Annales UMCS Informatica AI 5 (2006) 181-190

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

# Robustness of data hiding in image the Fourier spectrum

Piotr Kopniak*

*Institute of Computer Science, Lublin University of Technology,*
*Nadbystrzycka 36B, 20-618 Lublin, Poland*

**Abstract**

The following paper presents the results of tests conducted by the author in the field of verification of influence of JPEG lossy compression on the robustness of data hiding methods used for the colour image which has been transformed to the frequency domain. The data have been embedded to the Fourier magnitude spectrum of the image. The possibility of decoding the hidden data with two embedding methods and various parameter values as well as diverse compression rates has also been examined. The paper also contains a short description of the discrete Fourier transform.

## 1. Introduction

Nowadays many compressed pictures or films are distributed either on optical data carriers or in the Internet. Therefore, the protection of the author rights of the product is needed. There have also appeared numerous watermarking methods of the electronic media that make it possible to embed extra data enabling the author's identification. The digitally recorded data of the image are also a very effective carrier for steganography (the science dealing with hiding secret data into other messages). It is possible to encrypt the secret data in a digital image (for instance to create a secret communication channel) in such a way that the existence of those data is undetectable for an improper person.

The image containing the secret transfer between the receiver and the sender can be modified by an intruder who wants to decipher or destroy the content message. Due to it, there appears the problem of embedding the secret message in such a way that it is resistant to various picture transform methods, especially compression.

The choice of the method of embedding data to the image carrier is of great importance for data robustness. The spatial domain methods are not very effective for that reason as they are mostly based on the colour modifications of

**E-mail address*: p.kopniak@pollub.pl

particular pixels and during the compression colour values are the most frequently modified [1,2]. A far better solution is the employment of methods based on the modification of the waves describing the image as the secret message is spread on the whole surface of the image. The conducted tests that are being described in this paper were to verify this thesis in a practical way and to estimate the robustness of chosen steganographic methods which modify the image frequency coefficients and guarantee the data safety when using JPEG lossy compression.

## 2. Image compression

According to the way of compression, compression algorithms can be divided into lossless and lossy algorithms. The former ones enable the decreasing of the graphic file size in a way that does not exclude any information, for instance by means of recording the data with the set of pixels of the same colour instead of using every pixel separately: RLE (run length encoding) compression, LZW (Lemple-Ziv-Welch) compression or by introducing the indexed colour [3,4]. The examples of such algorithms are GIF (Graphics Interchange Format) [4] and PNG (Portable Network Graphics) [5].

Lossy compression algorithms are based on the statement that human eye is imperfect and it cannot discriminate slight colour differences to such an extent as luminance differences. Therefore, one can assign the same colour to a few nearby pixels without a significant influence on the picture quality. The most popular lossy compression algorithm is JPEG (Joint Photographic Experts Group) that is used for saving photographs. The great popularity of the lossy compression results from its capacity. The ratio of the file sizes achieved in JPEG compression to the file sizes achieved due to lossless LZW compression in the GIF format is 1:4 (as JPEG compression enables twenty times over reduction in the file size without the loss in quality that could be noticed by a human eye) [6].

The loss of data during compression results from two factors: colour quantization (the colour value is expressed by a real number rounded to an integer value) and colour conversion (consistent with CCIR standard [7]).

Thus, the data hidden in the image spatial domain (with the image described by a rectangular table of pixel colour values) is in danger when undergoing this kind of compression. To hide some confidential data we can also use an image transformed to a frequency domain. Due to the fact that the waves are not of local character and they pass trough the whole area their modification should give better results with this kind of compression. The research model of information embedding through magnitude modification has been presented below.

