Lossless and Reversible Data Hiding in Image Encryption Using Public-Key Cryptography

Abhinav Singh
NIT Kurukshetra, India.

Ravi Yadav
NIT Kurukshetra, India.

Ashish Chopra
NIT Kurukshetra, India.

Abstract – Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not of itself prevent interference, but denies the intelligible content to a would-be interceptor. Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Businesses use it to protect corporate secrets, government's use it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.

Images are the basic needs to understand anything easily so the protection of images from being misused is really important.

Index Terms – Image encryption, lossless data hiding, Reversible data hiding.

1. INTRODUCTION

Encryption and data hiding are two effective means of data protection in today's world. While the encryption techniques convert plaintext that is the data which needs to be sent is converted into unreadable text. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result. In present times, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption. There are so many different techniques should be used to protect confidential image data from unauthorized access.

2. RELATED WORK

IMAGE ENCRYPTION USING ADVANCED HILL CIPHER ALGORITHM Bibhudendra Acharya Panda suggests efficient method of encryption of image. Proposed AdvHill algorithm is more secure to brute force attacks as compared to original Hill cipher Algorithm is a fast encryption technique which can provide satisfactory results against the normal hill cipher technique. The proposed scheme is resistant against known plaintext attacks.

Improving for Chaotic Image Encryption Algorithm Based on Logistic Map

Ai-hongZhu proposes a new color image encryption algorithm based on Logistic map. Experimental results show this algorithm has low computational complexity, a large key space and good effect on encryption. The original image and the decrypted image have good identity. The encrypted image can resist various attacks.

IMAGE ENCRYPTION USING PIXEL SHUFFLING

Pankesh Bamotra suggests encryption of grayscale images using shuffling of sub-matrices of pixels. The idea is simple yet provides great security. The grayscale image to encrypt is converted into a matrix of grayscale values. Then depending upon level of encryption required the depth of encryption is chosen. Suitably the matrix is divided into sub-matrices which are shuffled in a random-order.

LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED
IMAGES WITH PUBLIC-KEY CRYPTOGRAPHY

Xinpeng Zhang proposes lossless, reversible, and combined data hiding schemes for ciphertext images encrypted by public-key cryptography with probabilistic and homomorphic properties.In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, andthe data-embedding operation does not affect the decryption of original plaintext image.

3. PORPOSED MODELLING

In this paper, a lossless data-hiding scheme for public-key-encrypted images is proposed. There are three parties in the scheme: an image provider, a data hider, and a receiver. With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data hider who does not know the original image can modify the ciphertext pixel values to embed some additional data into the encrypted image by multilayer wet paper coding under a condition that the decrypted values of new and original ciphertext pixel values must be same. When having the encrypted image containing the additional data, a receiver knowing the data-hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. In other words, the embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property. That also means the data embedding does not affect the decryption of the plaintext image. The sketch of lossless data-hiding scheme is shown in Fig. 1.the figure below depicts more clear view of the proposed system.

4. RESULTS AND DISCUSSIONS

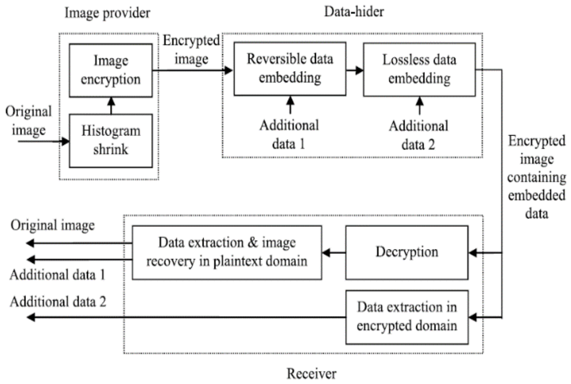

Image Encryption

In this phase, the image provider encrypts a plaintext image using the public key of probabilistic cryptosystem *pk*. For each pixel value *m(i, j)*, where (*i, j*) indicates the pixel position, the image provider calculates its ciphertext value *c(i,j).*

Data Embedding

When having the encrypted image, the data hider may embed some additional data into it in a lossless manner. The pixels in the encrypted image are reorganized as a sequence according

$$c'(i,j) = c(i,j)\cdot(r'(i,j))^{n} \mod n^{2}$$

to the data-hiding key. For each encrypted pixel, the data hider selects a random integer *r _(i, j)* in *Z∗n* and calculates

if Paillier cryptosystem is used for image encryption, while the data hider selects a random integer *r _(i, j)* in *Z∗ns*+1 and calculates

$$c'(i,j) = c(i,j)\cdot(r'(i,j))^{n^{s}} \mod n^{s+1}$$

if Damgård–Jurik cryptosystem is used for image encryption.

Data Extraction and Image Decryption

After receiving an encrypted image containing the additional data, if the receiver knows the data-hiding key, he may calculate the *k*th LSB of encrypted pixels, and then extract the embedded data from the *K* LSB-layers using wet paper coding. On the other hand, if the receiver knows the private key of the used cryptosystem, he may perform decryption to obtain the original plaintext image. When Paillier cryptosystem is used which implies

$$c(i,j) = g^{m(i,j)}\cdot(r(i,j))^{n} + \alpha\cdot n^{2}$$

5. CONCLUSION

This paper proposes lossless, reversible, and combined data hiding schemes for ciphertext images encrypted by public-key cryptography with probabilistic and homomorphic properties. In the lossless scheme, the ciphertext pixel values are replaced with new values for embedding the additional data into the LSB-planes of ciphertext pixels. This way, the embedded data can be directly extracted from the encrypted domain, and the data-embedding operation does not affect the decryption of original plaintext image. In the reversible scheme, a preprocessing of histogram shrink is made before encryption, and a half of ciphertext pixel values are modified for data embedding. On the receiver side, the additional data can be extracted from the plaintext domain, and, although a slight distortion is introduced in decrypted image, the original plaintext image can be recovered without any error.

REFERENCES

[1] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, and A. M. Darwish, "High capacity lossless data embedding technique for palette images based on histogram analysis," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1629–1636, 2010.

[2] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum rate prediction and optimized histograms modification for reversible data hiding," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 653–664, Mar. 2015.

[6] Wikipedia