Steganography in Frames of Graphical Animation

L. A. Balagyozyan, R. G. Hakobyan

National Polytechnic University of Armenia, Yerevan, Armenia

Abstract: Information exchanged between two parties is often targeted by a third party. Steganography in images is often used for handling threats, such as, in this case, an attacker suspecting the existence of confidential information. But even in this case, if a pattern is used, e.g., hiding the information in successive or every third pixel, the attacker might discover the pattern, and the following revelation of the secret information will cause no difficulties. To avoid such vulnerabilities, the information is hidden in the frames of graphical animation. In the frames, the positions of the pixels selected to store confidential information in the given work are determined by the values of a mathematical function. These actions will ensure the high secrecy of information.

1 INTRODUCTION

1.1 Cryptography and steganography

In the present time, when information is transferred often and in large volumes, information security and integrity are serious issues.

Data security is especially important for modern large mining enterprises because they often have several divisions in their structure, which can be in different locations (regions, countries, and continents). They might also be associated with partner organizations and have various contract companies. Considering that there is a constant flow of information in large volumes between the company's divisions, partner organizations, and contractors, data confidentiality and integrity for storage, transfer, and administration becomes an important security issue for the company. Special attention is needed to solve these problems.

Data protection has two main approaches:

- Cryptography
- Steganography

Cryptography is a solution for storing information securely. This type of encryption is using data converting technic. Converted data can be readable but does not make any sense, or it can be unreadable at all. For decrypting this type of data, every cryptography encryption has its secret key [1].

On the other hand, steganography is also a solution for secure data storage. But in this case, information remains the same as the original one. This method is storing or "hiding"

information in a secure place. That place can be any file, for example, an image, audio file, text file, etc.

1.2 Advantages and disadvantages of steganography vs cryptography.

The main advantage of choosing steganography over cryptography is that the hidden message does not attract any unnecessary attention to it. It hides the fact that a secret communication is taking place. Whereas in cryptography, no matter how unbreakably the message is encrypted, an attacker will know of its existence. For example, in some countries where encryption is illegal, violations of the law will be incriminated.

Moreover, implementing steganography using video or graphical animation formats can allow a very large amount of data to be hidden in them, as, compared to a steady image, they have a lot of frames.

The only aspect where cryptography is surpassing steganography is that except for supporting Confidentiality and Authentication security principles, it also supports Data integrity and Non-repudiation. But various applications have different conditions and requirements for their data hiding. Some require absolving the invisibility of their data and some may be fine with others knowing about the existence of their secret information. So, depending on the situation, they might need to use either cryptography or steganography.

1.3 General review

Everything around us is information or a medium of information. There are many ways to store information in a digital world. The simplest examples are text files, pictures, and videos.

This work explores graphical pictures in the role of information carriers, their formats, and memory storing features, and offers a secret information encryption method using secret information segmentations to small pieces, GIF format features, secret mathematical functions, and an LSB algorithm. The LSB (Least Significant Bit) method is the method, where the least significant bit of the pixel is replaced with the necessary value.

Various articles were researched, and this method was chosen as no other example was found, where a mathematical function is used to hide information in an image, especially in GIF file frames, which would significantly improve the secrecy of information.

2 GRAPHICAL PICTURES

2.1 Graphical picture types

Every image that can be displayed on a screen (created using a computer or photographed/scanned from the real world) is considered a digital or graphical image.

Graphical pictures are chosen as the carrier because they are easier to transmit over the internet. Graphic images are divided into two main families:

- Raster graphics
- Vector graphics

These two types are fundamentally different and have different uses. Graphical pictures belonging to the vector family consist of points and vectors. This structure allows you to store physically large images in a very small memory area, as only the coordinates and color descriptors for each segment of the image are stored in memory. These types of pictures are not threatened by size changes and do not lose their quality as a result of such a transformation. They are used in large-scale printing by graphic designers, etc.

However, it is inconvenient and unprofitable to have a picture of a forest in a vector format, as each new color segment must be described by a new set of vectors. To solve this problem, there are raster graphical pictures or, as commonly known, pictures that are using pixel structure. Raster images are made up of pixels and store a sequence of colors or a sequence of pixels in the memory. Pixel is a color dot; it can contain one or more colors depending on the type of image. In the RGB color model, a pixel has 3 colors: red, green, and blue. Depending on the picture format, there can be allocated 8 and/or more bits for each color in every pixel. Raster images can express more detail in a picture, but they usually take up more memory space and possibly can lose quality when the physical size of the image is being changed. These types of pictures are used for editing, printing, and showcasing [2].

2.2 Graphical pictures compression

But if all graphical pictures were saved by storing a sequence of pixels in the memory, each picture would have captured thousands of bytes of notes about every pixel. This problem was solved by the image compression algorithms.