## 3. Image Fourier transform

The spectrum modification model is based on the image frequency representation that has been achieved as a result of two-dimensional discrete Fourier transform [2,8-10]. The transform consists in image pixel value approximation by means of composing numerous periodical sinus and cosines functions. The transform for a two-dimensional area with the size M by N representing the data of the image (that is the function I (m, n)) looks like the following:

$$F(u,v)=\frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}I(m,n)\exp\left[-j2\pi\left(um/M+vn\right)/N\right].$$

As the result of this transform we gain the function of two variables representing the vertical and horizontal frequencies. In the case of a colour RGB picture the transform is conducted separately for each of the colour components, i.e. three transforms are conducted. The spatial image representation can be restored again by means of the reverse Fourier transform:

$$I(m,n)=\frac{1}{MN}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}F(u,v)\exp\left[j2\pi\left(um/M+vn\right)/N\right].$$

The set of complex numbers in which for RGB picture three complex numbers describe one spectrum point is what we receive as a result of the transform. The set of complex numbers moduluses |F(u,v)| - sinus and cosines functions amplitudes – is used in order to transform the image. By decreasing or increasing amplitudes for various frequencies we are able to transform images efficiently, for instance to delete temporal noise of image scanning process or to filter the image with low and high-pass filters.

The examplary spectrum charts are shown in Fig. 1.

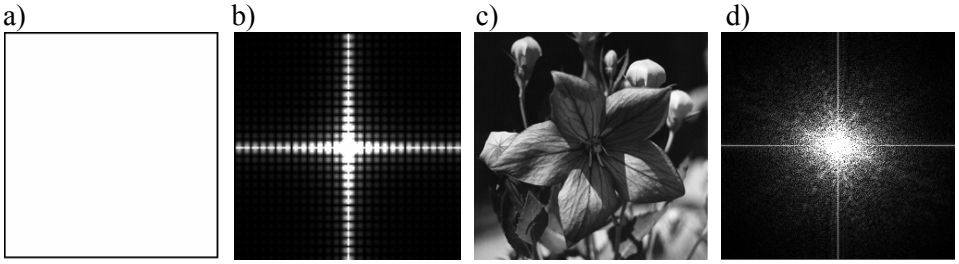



Fig. 1. Fourier transform spectrum charts; a) and c) plain images; b) and d) spectrum charts of images a), c) after the transform

The shifts of pictures in any possible direction do not cause any changes in the picture spectrum as it is always a complex number module that is taken into account and it stays indifferent. The shifting of the picture results in the shifting of its spectral representation at the same angle in relation to the middle of the picture [9,11]. Therefore, if we want the data to be transform resistant we should

add them to the circle the middle of which is in the middle of the spectral chart. However, there still remains one question: what influence does the compression have on the frequency spectrum?

## 4. Methods of magnitude spectrum modification

In the conducted research the data bites of the hidden message were added to the waves amplitudes with two methods. The first one was developed for image watermarking by Licks [12] and the second is Lee and Chen steganography algorithm [13,14] adapted by the author to image frequency domain.

In the first data embedding model the particular data bites were added to the circular waves amplitudes at certain points (u, v) in such a way that for every value of the total horizontal frequency 'u' from the <0, r> range (where r represents the radius of the circle) the vertical frequency value has been counted according to the following dependence:

$$v = \sqrt{r^2 - x^2}$$

Before the data bites with 'l' value were added they had also been multiplied by the constant (that is later called the multiplier) in order to differentiate the essential information from the background. Moreover, in order to provide the accurate '0' value bite interpretation (i.e. they are not understood as '1' during the readout) the values of adequate amplitudes were divided by the multiplier value. Due to the fact that the spectrum chart is symmetrical in relation to the middle i.e. the point with (u,v) frequency = (0,0), the data were also added symmetrically in relation to the middle.

