development of probabilistic-statistical methods of recognition, application of artificial intelligence elements to estimate the reliability of steganographic transforms and to design detectors (filters) for analyzing information streams in order to detect and overturn hidden communication channels. In this case, the verification of the hidden information presence is specified by a certain estimate using statistical criteria (sequential correlation, entropy of the image, dispersion of the LSB, etc.). Solutions developed for this purpose should not only provide a low rate of error in the recognition of incoming messages (especially when using encryption of the data), but also be able to detect messages embedded using different steganographic methods. Compared to the applications designed to steganographically conceal data, the quantity and quality of steganoanalytical systems are rather low.

2) Analysis of specific steganographic software solutions to restore the concealment algorithms and work out the optimal analysis method. The main difficulty is again the large number of specific algorithms that demand individual approach as well as significant amount of computations.

3) Development of the technology of automized active and malicious attacks to make the anticipated steganogram irreducibly distorted in order to provoke its re-transmission within another container, which would confirm the existence of a covert channel [3].

BIOCHEMICAL STEGANOGRAPHY

Most modern steganographic systems use only digital containers, such as files of various nature, binary sequences etc [9]. However, there are other fields of interest for steganography, as the environment can provide a considerable variety of non-digital containers.

We are surrounded by billions of organisms, every cell of which contain DNA-molecules. They are the central repository of information in the cell [13]. Biological computing and quantum computing are believed to be the two most promising technologies under development right now [14]. And as cryptography now mostly works with factorization problems, which makes the messages subjects to attack by quantum computers, biochemistry presents the whole new sphere of potential information security solutions.

DNA-steganography is a process of camouflaging a DNA-encoded message within the enourmous complexity of genomic DNAs [13]. Due to the DNA-code variability among different species, an organism, selected at hazard, possesses random DNA-code. Such a characteristic makes these molecules potentially good containers. Another doubtless advantage is their tiny size, as huge amounts of information can be encoded within a container that cannot even be seen by a human eye without proper amplification. DNA is also a quite solid structure and one highly resistant to possible biochemical attacks.

Nevertheless, despite obvious perspectives of using DNA as a means of biochemical steganography, most of the attention has been received by DNA-cryptography so far.

A DNA-molecule is a sequence of four nucleotides – Adenine (A), Cytosine (C), Guanine (G) and Thymine (T), that are grouped in triplexes, so called *codones*, and form two anti-parallel strands [9, 14]. Complementary DNA strands can self-assemble by forming hydrogen bonds between bases (base pairing) of each strand specifically with A bonding only to T and G only bonding to C [10]. Four different bases mean 4^n possible different n-meres that encode genetic information through a number of aminoacids [6, 8]. Another macromolecule to be potentially used is RNA. It is similar to a DNA-molecule with an exception that the base structure is a different 5-atom sugar – ribose, and uracil (U) corresponds to thymine [9].

So, how do we encode information within a biomolecular structure? A message can be encrypted in a DNA strand, every symbol being encoded by a codon defined in the specially designed table (the technic resembles the use of one-time-pads). For example, ‘A’ may be encoded by a CGA

sequence, ‘B’ by CCA and so on [14]. The secret message is then presented as a sequence of codones. Some of the aminoacids are presented: alanine – GCT, GCC, GCA, GCG; asparagine – GAT, GAC; fenilalanine – TTT, TTC [9].

Then the strand is flanked by polymerase chain reaction (PCR) primer sequences and hidden by mixing it within many other additional “distracter” DNA strands [10, 9]. Polymerase Chain Reaction (PCR) is a process, during which PCR primers become complimentary to the F and R primer “keys” in Secret Message DNA [13]. They are then hidden in a microdot [14]. Knowing the secret key and the primer sequences, a user can extract the strand using known DNA separation methods (hybridization with the complements of the “secret key” strands might be placed in solid support on magnetic beads or on a prepared surface; may be combined with amplification steps and/or PCR [15]) and read the message.

A problem with such approach is that the probability profile of aminoacids in nature is not the same as that of a secret message [9]. The secret “tags” have to be indistinguishable from “distracter” DNA strands and the entropy has to be as in any DNA-molecule – between 1.2 and 2 [15]. This creates the need to use models of real DNA-molecules along with some other solutions. One of the enhancement technics suggested recently is the use of *sequencing* (determining the sequence of nucleotides in a DNA-fragment). There are a lot of sequenced genomes provided in open arrays already. Some of them are 55 genomes of bacteries, a yeast genome and those of other standart laboratory objects [6]. Another techinc is to construct the “distracter” strands so that their distribution mimics the plaintext source distribution. One of the easiest possible ways to do so is to synthesize a DNA-molecule that depends only on the plaintext and the secret key [9, 15]. The compression of the plaintext is also possible. If the resulting distribution of the plaintext approximates a universal distribution, then a random distracter sequence may suffice to provide security needed [15]. The use of a substitute random combination of sequenced genomes (from exotic organisms, for example) may be an enhancement solution, as well [13]

There is a work [16] devoted to the use of run-length encoding (RLE) systems in biochemical steganography, though it is stated, that their application in practice still provides more questiones than answers.