Graphic compression occurs with 2 types of images:

- Lossy
- Lossless

Compression algorithms without data loss (lossless compression) allows you to completely recover all pixel data after compression. In the case of lossy compression, it is still possible to recover pixels, but only a fraction of the information that makes the original image will be recovered. As a result, the image caused by the lossy compression takes up less memory space and image recovery uses less computing resources and memory [3].

2.3 Carrier image, carrier image file format

A carrier image is an image that the user is choosing for storing the secret data. In theory that can be any type of image, e.g., JPEG, PNG, GIF, etc. But for this method, the GIF file format was chosen as the carrier image, as it can store several graphical images in one file. The GIF format uses the Lempel-Ziv-Welch (LZW) lossless compression algorithm, which is why it is popular and often used by graphic designers; it is a very common data type for storing graphical animation, very widely used in WEB browsers, and it stores unique color pallets for each frame of the graphical animation [4].

That last ability is very important for this method because when the secret data is hidden in the frame, that frame loses some color depth, and if there was a single pallet for all frames or a combined one, these losses would become visible to the human eye.

2.4 GIF image file format

In GIF format, each color has an 8-bit memory space; thus, each pixel has 24-bit memory space. In case of containing more than one frame, GIF allocates an individual color palette, consisting of 255 colors, for each frame.

But you can have a GIF image with more colors. Such an image can be obtained in a very simple way. If you divide each frame of the GIF image into sections, then each of them will be a new frame. After such a change, you can get a graphic image containing 2295 colors [5].

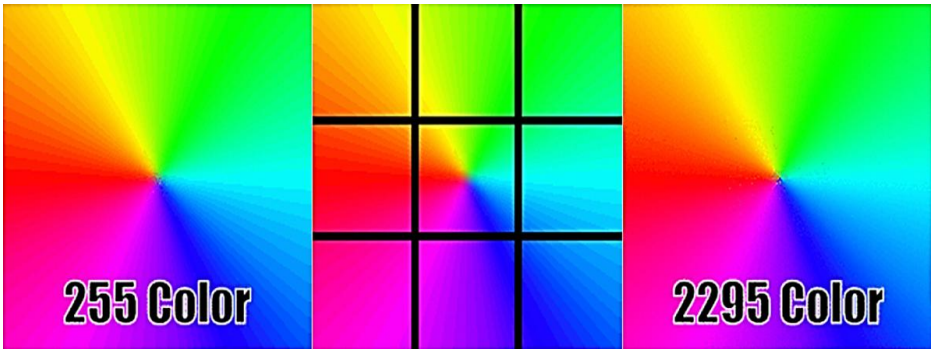

Fig. 1. 2295 color GIF generation example.

2.5 Color model

The RGB (Red Green Blue) color model is an additive color model, where red, green, and blue colors are added in different quantities to create a wide range of colors.

In the RGB color model, color is described by the number of each component, which is described by its value. The color is described by a triad of red, green, and blue components, each of which can be valued from zero to the maximum preset value.If the value of all components is zero, then the resulting color is black, and in the case of maximum values of all components, it is white. RGB core values range from 0 to 255 [6].

This work uses the RGB color model, as it is intended to be displayed on TVs and monitors.

3 HOW THE PROGRAM WORKS

3.1 Preparations

The encryption program receives a mathematical function, secret information, and a graphical animation in which the secret information will be stored by the user.

The program divides the confidential information into a random number of small pieces of data. Then graphical animation is divided into separate frames and stored in an array. From this array, some frames are chosen for further encryption. The number of chosen frames depends on how many pieces our graphical animation has been divided. In the end, an array of specially selected frames is created.

The confidential information is read, each character replaced by ASCII code, and their bit sizes are calculated.

Then, for all selected frames, the chosen mathematical function is virtually overlaying each of them as shown in Figure 2, where red dots are the pixels that will be used for encryption. This overlay is creating an array of pixels (that are the aforementioned graphs) that are used to hide the current secret data segment.

Fig. 2. Overlaying mathematical function's graph over the carrier-image.

Some complications may occur while overlaying the graph and the carrier-image: pixels under the graph might have negative value, be not an integer, or even not fit within the image borders. These problems are solved by modulation, rounding, scaling, or various combinations of those. During scaling, the maximum value of the function is divided by the number of horizontal pixels in the image. This gives us the scaling factor used to scale the entire graph. Sometimes, the values of the function can be negative. In such cases, the value is modulated (Fig. 3-4) before scaling.