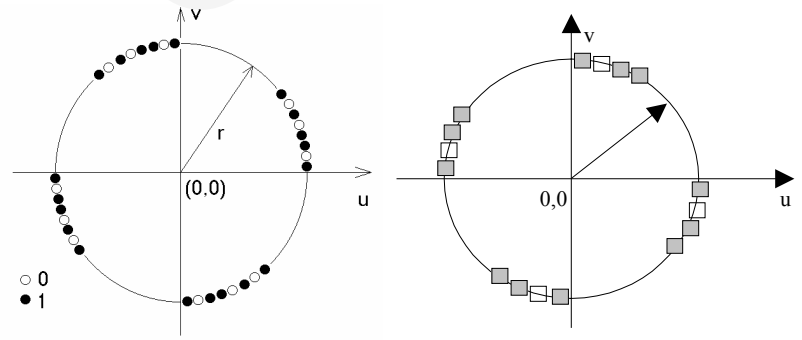



Fig. 2. The way of adding the data to the spectrum: left – Licks method, right – Lee and Chen method

So as to increase the data resistance the same bites of secret information were embedded not twice but four times and in such a way that the same information was added to every four quadrant of the chart (Fig. 2). The readout of the data was based on reading of the values in four points: (u,v), (v,-u), (-u,-v) and (-v,u) and their average.

The second data embedding model is a modified Lee and Chen algorithm. It has been created initially for the spatial domain of gray scale images. The model has been adopted frequency domain of RGB images.

The original algorithm has many stages such as: message compression, encrytpion and permutation which were introduced to reach high cryptographic data security. These stages were omitted in our research because they have no infuence on the received bit error level. The research model has no image preprocessing, either. In this method the message data bits were embedded to average values of magnitude sets contrary to the first method. The sets might be chosen in many different ways. It has been decided to choose the square sets placed circularly like in the Licks method in order to have almost the same frequency modification.

At the beginning of the embedding process the average values of the chosen areas of carier image frequency spectrum were calculated. Next, all the average values range was divided to define the number of equal-sized intervals. They were used for stego-table generation. The generation was conducted by adding one bit from pseudo random number generator (PNRG) to each interval. The seed of PNRG is one of the stego-keys of the method.

After the stego-table generation the right data embedding process was performed. Each message bit was added to one of the chosen magnitude blocks. First, the interval containing the calculated average is found in the stego-table. If a massage bit value is equal to a bit value corresponding to a found interval in the table, then the average value of the block is modified in such a way that it is equal to the middle value in that interval. When the bit values are different, then the closest interval with the proper bit value is looked for. Finally, the average block value is modified in such a way to be equal to the middle of the new interval.

Additionally, to achieve minimal average modification, the bits in a random bit string from PNRG were replaced in the following manner: bit “0” was replaced with string “01” and bit “1” was replaced with string “10”. After this replacement, if we must modify the average to another interval we change the magnitudes to a neighbour interval only.

## 5. Conducted research

The first step conducted during the research was to examine the robustness of the embedding method invented for gray scale images by Licks used for RGB images. At the beginning we must define the maximum value of the multiplier and the minimal value of the radius for which the embedded information does not cause visible changes in the image. Test images are shown in Fig.3.

It has been settled that the maximum value of the multiplier for medium and high frequencies of the pictures with 256×256 resolution is about 50. With

higher values of a multiplier or a radius smaller than 50 points, the distortions visible with naked eye in the spatial domain have appeared.

Fig. 3. Test images

Another step was checking the resistance for the distortion of data for four different radius lengths (50, 75, 100, 125 points) and three different multipliers (10, 20, 50). The size of the defect has been expressed as a percentage value of the error bites (BER) within the reconstructed information. The information that was entered was the following set of 25 characters: "abcdefghijklmnopqrstu wxyz." The next information bites were embedded successively to the red, green and blue component of the spectrum. Due to this it was possible to place 3 data bites at one point of the spectrum. All the pictures that had been modified and transformed to the spatial domain were stored with four different compression rates described with three JPEG qualities: 1.0, 0.9 and 0.8 where 1.0 quality factor means the highest quality and the lowest compression (according to Java Advanced Imaging library [15]):

1) BMP bitmap file – no compression,
2) JPEG compressed file with 1.0 quality factor, compression rate 3:1,
3) JPEG compressed file with 0.9 quality factor, compression rate 8:1,
4) JPEG compressed file with 0.8 quality factor, compression rate 12:1.

