

CRYPTOGRAPHY AND STEGANOGRAPHY OF VIDEO INFORMATION IN MODERN COMMUNICATIONS

Zenon Hrytskiv, Sviatoslav Voloshynovskiy and Yuriy Rytsar

Abstract. In this paper image cryptography and steganography performed in frequency domain using random phase mask encoding are presented. The use of random phase mask allows to decorrelate initial image and makes it unrecognizable. This property is used for proposed image encryption and for steganography to increase the security level of the encoded image and to make it less visible. Finally, two keys are needed to decrypt the image. The efficiency of the proposed approach is demonstrated by the computer modeling.

1. Introduction

The growing possibilities of modern communications require the special means of confidential and intellectual property protection against unauthorized access and use. Especially these problems are actual for computer networks, which make possible to exchange the large amount of video information, and for TV systems.

The formulation and solution of two problems of image cryptography and steganography considered from the common position are presented in the paper. Image cryptography is considered as an encoding technique for data transmission through communication channels under condition that the third party could not read and interpret this data in right way. However, transmitted data have not clear logical context that can attract attention of the interested people and impel to the unauthorized break of product protection. Additionally, such kind of data encoding meets a lot of obstacles concerned either with the prohibition of the establishment, where one works,

Manuscript received February 26, 1998.

A version of this paper was presented at the third Conference Telecommunications in Modern Satellite and Cables Services, TELSIS'97, October 1997, Niš, Yugoslavia.

Prof. dr Z.D. Hrytskiv and S.V. Voloshynovskiy are with State University Lvivska polytechnika, Department of Radio Technical Devices, S.Bandery Str., 12, 290646, Lviv, Ukraine. Y.B. Rytsar is with Institute of Physics and Mechanics, Naukova Str., 5, 290601, Lviv, Ukraine.

to use any kind of encrypted information or with not very pleased attitude of local rule to such kind of messages. Nevertheless, cryptography has become one of the main tools for privacy, trust, access control and authentication, digital signatures and electronic payment, secure messaging.

The second problem is closely related with the protection of author rights and namely with the overspreading and use of video products without permission of copyright owners especially by digital channels (i.e. CD-ROM's, Internet or video recorders), because digital formats make possible to provide high image quality even under multicopyng. Therefore, the special part of invisible information is implanted in every image that could not be easily extracted without specialized technique saving image quality simultaneously. This is the task of steganography. According to it, the additional possibility appears to compensate the cryptography drawback connected with the lack of the logical meaning in the image. Moreover, it is possible to transmit the private letter or image under another photo (e.g. known top-model or Shuttle) without any suspicion on this information and with satisfactory quality.

The paper presents a version of digital image cryptography based on random phase mask implementation, multispectrum image steganography technique and the combination of the above approaches. Section 2 presents the proposed image cryptography based on the random phase mask encoding. The image steganography encoding is considered in Section 3 and Section 4 concludes that paper.

2. Image cryptography

The traditional approach to image encoding consists in the source coding, encryption and channel coding [1].

The source coding is used to compress data and match it with the bandwidth of communication channel. However, the obtained data are sensitive to the communication noise and not protected against unauthorized use. To overcome these disadvantages the next two stages are to be used. To protect data against unauthorized access the encryption is accomplished. The encryption stage is performed separately from source coding. To reduce influence of the communication channel noise the channel coding is used which is based on the specialized error correction codes able to detect and correct errors directly during data transmission. Both encryption and channel coding require the introduction of the redundant information in initial data that leads to the increase of data size and corresponded time of transmission.

The paper presents alternative approach to image encoding which is based on the transform technique using random phase masks. The phase informa-

tion is known to be very important for image processing [2]. The performed computer experiments show that just phase information makes possible to reconstruct image uniquely. The phase of the given image in combination with the averaged amplitude spectrum obtained from the group of images gives the satisfactory results in the most practical important cases. Therefore, adding some component in the phase spectrum of the image one can essentially change the initial image structure. The above phenomenon could be efficiently used for image encryption. Moreover, the localized communication noise is spread over all reconstructed image that makes it invisible opposite the above mentioned approach where localized noise conditions local noise associated with blocking effect [3].

