A Survey on Image Encryption and Decryption

Utkarsh Shastri[1], Shalini Tiwari[2], Geremsa Swargiary[3]

[1,2,3]*Student, Department of Computer Science and Engineering, Babu Banarasi Das Institute of Technology, Ghaziabad, India*

Abstract**: In the past few years, the attention of researchers have been more likely about information security. A lot of image encryption techniques are available to secure the data and information an image can contain. The way it's growing day by day it have been no more just about securing some data but a national or international concern. Nations are using these technologies to insure their own security. Due to some intrinsic features of images like bulk data capacity and high data redundancy, the encryption of image is different from that of text; therefore it is difficult to handle them by traditional encryption methods. A new image encryption algorithm based on Magic Rectangle (MR) is being applied. In the same the plain image is converted into blocks of single bytes and later is replaced by MR value. Controls are in user's hand as they select the parameters. Subsequently the image is being encrypted with public key cryptography algorithm such as RSA, ElGamal etc. Experimental results Shows that these algorithms can be successfully used in encrypting/decrypting the images with respective secret keys with good encryption effect.**

Keywords**: Encryption, Decryption**

1. Introduction

Encryption as provided in a process is all about converting some data, messages, or information into a form of unreadable format that only intended personals can access. Same happens when we talk about image encryption. By encryption of an image it's necessary that the intended person have access to the keys to decrypt the message in a readable format.

The word encryption itself means hidden or secret. For different reasons people have been protecting their messages, the interest led them to find new ways of doing the same as with the time encryption of information changed in many ways. Threads on computer and network security increase with each passing day and the world introduces number of growing resources. No computer or network is immune from attacks.

2. Literature survey

Signal-processing modules occupied directly on encrypted data provide an elegant solution to request scenarios where valuable signals must be protected from a malicious processing device. We investigate the implementation of the discrete Fourier transform (DFT) in the encrypted domain by using the homomorphic properties of the underlying cryptosystem. The protection of digital data when it is processed by other parties has arisen as a major concern for the general public, and an important topic of research. The field of Signal Processing in the Encrypted Domain (SPED) has emerged in order to provide efficient and secure solutions for preserving privacy of signals that are processed by un-trusted agents. The impossibility of using a strategy based solely on current homomorphic encryption systems, and we propose several novel secure protocols for a privacy-preserving execution of the least mean squares (LMS) algorithm, combining different SPED techniques, and paying special attention to the error analysis of the finite-precision implementations. Signal processing tools working directly on encrypted data could provide an efficient solution to application scenarios where sensitive signals must be protected from an untrusted processing device. In this paper, we consider the data expansion required to pass from the plaintext to the encrypted representation of signals, due to the use of cryptosystems operating on very large algebraic structures. A general composite signal representation allowing us to pack together a number of signal samples and process them as a unique sample is discussed. The purposes of copy protection and copy deterrence for multimedia content are discussed. In copy deterrence, a content owner (seller) inserts a unique watermark into a copy of the content before it is sold to a buyer. If the buyer sells unauthorized copies of the watermarked content, then these copies can be traced to the unlawful reseller (original buyer) using a watermark detection algorithm. Homomorphic property of public-key cryptosystems is applied for various cryptographic protocols, such as electronic cash, elective system, bidding protocols, etc. Several fingerprinting protocols also exploit the property to achieve an asymmetric system. However, their enciphering rate is particularly low and the implementation of watermarking technique is difficult.

When it is chosen to transmit redundant data over an insecure and bandwidth-constrained network, it is customary to first compress the data and then encrypt it. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. Although counter-intuitive, we show surprisingly that, complete the use of coding with side information principles, this reversal of order is indeed possible in some settings of interest without loss of either optimal coding efficiency or perfect secrecy. Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted realworld sources, such as images, the key to increase the compression efficiency is how the source dependency is exploited. Approaches in the literature that make use of Markov properties in the Slepian-Wolf decoder do not work well for grayscale images. In this correspondence, a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local data based on it, and use the statistics to decode the next resolve level.

A. Existing system and challenges

Adaptive filtering can be implemented in the encrypted domain based on the homomorphism properties of a cryptosystem and a composite signal representation method can be used to reduce the size of encrypted data and computation complexity. In joint encryption and data hiding, a part of significant data of a plain signal is encrypted for content protection, and the remaining data are used to carry the additional message for copyright protection. With some buyer–seller protocols, the fingerprint data are embedded into an encrypted version of digital multimedia to ensure that the seller cannot know the buyer's watermarked version while the buyer cannot obtain the original product.

- The pixel positions are shuffled and the pixel values are not masked in the encryption phase.
- We used to reduce the size of encrypted data and computation complexity.

3. Materials and methods

A. Proposed System

A series of pseudorandom (is an algorithm for generating a sequence of numbers that approximates the properties of random numbers) numbers derived from a secret key are used to encrypt the original pixel values. After decomposing the encrypted data into a sub image and several data sets with a multiple-resolution construction, an encoder quantizes the sub image and the Hadamard coefficients of each data set to effectively reduce the data amount. Then, the quantized sub image and coefficients are regarded as a set of bit streams. When having the encoded bit streams and the secret key, a decoder can first obtain an approximate image by decrypting the quantized sub image and then reconstructing the detailed content using the quantized coefficients with the aid of spatial correlation in natural images. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bit streams are received.

B. Advantages

- A channel provider without the knowledge of a cryptographic key and original content may tend to reduce the data amount due to the limited channel resource.
- The original gray image is encrypted by pixel permutation.

4. Result and discussion

The application generates key for the user to create a key (integer number) that will be served as the secret key for both encryption and decryption. The warning alerts the user if key generation by system failed due to unforeseen circumstances.

A. Advantages

- Pixels are converted to bits.
- No attacker can tamper the contents
- Completely unreadable by human
- Pixel values are masked.
- Image content is not altered during the process The images are encrypted so that except the licensed user nobody can distribute or sell the image and also prevents from modification of the image. For example academic websites have figures related to study. So encryption of those images prevents from distribution. The images are secured to maintain confidentiality of important data. For example photos of terrorists should not be available to the public, While uploading and downloading images from sites the images are encrypted to prevent from being manipulated by any third party. Because personal images are always prone to attack by malicious users. The encryption of image prevents users from sharing the pictures from one media to another. For example to prevent the stills of yet to release films might be encrypted to prevent from distribution. In web pages that contain sensitive data, images have to be encrypted. Secret or confidential information has to be shared with a wide variety of people who cannot be predicted, and who may occur singly, or in groups. If a hacker tries to save the contents the contents of the image should become unreadable. Since employee data may include his and his family photos it is important to keep them in encrypted format. So that it benefits the employee as well as the organization. Photos of the recent events or sensitive news may be distributed or be stolen by other sites. So images may be kept encrypted in such scenarios.

5. Conclusion

This paper has proposed a novel scheme of scalable coding for encrypted images. The original image is encrypted by modulo-256 addition with pseudorandom numbers, and the encoded bit streams are made up of a quantized encrypted sub image and the quantized remainders of Hadamard coefficients. The produced output was bit streams. At the receiver side, while the sub image is decrypted to produce an approximate image, the quantized data of Hadamard coefficients can provide more detailed information for image reconstruction. Since the bit streams are generated with a multiple-resolution construction, the principal content with higher resolution can be obtained when more bit streams are received.

References

[1] D. I. G. Amalarethinam and J. S. Geetha, "Image encryption and decryption in public key cryptography based on MR," *2015 International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, 2015, pp. 133-138.