The hidden data was decoded in two different ways: 1. with the multiplier used for data embedding, 2. with the multiplier with which the percentage of error bites was the lowest. The results of the test are shown in the following tables.

Table 1 presents the percentage of error bites within the hidden data for various radius values along which the data were embedded. The first four lines show the percentage of errors for the same multiplier value that was used for saving and decoding. The latter lines show the values of multipliers chosen experimentally in such a way to achieve the lowest percentage of errors while decoding.

Table 2 presents the percentage of error bites for various multiplier values used for saving and decoding the data as well as for various ways of embedding the bites with secret information. In the first way the subsequent information bites were embedded to each of the colour components separately – every point in the spectrum contained 3 bites of hidden data. The other way was based on

embedding of the same bite of hidden data to all the three colour components of the spectrum at the same point. In every case the same multiplier was used for both saving and decoding.

Table 1. The percentage of error information bites decoded from a compressed graphic files in relation to the radius (Licks method)

| Radius | Multiplier = 50<br>Quality factor of JPEG | | |
|---|---|---|---|
| | 1.0 | 0.9 | 0.8 |
| 125 | 52.0 % | 53.5 % | 53.5 % |
| 100 | 50.0 % | 53.5 % | 53.5 % |
| 75 | 35.0 % | 43.5 % | 50.0 % |
| 50 | 15.5 % | 25.0 % | 26.0 % |
| Best Multiplier | 16 | 16 | 6 |
| 125 | 31.5 % | 34.0 % | 40.5 % |
| Best Multiplier | 17 | 15 | 9 |
| 100 | 28.5 % | 32.5 % | 36.5 % |
| Best Multiplier | 23 | 21 | 18 |
| 75 | 23 % | 31.5 % | 32.5 % |
| Best Multiplier | 30 | 20 | 28 |
| 50 | 3.5 % | 22 % | 23 % |

Table 2. The percentage of error information bites decoded from compressed graphic files in relation to the multiplier and the way of data embedding (Licks method)

| Multiplier | Radius = 75, Succesive information bites within RGB components<br>Quality factor of JPEG | | |
|---|---|---|---|
| | 1.0 | 0.9 | 0.8 |
| 50 | 35.0 % | 43.5 % | 50.0 % |
| 20 | 32.0 % | 37.0 % | 46.0 % |
| 10 | 22.5 % | 30.5 % | 34.0 % |
| Multiplier | Radius = 75. The same information bite in all RGB components<br>Quality factor of JPEG | | |
| | 1.0 | 0.9 | 0.8 |
| 10 | 0 % | 0 % | 1.5 % |

The results of image compression coded with the Licks's method which modify single magnitude to embed one message bit used for RGB images were poor. So we decided to use the Lee and Chen embedding algorithm employing more magnitudes for embedding one message bit. We have choosen four different dimensions for square regions of magnitudes: 2x2, 3x3, 4x4 and 5x5 points of image magnitude spectrum and four numbers of intervals on which the average values range was divided: 32, 16, 8 and 4 intervals. Each of the carrier

images was compressed with four JPEG compression quality factors: 1.0, 0.9, 0.8 and 0.7.

Table 3. The percentage of error information bites decoded from the compressed graphic files in relation to the JPEG quality factor, radius, no. of intervals and block size