Given everything stated above, any possible attack on a DNA-based steganographihc system would not be successful if it is purely computational [13]. The ways of resisting biochemical attacks, though, are an important question to pay attention to in the future development of DNA-steganography.

Current DNA-steganography technology is still in a period of laboratory exploration and focused on experiments [14]. A possible explanation of the lack of expected activity in the field is that it is a multidisciplinary area which demands knowledge in both biology and cryptography and so requires researchers from both areas to work in a new cooperative way [14]. Possible spheres to implement these technics in are negotiable instrument anti-forgery, personnel identity and access control, anti-theft marking and product authentication [17]. All of them are instruments of securing business profit and are thus attractive for service and production. Only a few examples of using DNA-steganography as a sort of watermark are know. In 2000, during the Olympics in Sydney the Australian Olympic Committee used the DNA based tracking technology to protect Sydney Olympic licensed merchandise from counterfeiting [17].

CONCLUSION

A variety of steganographic solutions was analyzed. Among them such methods were selected that are not either widely used in software applications or lack attention in general. Nevertheless, their perspective usage was discussed. Taking into account all the fact mentioned above, the next directions of development of steganography are suggested:

- Steganography in cyber-physical systems and the Internet of Things in particular;
- The use of stream containers;
- Semantic and syntactic methods;
- Some enhancement in steganoanalysis technics;
- Biochemical steganography practical application.

Information is surely becoming an asset of the highest value. Seeing as the cyberspace is more of a battlefield for different forces continuously confronting each other, it is obvious that information security sphere requires the best solutions possible. Steganography has proven to be an effective means of secret data concealment ensured with centuries of practical use. And, just as any other science, it is in the state of constant development. Being aware of perspective ways to use its methods for our cause, we get access to numerous up-to-date possibilities of providing information security of the highest level.

REFERENCES

1. Е.Л. ЗОРИН, Н.В. ЧИЧВАРИН: Стеганография в САПР. Учебное пособие. МГТУ им. Н.Э. Баумана, Москва (pdf).
2. ALEXANDRE MIGUEL FERREIRA: An Overview on Hiding and Detecting Stego-data in Video Streams. University of Amsterdam, System & Network Engineering – Research Project II, March 23 2015.
3. KONAKHOVICH G. F., PUZYRENKO A. YU.: Computer steganography. Theory and practice with Mathcad (Rus). MK-Press Kyiv, Ukraine 2006.
4. FRIDRICH, JESSICA, M. GOLJAN, D. SOUKAL: Searching for the Stego Key. Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 2004 (pdf): http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf.
5. CHRISTOPHER LEAGUE: An overview of digital steganography, particularly within images, for the computationally curious. Long Island University 2015: https://www.youtube.com/watch?v=-7FBPgQDX5o.
6. Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and When You Made Your Print. Electronic Frontier Foundation October 2005: https://www.eff.org/press/archives/2005/10/16.
7. Echo Data Hiding (html): http://www.slidefinder.net/a/audio_steganography_echo_data_hiding/ 24367218
8. AKBAS E. ALI: A New Text Steganography Method by Using Non-Printing Unicode Characters. Eng& Tech. Journal, 28 (1) 2010 (pdf): http://www.uotechnology.edu.iq/tec_magaz/volume282010/No.1.2010-/researches/Text%287%29.pdf.
9. А.В. АГРАНОВСКИЙ, А.В. БАЛАКИН, В.Г. ГРИБУНИН, С.А. САПОЖНИКОВ: Стеганография, цифровые водяные знаки и стеганоанализ. Москва: Вузовская книга 2009.
10. Cyber-Physical system: https://en.wikipedia.org/wiki/Cyber-physical_system.
11. Internet of Things: https://en.wikipedia.org/wiki/Internet_of_things.
12. STEVEN J. MURDOCH, STEPHEN LEWIS: Embedding Covert Channels into TCP/IP. University of Cambridge, Computer Laboratory (pdf): http://www.cl.cam.ac.uk/users/fsjm217, srl32g/.
13. CARTER BANCROFT, PH.D.: DNA-Based Technologies: Computation, Steganography, Nanotechnology. Talk at Material Science and Engineering, Stony Brook University, April 2011.
14. ADITIT SHARMA: Security and Information Hiding based on DNA Steganography. International Journal of Computer Science and Mobile Computing, Vol. 5, March 2016: www.ijcsmc.com.

15. ASHISH GEHANI, THOMAS H. LABEAN, JOHN H. REIF: DNA-based Cryptography. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 54, 2000 (pdf).
16. TOMONORI KAWANO: Run-length encoding graphic rules, biochemically editable designs and steganographical numeric data embedment for DNA-based cryptographical coding system. Commun Inteqr Biol. March 2013: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3609851/
17. WENDELL M. SMITH: DNA Steganography for Security Marking. 5th World Product and Image Security Convention, PISEC '03, Czech Republic. Technology Transfer Group: http://www.polestarltd.com/ttg/isspeeches/pisec03/index.html