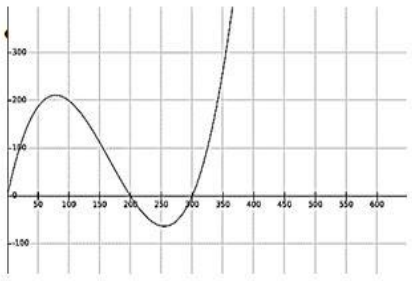

Figure 3. Before modulation¶

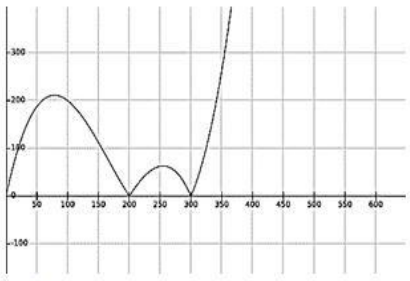

Figure 4. After modulation¶

3.2 Hiding the information

The program reads the selected frame, gets its dimensions, size, and color model. The color model is RGB, so each pixel consists of three layers.

By counting the number of pixels available, and multiplying by three, the number of layers, we get the number of bits available for replacement. Comparing with the size of the selected part of confidential information, we make sure that the size of the information does not exceed the number of bits intended for hiding.

3.3 LSB algorithm

After these operations, the selected pixels' bytes are replaced using the LSB method (Fig. 5) – the most used algorithm for steganography. When using the LSB method, the value of the least significant bit of the chosen byte is changed to the desired value. While the values for the pixel colors are changed, the visual difference is negligible and invisible to an unarmed eye [7].

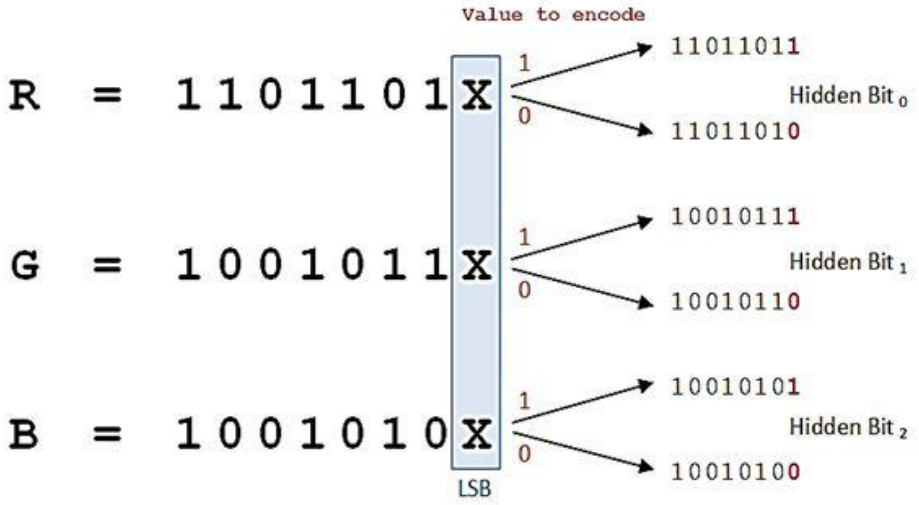

Fig.5. How the LSB algorithm works.

LSB, being the simplest algorithm to hide information, was chosen only for example, as in the study LSB is only an auxiliary algorithm, and the feature of this solution is the use of mathematical function and GIF animation frames. If necessary, a more complex and robust algorithm can be used.

3.4 End of the program

After all selected frames have some part of the secret data, the program generates new graphical animation using carrier frames, the frames that weren't chosen in the first steps, and the initial parameters of graphical animation (each frame duration, overall speed, frame sequence, animation loop counts).