| BER = 0% | | | | | BER < 3.00% | | | | |
|---|---|---|---|---|---|---|---|---|---|
| BER | Block size | No. intervals | Radius | JPEQ quality | BER | Block size | No. intervals | Radius | JPEQ quality |
| 0 | 4 | 4 | 50 | 0.7 | 2.78 | 5 | 4 | 50 | 0.7 |
| 0 | 3 | 4 | 50 | 0.7 | 1.09 | 2 | 4 | 50 | 0.7 |
| 0 | 3 | 4 | 50 | 0.8 | 1.47 | 4 | 4 | 75 | 0.7 |
| 0 | 4 | 4 | 50 | 0.8 | 1.43 | 2 | 4 | 75 | 0.7 |
| 0 | 4 | 4 | 75 | 0.8 | 2.78 | 5 | 4 | 50 | 0.8 |
| 0 | 5 | 4 | 75 | 0.8 | 2.17 | 2 | 4 | 50 | 0.8 |
| 0 | 3 | 4 | 50 | 0.9 | 1.43 | 2 | 4 | 75 | 0.8 |
| 0 | 4 | 4 | 50 | 0.9 | 1.09 | 2 | 4 | 50 | 0.9 |
| 0 | 4 | 8 | 50 | 0.9 | 2.78 | 5 | 4 | 50 | 0.9 |
| 0 | 5 | 4 | 75 | 0.9 | 1.67 | 3 | 8 | 50 | 0.9 |
| 0 | 4 | 4 | 75 | 0.9 | 1.09 | 3 | 4 | 75 | 0.9 |
| 0 | 3 | 4 | 100 | 0.9 | 1.43 | 2 | 4 | 75 | 0.9 |
| 0 | 3 | 4 | 50 | 1.0 | 2.08 | 4 | 4 | 100 | 0.9 |
| 0 | 4 | 4 | 50 | 1.0 | 1.56 | 2 | 4 | 100 | 0.9 |
| 0 | 2 | 4 | 50 | 1.0 | 1.32 | 5 | 4 | 100 | 0.9 |
| 0 | 5 | 4 | 50 | 1.0 | 2.17 | 2 | 8 | 50 | 1.0 |
| 0 | 4 | 8 | 50 | 1.0 | 2.27 | 4 | 16 | 50 | 1.0 |
| 0 | 3 | 8 | 50 | 1.0 | 2.14 | 2 | 4 | 75 | 1.0 |
| 0 | 5 | 8 | 50 | 1.0 | 1.09 | 3 | 4 | 75 | 1.0 |
| 0 | 5 | 4 | 75 | 1.0 | 1.79 | 5 | 8 | 75 | 1.0 |
| 0 | 4 | 4 | 75 | 1.0 | 1.04 | 4 | 4 | 100 | 1.0 |
| 0 | 3 | 4 | 100 | 1.0 | 1.56 | 2 | 4 | 100 | 1.0 |
| | | | | | 1.32 | 5 | 4 | 100 | 1.0 |

## Conclusions and further research

The best results are achieved when we embed information to the waves amplitudes within the range of medium frequencies. It is a kind of compromise between the data resistance to the destruction and distortions of the data caused by their placement. The number of errors caused by compression is adequate to the increase in frequency (radius in image spectrum). During JPEG compression we can observe the biggest distortions among the highest frequency harmonic components because they are removed at the quantization process. The loss of data also appears during the conversion of a colour to YCbCr colour space. Some significant distortions in the picture after conducting the reverse transform

also appear when we modify low frequency waves. When the radius is 50 even the multiplier of 10 causes visible colour changes in the picture, which can be especially observed in the large, dark areas of low changeability.

In the Licks algorithm the use of lower multiplier values that are closer to those of modified amplitudes results in the fact that the data is more resistant to distortions. However, when the multiplier values are too low, e.g. about 0.5 of the modified amplitude value, it causes more significant errors. Compression results in "the smoothing out of the spectrum" i.e. the modified coefficients values are lowered, especially for high frequencies. Therefore, to reduce the number of errors we should also reduce the multiplier used for decoding.

The application of the method in which each data bite is embedded to each colour component instead of each component of a different data bite could result in the significant increase in the resistance of the secret data to JPEG compression. The error-free readout is possible even with 9:1 compression where the JPEG quality factor in the first method is 90%.

Better results than in the first method have been achieved in the second one, see Table 3. When we used the Licks algorithm, good results (which mean BER = 0%) were only in one case for the image compressed with 1.0 and 0.9 JPEG quality factors. In the second method BER = 0% was for the images compressed with all tested JPEG quality factors. If a radius was shorter and the quality was higher, then BER was smaller. The best results were for radius 50, 4 intervals and 4x4 size of magnitude block.

