ISSN: 2321-7782 (Online)
Volume 3, Issue 11, November 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Data Security Using Public Key Cryptography

Bansode Pratik Vishwasrao[1]
B.E (CO)
Dr. D. Y. Patil College Of Engineering
Ambi, Talegaon, Pune, India

Patole LakhanVasant[2]
B.E (CO)
Dr. D. Y. Patil College Of Engineering
Ambi, Talegaon, Pune, India

Suryawanshi Abhay Avinash[3]
B.E (CO)
Dr. D. Y. Patil College Of Engineering
Ambi, Talegaon, Pune, India

Patil Sachin Bhimrao[4]
B.E (CO)
Dr. D. Y. Patil College Of Engineering
Ambi, Talegaon, Pune, India

Prof. Vikas P. Mapari[5]
Dept.Of Computer Engineering
Dr. D. Y. Patil College Of Engineering
Ambi, Talegaon, Pune, India

Abstract: ***In this paper, System uses the cryptography and stegnography concepts which proposes a lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homomorphic properties. In the lossless scheme, the cipher text pixels are replaced with new values to embed the additional data into several LSB-planes of cipher text pixels by multiple layer wet paper coding. Then, 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, the preprocessing is employed to shrink the image histogram before image encryption, so that the modification on encrypted image for data embedding will not cause any pixel oversaturation in plaintext domain. Although a slight distortion is introduced, the embedded data can be extracted and the original image can be recovered from the directly decrypted image. Due to the compatibility between the lossless and reversible schemes, the data embedding operations in the two manners can be simultaneously performed in an encrypted image. With the proposed combined technique, a receiver may extract a part of embedded data before decryption, and extract another part of embedded data and recover the original plaintext image after decryption.***

Keywords: Cryptography, Stenography, LSB-Technology, Data Embedding.

I. INTRODUCTION

Encryption and information hiding are two viable methods for information security. While the encryption procedures change over plaintext content into mixed up cipher text, the information concealing strategies insert extra information into spread media by presenting slight alterations. In some mutilation unsuitable situations, information concealing may be performed with a lossless or reversible way. In spite of the fact that the expressions "lossless" and "reversible" have a same which means in an arrangement of past references, we would recognize them in this work.

We say that information hiding technique is lossless if the display of cover signal containing installed information is same as that of unique cover despite the fact that the spread information has been adjusted for information inserting. For instance, the pixels with the most utilized shading as a part of a palette picture are doled out to some unused shading lists for conveying the extra information, and these files are diverted to the most utilized shading. Thusly, despite the fact that the files of these pixels are modified, the genuine shades of the pixels are kept unaltered. Then again, we say an information concealing system is reversible if the first cover substance can be consummately recouped from the spread rendition containing installed information despite the fact that a slight bending has been presented in information implanting strategy.

Various instruments, for example, distinction extension, histogram shift and lossless pressure, have been utilized to build up the reversible information concealing systems for computerized pictures. As of late, a few decent forecast methodologies and ideal move likelihood under payload-mutilation measure have been acquainted with enhance the execution of reversible information covering up.

II. Related Work

This method offers a promising result and outperforms the former existing methods in terms of the natural scene classification. The method in presented the holistic representation of spatial envelop with a very low dimensionality for representing the scene image. This approach presented an outstanding result in the scene categorization. The method in proposed a new approach for image classification with the receptive field design and the concept of over completeness methodology to achieve a preferable result. As reported in, this method achieved the best classification performance with much lower feature dimensionality compared to that of the former schemes in image classification task. Works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

III. Survey of proposed system

In existing system third user can easily identify the data where is encrypted. Once we perform encryption on image the size of image is also increases. To proposes a lossless, a reversible, and a combined data hiding schemes for cipher text images encrypted by public key cryptosystems with probabilistic and homomorphism properties. Proposed system is as follow:

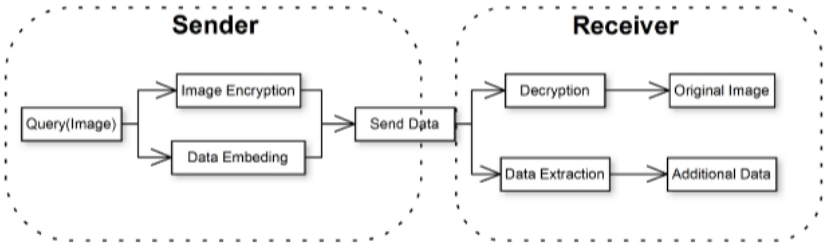

Fig.3.1 System Architecture

IV. Algorithm of Proposed system

Step1: Forbidden Zone Data Hiding (FZDH) simply makes use of FZ to adjust the robustness invisibility trade off.

Step2: Masking is applied to data hiding and watermarking in a number of efforts, as in order to incorporate perceptual analysis, so that perceptually usable host signal samples and permissible distortion margins are determined

Step3: FZDH involves a set partitioning to determine the range of host signal where alteration is allowed.

Step4: FZDH employs a mapping in the AZ, for which quantizer are not the only choice

Step5: In FZDH, initially all regions are forbidden and one decreases these zones according to the desired level of decoding error with respect to a channel noise level.

Step6: FZDH keeps some of the host signal unaltered.

Step7: FZDH approaches to the data hiding problem from a different perspective than coding techniques: there exists uncoded portions of the host signal range.

V. LOSSLESS AND REVERSIBLE SCHEME

A) Lossless Data Hiding Scheme

- 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 multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text 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.
- The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as theoriginal plaintext image due to the probabilistic property

B) Reversible Data Hiding Scheme

- This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider.
- When having the encrypted image, the data-hider modifies the ciphertext pixel values to embed a bit-sequence generated from the additional data and error-correction codes.
- Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side.
- Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image.

C) Combined Data Hiding Scheme

- A lossless and a reversible data hiding schemes for public-key-encrypted images are proposed. In both of the two schemes, the data embedding operations are performed in encrypted domain.
- On the other hand, the data extraction procedures of the two schemes are very different. With the lossless scheme, data embedding does not affect the plaintext content and data extraction is also performed in encrypted domain.
- With the reversible scheme, there is slight distortion in directly decrypted image caused by data embedding, and data extraction and image recovery must be performed in plaintext domain.
- That implies, on receiver side, the additional data embedded by the lossless scheme cannot be extracted after decryption, while the additional data embedded by the reversible scheme cannot extracted before decryption.

VI. CONCLUSION

This paper conclude that, the system uses lossless and reversible technology hence the quality of particular input image is not distorted. Here we used a public key cryptography which gives the more security and privacy to that particular image transmitted from sender to receiver. So the main purpose of using this lossless and reversible scheme is gives the high quality at receiver side and also give the proper security at the time of transmission.

ACKNOWLEDGEMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

References

1. N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.
2. J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.
3. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.
4. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005.
5. X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.
6. X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316−325, 2013.
7. W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.

AUTHOR(S) PROFILE

Bansode Pratik Vishwasrao, pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil College Of Engineering,Ambi,Talegaon, Pune.

Patil Sachin Bhimrao, pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil College Of Engineering,Ambi,Talegaon, Pune.

Suryawanshi Abhay Avinash, pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil College Of Engineering,Ambi,Talegaon, Pune.

Patole Lakhan Vasant, pursuing the B.E degree in Computer Engineering at Dr.D.Y.Patil College Of Engineering,Ambi,Talegaon, Pune.

Vikas P. Mapari, assistant Professor in department of Computer Engineering at Dr. D. Y. Patil College Of Engineering, Ambi, Talegaon, Pune.