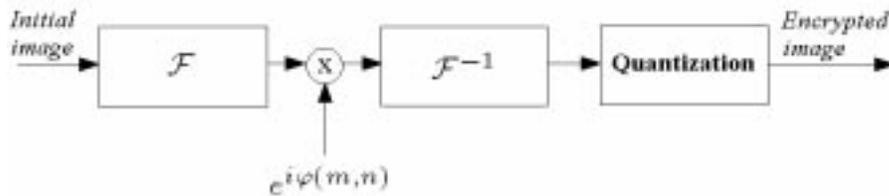


Figure 1. Block diagram of image encryption based on random phase mask encoding where $e^{i\varphi(m,n)}$ is random phase mask and m, n are samples of spatial frequencies.

The proposed encryption consists of Fourier transform of the initial image needed to be encrypted, phase modification, inverse Fourier transform, quantization and image conversion to any graphical image format for data visualization and further transmission across the communication channel or storage. The block diagram of image encryption based on random mask encoding is shown in Fig. 1. Initial image is transformed in spatial frequency domain by means of direct fast Fourier transform (FFT) \mathcal{F} . The amplitude of the transformed image is saved without changing while the phase is modified by the multiplication on the complex exponential component $e^{i\varphi(m,n)}$ which is further called phase mask. The phase mask has the random character and is associated with the key for encryption. There are several ways to receive random or quasi-random phase masks suitable for the encryption purposes. It was proposed to use the quasi- m - arrays and the Gold code arrays as the reference function for random phase mask generation [3]. Although, there are a lot of possible combinations of the above arrays their potential number is finite. Moreover, the special algorithm is required to order phase mask in accordance with the main properties of phase characteristics of real 2D signals, i.e. phase is odd function.

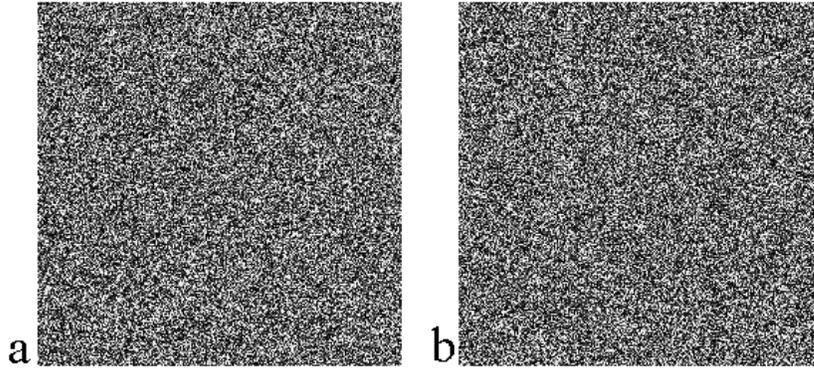


Figure 2. The phase masks used for computer encryption.

The additional problems could appear which are closely related with mismatches of the image size and the order of the chosen reference function for phase mask generation. Therefore, it will restrict the general number of possible key combinations. To make the choice of the phase mask independent from the size of the initial image and to simplify the process of the phase mask generation we proposed to receive it as the phase of any random field in spatial coordinate domain or even from another image. Obviously, the number of possible combinations is essentially increased in this case that complicates the possibility of the unauthorized decryption. The modified spectrum is then transformed in coordinate domain using inverse FFT \mathcal{F}^{-1} . Although the initial image has the fixed number of possible gradations the image after inverse FFT will be not integer.

Therefore, to compress data and to enable the digital visualization of the encryption results the necessity of the quantization appears. The several approaches could be used for this aim. The most simple approach consists in the scalar quantization. However, the results of the computer simulation show the high sensitivity of the decoded image to the round-off errors. Therefore, to minimize the quantization noise Lloyd–Max quantization is frequently used [4],[5]. The quantized image is then converted in BMP format.

To demonstrate the main features of the described approach the computer modeling is performed on the examples of grayscale images. Two random phase masks shown in Fig. 2a,b were used for this aim. These masks are obtained from random field with uniform distribution.