The second method provides a better steganographic sequrity, too. Higher magnitude modifications in the Licks method caused a visible circle on the Fourier image spectrum and add dectruction possibility to an active warden (Fig. 4). The average modifications in the second method in most cases were not visible and the destruction possibility is lower without a key i.e.: radius, shape of block and stego-table.

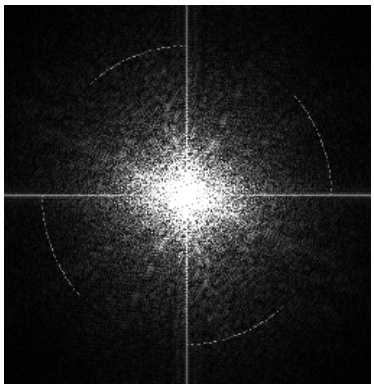
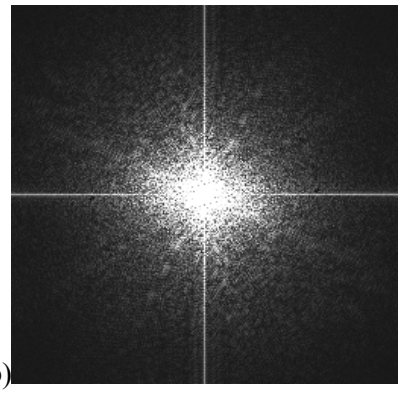
a)  b) 

Fig. 4. Modified Fourier magnitude spectrum of image: a – Licks'es method, b – modified Lee and Chen method

The future research will be done in order to find the data embedding method that would be more resistant to the lossy compression and digital filtering. Therefore, the influence of the use of colour conversion as well as other multiresolution transforms such as wavelet transforms or filer pyramids on the improvement of test results should be checked.

## References

[1] Kopniak P., *Porównanie odporności na zniekształcenia danych ukrytych w obrazie metodą LSB i metodą modyfikacji widma*, Polskie Towarzystwo Informatyczne, Lublin, (2004), in Polish.
[2] Katzenbeisser S., Petitcolas F., *Information Hiding. Techniques for Steganography and Digital Watermarking*, Artech House, Inc., Norwood, (2000).
[3] *Formaty graficzne* <http://magazyn.wsinf.edu.pl/grafika/Formaty.doc>.
[4] *GIF89a Specification* <http://www.w3.org/Graphics/GIF/spec-gif89a.txt>.
[5] *PNG Documentation* <http://www.libpng.org/pub/png/pngdocs.html>.
[6] *JPEG image compression FAQ, part 1/2* <http://www.faqs.org/faqs/jpeg-faq/part1>.
[7] *CCIR 601* <http://www.fact-index.com/c/cc/ccir_601.html>.
[8] Fortuna Z., Macukow B., Wąsowski J., *Metody numeryczne*, WNT, Warszawa, (1993), in Polish.
[9] Seul M., O'Gorman L., Sammon M., *Practical Algorithms for Image Analysis*, Cambridge University Press, (2001).
[10] Wojnar L. Kurzydłowski, Szala, *Praktyka analizy obrazu*, Polskie Towarzystwo Stereologiczne, Kraków, (2002), in Polish.
[11] Gonzales R.C., Woods R.E., *Digital Image Processing*, Addison-Wesley Publishing Company, (1993).
[12] Licks V, Jordan R., Azevedo D.F.G., Correa J.S., Frano P.R.G., Ragundes R.D.R., *Circular Watermark Robust Against Geometric Attacks*, accepted for IEEE International Symposium on Information Theory and Its Applications, Hawaii, USA, (2000).
[13] Lee Y.K., Chen L.H., *High Capacity Image Steganographic Model.*, 2000, <http://debut.cis.nctu.edu.tw/pages/publish/research_e.htm>
[14] Lee Y.K., Chen L.H., *An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*, (1999), <http://debut.cis.nctu.edu.tw/pages/publish/research_e.htm>.
[15] *Programing in Java Advanced Imaging*, Release 1.0.1. Sun Microsystems, Inc., November (1999).