3.5 Block diagrams of the described method.

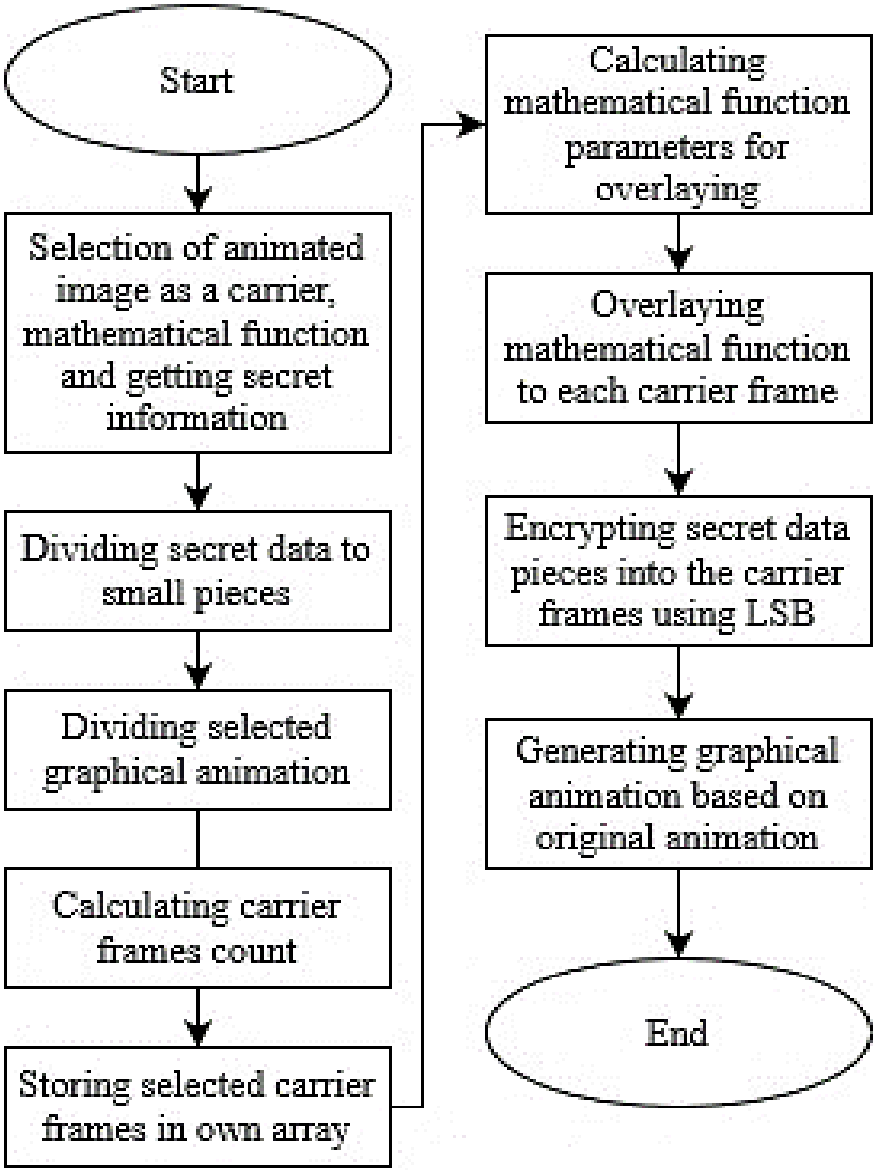

Figure 6. Block diagram of described method

3.6 Results

After hiding the information in the graphical animation, there is no difference to an unarmed eye in the carrier-frame in comparison with the original frame (Fig. 7-8).

Information is stored only in pixels whose positions correspond with the values of the function.

Fig.7. Carrier-frame before steganography

Fig. 8. Carrier-frame after steganography

Regardless of the complexity of the chosen mathematical function, the number of pixels available in the image is equal to the length of the image. It is desirable to monitor the alignment of selected pixels in an image to avoid accidental patterns and change the mathematical function if the pattern is appearing.

4 CONCLUSION

As a result of this work, a program is created which hides information in a GIF format graphical animation's frames with an RGB color model.

To complicate the process of revealing the hidden information, the animation is split into frames and the information is split into parts. The values of a pre-selected f(x) function are the corresponding pixel positions where the information is hidden. For the receiver to access the information, it is necessary to secretly transfer the function to him. This can be done directly during a meeting or using the RSA algorithm. The mathematical function is advised to be unique for each frame and to be changed over time to neutralize any progress made by the attacker in finding the key.

This method can have several practical applications in different industries. For example, it can be used in the mining industry for storing secret geolocation of mines, minerals, etc. Also, it can be used for keeping secret databases (as you can also keep a large amount of information in the GIF). Overall, every company in that industry that needs to keep its information safe and not get any unwanted attention and be attacked, can benefit from this method.

REFERENCES

1. A.G. Konheim,*Computer Security and Cryptography*. (Hoboken, NJ: John Wiley and Sons, Inc, 2007).
2. J. Ankit, *Vector vs Raster Graphics*, (2018) Jain Ankit, viewed 15 May 2020, https://www.geeksforgeeks.org/vector-vs-raster-graphics
3. D. Hemmendinger*Data Compression*, Hemmendinger David, viewed 23 May 2020, https://www.britannica.com/technology/data-compression, (2000)
4. T.A. Welch,*A Technique for High-Performance Data Compression*, viewed 21 May 2020, Sperry Research Center, (1984)
5. P. Howard, *True-Color GIF Example*, viewed 21 May 2020, http://phil.ipal.org/tc.html, (2012)
6. W.Bender, et al, *Techniques for Data Hiding*. *Riverton*. (NJ: IBM Systems Journal, 1996)
7. M. de Haas,*What are Color Models?* Marten de Haas, viewed 19 May 2020, https://www.wigglepixel.nl/en/blog/what-are-color-models/ (2018)