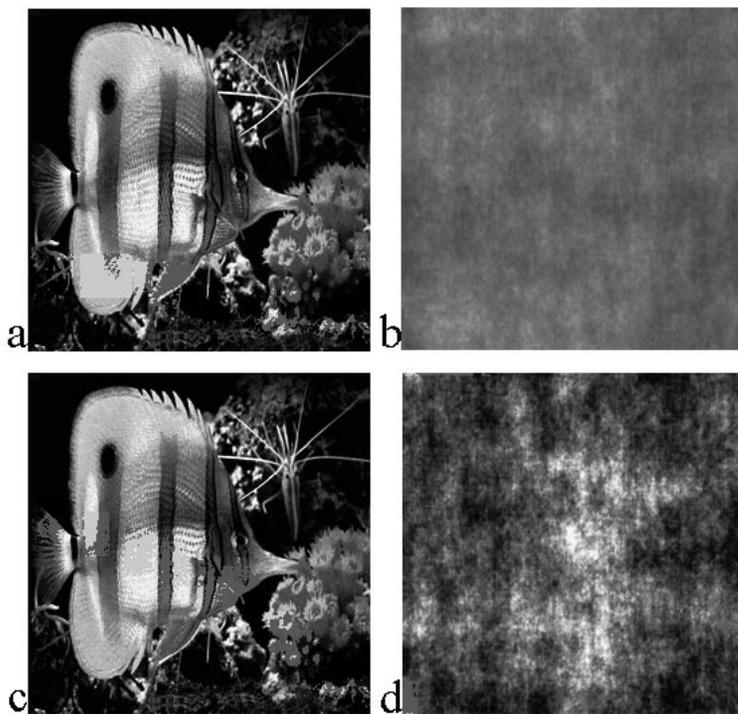


Figure 3. Initial image "Fish" (a) and the result of the encryption (b) using phase mask from Fig. 2a. The results of image decryption with the correct choice of phase mask from Fig. 2a (c) used for encryption and phase mask from Fig. 2b (d).

The initial image "Fish" needed to be encrypted is shown in Fig. 3a. The result of the encryption based on Lloyd–Max quantization and with use of phase mask from Fig. 2a is shown in Fig. 3b. The result of the image decryption with the correct use of phase mask used for encryption is shown in Fig. 3c and the result of image decryption with phase mask from Fig. 2b is demonstrated in Fig. 3d. In the case of proper choice of random phase mask image is completely reconstructed (Fig. 3c) and the decrypted image has random character, if the phase mask is not properly chosen that corresponds to the attempt of the unauthorized decryption. In the case of implementation of the quasi- m -arrays and the Gold code arrays which are the binary function it is necessary to guess $2(M^2/2)$ binary values of the phase mask, where $M \times M$ is the image size, or to know the corresponded order of the used reference function and the cyclic law of phase mask struc-

ture organization. In the proposed case of the phase mask extracted from random field, the regular structure of the phase mask does not exist and the dynamic range of real values is $[-180^\circ; +180^\circ]$. If integer values of phase mask are only used, it is necessary to guess $360(M^2/2)$ for unauthorized access. However, such phase mask, as a key, requires more disk space to be stored. The advantages of its implementation are obvious concerning the future reliability. Giving the general classification of such kind of cryptography we could relate it to key-based approach with symmetric (secret-key) algorithm, because the same key is used for encryption and decryption.

Summarizing this Section we can conclude that the encrypted images have no more longer strict logical context which is the main goal of cryptography. However, this fact could attract the attention of the third party and impel it to the beginning of cryptanalysis (i.e. to the breaking ciphers and retrieving the plaintext without knowing the proper key). Therefore, we propose to use steganography to hide the encrypted image in the structure of another image called "container" or background image.

3. Image steganography

In this paper we consider steganography not as alternative to cryptography, but as a means of its supplementing to reduce the chance of the encrypted image being detected. Developing this method of steganography we haunt the aim to design the common unified approach to image cryptography and steganography. Therefore, the frequency domain based approach, used for the above proposed cryptography, was chosen. The steganography performed in frequency domain has a number of the advantages in comparison with the steganography performed in the coordinate domain which mainly uses *Least Significant Bit* method (i.e. software like **Hide and Seek v4.1, S-Tools**). First, after proposed encryption the initial image loses the logical context and edges corresponded the object borders which are very important for object recognition and scene interpretation. Therefore, after steganography encoding these edges are not more visible on the image in comparison with the direct 'insertion'. From this point of view, we could consider the cryptography as a method of image decorrelation. Second, the two keys appear. The first key is connected with phase mask used for image cryptography and the second one is associated with the background image (container) that increases the reliability of the system. Third, the proposed steganography performed in the frequency domain does not require the header which is typical for coordinate domain based systems. Systems which use the noise modulation and *Least Significant Bit* method spread data throughout the image in some random way. To save this information where the data are allocated the header is required which is typically added

to the encrypted image. This header information identifies the method used. However, the existence of header could point the cracker in the direction of right cryptanalysis. **White Noise Storm** and **S-Tools** have the option to remove the header, but others do not. Therefore, the proposed approach have one more level of reliability due to the absence of the header. Forth, some programs, like **Hide and Seek**, have the restriction on the possible image size which could be implanted in the background image. This fact is connected with method used for data encoding. **Hide and Seek** uses *Least Significant Bit* of each pixel to encode characters or pixels of the initial image, 8 pixels per character. Therefore, the size of image that could be encoded is at least in 8 times smaller, if do not take into account the size of the needed header. The proposed version of the steganography has not such kind of restriction, because it uses all available surface of the background image with relation 1 pixel of background image – 1 pixel of encrypted image.

