ISSN 2348 – 9928
IJAICT Volume 2, Issue 5, May 2015 Doi:01.0401/ijaict.2014.02.17 Published Online 05 (05) 2015

A SURVEY FOR CRYPTOGRAPHY AND STEGANOGRAPHY OF VIDEO INFORMATION IN MODERN COMMUNICATIONS

Prof. V.R. Prakash
Assistant Professor,
Electronics and Communication Engineering
Hindustan University,
Chennai, Tamilnadu, India.

Prof. P. Kumaraguru
Assistant Professor,
Electronics and Communication Engineering
Hindustan University,
Chennai, Tamilnadu, India.

Abstract — The image cryptography and steganography performed in frequency domain using random phase mask encodingare presented. These of random phase maskallowsto deccorrelate initial image and makes it unrecognized. 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 o decrypt the image. The efficiency of the proposed approach is demonstrated by the computer modeling.

Keywords— Image Encryption, Image Correlation, Decryption, Steganograph, Least Significant Bits.

I. INTRODUCTION

The growing possibilities of modern communications require the special means of confidential and intellectual property protection again stun authorized 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 haven to 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, to use any kind of encrypted information or with not very pleased attitude of local rule to such kind of messages. Never the less, 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 over spreading 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 multi copying. 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, multi spectrum 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 Section3 and Section4 concludes that paper.

II. 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 band width of communication channel. However, the obtained data are sensitive to the communication noise and not protected again stun authorized use. To overcome these disadvantages the next two stages are to be used. To protect data against 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 unauthorized access the encryption is accomplished. The encryption stage is performed separately from source coding.

ISSN 2348 – 9928
IJAICT Volume 2, Issue 5, May 2015 Doi:01.0401/ijaict.2014.02.17 Published Online 05 (05) 2015

To reduce influence of the communication channel noise 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 information is known to be very important for image processing [2]. The performed computer experiments show that just phase information makes

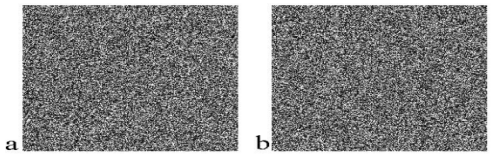

Fig 1: Image Encryption Based On Random Phase Mask Encoding

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)F. The amplitude of the transformed image is saved without changing while the phase is modified by the multiplication on the complex exponential componential'(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 aloof 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 signals, i.e.phase is odd function.

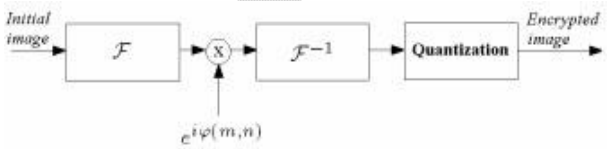

Fig 2 : The phase masks used for computer encryption.

Possible to reconstruct image uniquely. The phase f 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 overall reconstructed image that makes it invisible opposite the above mentioned approach where localized noise conditions local noise associated with blocking effect [3].

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. 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 forth is aim. The simplest 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 [4],[5]. The quantizated 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 gray scale images. Two random phase masks shown inFig.2a,b were used for his aim. These masks are obtained from random Field with uniform distribution.

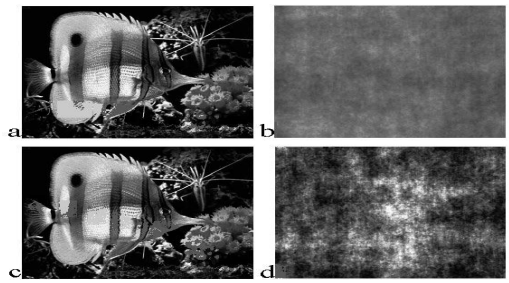

Figure3. Initial image "Fish"(a) and he result of the encryption (b) Using phase mask

From Fig. 2a. There 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 been cryptedis showninFig.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. There result of the image decryption with the correct use of phase mask used for encryption is shown inFig.3 can the result of image decryption with phase mask fromFig.2b is demonstratedinFig.3d.Inthecase 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 quasim arrays and the Gold code arrays which are the binary function it is necessary to guess 2(M2/2) binary values of the phase mask, where M*M is the images zero to know the corresponded order of the used reference function and the cyclic law of phase mask structure 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 frequently used dynamic range of real values is[-180:+1802]. If integer values of phase mask are only used, it is necessary to guess 360 (M2=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 plain text with out knowing the proper key). Therefore, we proposed housesit geography to hide the encrypted image in the structure of another image called

III. STEGANOGRAPHY VS CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. According to dictionary.com: ***Steganography is***: "Hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message" and Cryptography is "The process or skill of communicating in, or deciphering secret writing or ciphers." Steganography can be used to cloak hidden messages in image, audio and even text files. It has until recently been the poor cousin of cryptography. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video. Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message.

Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. The distinction between cryptography and steganography is an important one, and is summarized by the following table.

Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the *contents* of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithms are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Table 1: Comparison

IV. COMBINED CRYPTO STEGANOGRAPHY

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the

cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

A pictorial representation of the combined concept of cryptography and steganography is depicted in fig 4.

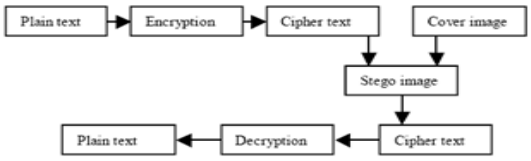

Fig 4 : cryptography and steganography

In, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types [4]:

Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

V. CONCLUSION

A steganography method is proposed to embed information within an encrypted image data randomly. This method will be expected to spread hidden information within encrypted image data randomly based on the secret key before transmission. Thus, this information appears to be nothing out of the usual and should be available to the receiver to rebuild the same secret transformation table, which is needed to rebuild the transformed image, and then recover the original image. The insertion positions of this information will be randomly selected. Experimental results of this method show that the correlation and entropy values before and after insertion process were the same, offering a simple and strong way to conceal the data in the encrypted image. Thus, it will be used to reduce the chance of the encrypted image being detected and then enhance the security level of the encrypted images.

References

[1] R.C.Gonzalez and R.E.Woods: Digital ImageP rocessing. Addison Wesley, Reading, 2012.

[2] A.V.Oppenheim and J.S.Lim: The importance of phase in signals. Proc.of the IEEE, vol. 9,1981, pp.529

[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.

[4] Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, " An Encrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh. 2009.

[5] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12

[6] Alan Siper, Roger Farley and Craig Lombardo, "The Rise of Steganography", Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005.

[7] B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010

[8] Domenico Bloisi and Luca Iocchi, "Image Based Steganography and Cryptography", Sapienza University of Rome, Italy. 1650-2012.