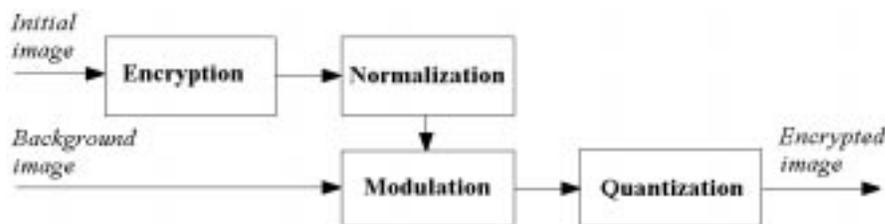


Figure 4. Block diagram of generalized image steganography.

Summarizing the large amount of the existed steganography techniques we have developed the generalized scheme of modern image steganography. The typical diagram of it is shown in Fig. 4. The initial image is transformed in the noise signal by means of the encryption. In the above proposed cryptography this goal is successfully reached using random phase mask encoding. To make the encrypted image invisible the noise signal is normalized. In our approach, the normalization consists in the decrease of the amplitude and phase of the encrypted image in the given number of times. For the most known techniques the normalization stage is accomplished interactively to ensure the compromise between the invisibility of the encrypted image and possibility of its further unique reconstruction. It was established in our experiments that the possible decrease is in the range of 14–18 to satisfy the above compromise and it is performed automatically without interactive control. The modulation stage consists in the simple add operation of the modified components of the encrypted image and the corresponded components of the background image in the proposed method. The described pro-

posed joint cryptography/steganography approach is shown schematically in Fig. 5.

The next example demonstrates the main features of the above proposed combined version of cryptography and steganography. Image "Lena" (Fig. 6a) is the background image that will be transmitted by communication channel. This image will be visible one. Image "Airfield" (Fig. 6b) is the image needed to be encrypted. This image will be invisible one and should not be seen without special signal processing. The image "Airfield" encrypted by using proposed cryptography approach with phase mask from Fig. 2a is shown in Fig. 7a. Thus, the initial image structure is not recognized and to decode it is necessary to know the phase mask that plays the role of encryption key. The result of proposed steganography approach application to the combination of image from Fig. 7a and "Lena" is shown in Fig. 7b. The result of data extracting from Fig. 7b and corresponded image decryption coincides with image from Fig. 6b.

To decode image the background image should be known exactly. It predicts that all conditions of this image receiving should be saved, i.e. the corresponded viewpoint, light, and even defocusing and aberration of camera should be the same as for the used background image. Obviously, when the unknown territory, face or some scene is used, it is impossible to satisfy all this requirements simultaneously.

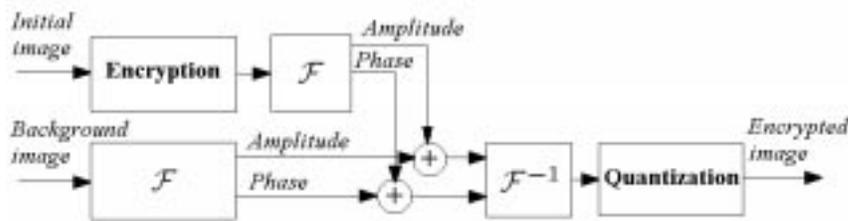


Figure 5. Block diagram of combined image encryption and steganography based on random phase mask encoding.

The next example demonstrates the stability of the method to the attempt of the unauthorized break. Let us assume that the phase mask used for encryption is known for the third party for some reasons, but the background image is not. We used in our experiment the well-known image "Lena" as the background image, but it was just shifted horizontally at 1 pixel to model only one unknown parameter for the third party (Fig. 8a).



Figure 6. Image "Lena" (a) is the background image that will be transmitted and image "Airfield" is the image to be encrypted.

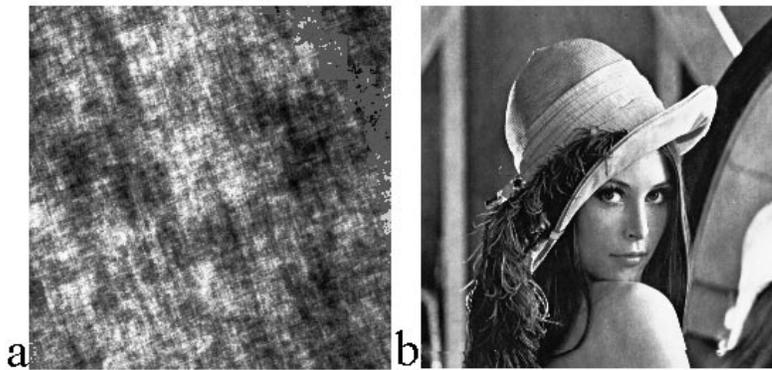


Figure 7. Encrypted image "Airfield" (a) using the random phase mask encoding and result of image steganography encoding (b).

The rest of encryption and steganography encoding were performed in the same way as for the above example. Let us assume that the third party has standard unshifted image "Lena" (Fig. 6a) and tries to use it directly for decryption. The image after steganography decoding is shown in Fig. 8b and after decryption in Fig. 8c. Therefore, only one factor, that could appear during image fragmentation, conditions the complete destroy of the image regular structure. Therefore, to decrypt image uniquely the two keys are required.

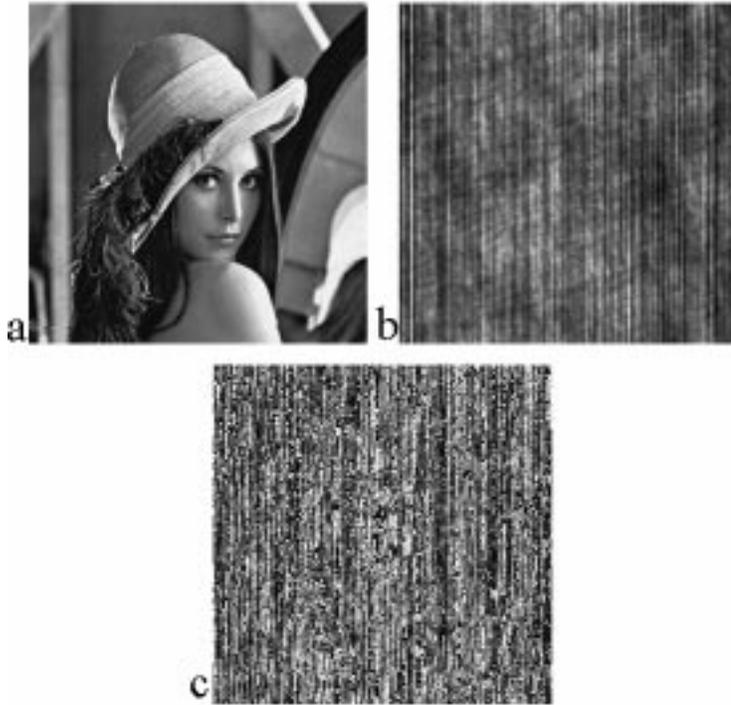


Figure 8. Image decryption with the unknown background image: background image used for steganography encoding (a), image received after steganography decoding (b) taking as the background image initial unshifted "Lena"; resulted image (c) of decryption from image (b).

4. Conclusions

In this paper the problems of image cryptography and steganography using frequency domain encoding with random phase masks were considered. The performed computer simulation demonstrates the high efficiency of the proposed technique and the analytical comparative analysis indicates a number of advantages in comparison with the existed steganography software. The results of attempt of unauthorized decryption and steganography decoding are given.

REFERENCES

1. R.C. GONZALEZ AND R.E. WOODS: *Digital Image Processing*. Addison-Wesley, Reading, 1992.

2. A.V. OPPENHEIM AND J.S. LIM: *The importance of phase in signals*. Proc. of the IEEE, vol. 69, 1981, pp. 529–541.
3. C.J. KUO AND C.S. HUANG: *Robust coding technique–transform encryption coding for noisy communications*. Optical Engineering, vol. 32, Jan. 1993, pp. 150–156.
4. S.P. LLOYD: *Least square quantization in PCM*. IEEE Trans. Inf. Theory, vol. IT–28, March 1982, pp. 129–137.
5. J. MAX: *Quantizing for minimum distortion*. IRE Trans. Inf. Theory, vol. IT–6, pp. 7–12, March 1960.