IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

Advanced Information Securing by Combining Fortified Binary Image Steganography and Asymmetric Encryption Standard

Jeyapradha M
Assistant Professor, Department of Computer Applications,
The Standard Fireworks Rajaratnam College for Women, Sivakasi, Tamil Nadu, India

Abstract: *In information security, image steganography is one of the information securing process. Image steganography is mostly used in medical fields for hiding medical prescription data behind the medical images. Designing steganographic algorithms for empirical cover sources, such as digital images, is very perplexing due to the lack of accurate models. The most successful approach today avoids estimating the cover source distribution because this task is infeasible for complex and non-stationary sources. Instead, the steganography problem is formulated as source coding with fidelity constraint the sender entrenches the message with minimizing the distortion. Practical algorithms that entrench near the theoretical payload–distortion bound are available for a very general class of distortion functions. With the current framework, the only task left to the sender is essential for the design of the distortion function. Here information is which wants to be confidential that information's are stored behind the image pixels. However, due to increasing crypt analysis attacks and binary image de stenographic process image steganography has very less security. So improving the security in image steganography process, the current system provide the asymmetric encryption standard for improving more security in steganography.*

Keywords: Steganography, Encryption, Distortion, Information securing

I. INTRODUCTION

The key idea behind the security of steganographic methods is the statistical un-detectability. It may be influenced by many factors, such as the choice of cover object, the type of modification operation on cover elements, the number of embedding changes (related to the payload), and the distortion functions used to recognize individual elements that could be improved during embedding. The factors stated above are the same for designing the distortion function will be an important approach to minimalizing the impact caused by embedding, and thus increase the security performance of steganography.

To reduce the effect caused by data embedding, the sender should pick the modified elements (pixels/coefficients) in such a way that the caused detectable distortion is as small as possible. Embedding the secret message bits under the regulation of minimalizing distortion function can improve the security performance of steganography for a long time. In presented the perturbed quantization (PQ) steganography. As a specific case, they pointed out that the sender can constrain the embedding changes to those DCT coefficients that experience the largest quantization error, i.e., the coefficients with the quantization error of 0.5± (is a small positive number). The coefficients are rounded to the other value, may result the smallest embedding distortion.

However, unless the current model is a complete statistical descriptor of the empirical source, such optimized schemes may, paradoxically, end up being more detectable if the Warden designs the detector “outside of the model”, which brings us back to the main and rather difficult problem modeling the source. All of today’s most secure steganographic schemes for digital images use heuristically defined distortion functions that constrain the embedding changes to those parts of the image that are difficult to model (e.g., complex textures or “noisy” areas).

II. LITERATURE REVIEW

Ashraful Tauhid A et al. in 2019, proposed two prominent techniques to obtain secure communication over the shared media like the Internet. Steganography is slightly ahead of cryptography because of its stealthy characteristics. In this, a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

new method has been proposed which combines cryptography and steganography to ensure even more secure communication. The Advanced Encryption Standard (AES) in spatial domain of the carrier/cover image and Least Significant Bit (LSB) replacement in the transformed domain of the same image has been used after performing a Discrete Cosine Transform (DCT) on the pixels.

Ashish Shetty et al. in 2020, projected a dual image steganography, which plays a significant role in securing secret/sensitive data within two wrapped images, which uses 256-bit AES Encryption for ciphertext using Haar Discrete Wavelet Transform (HDWT) for hiding the data in one of the high-frequency sub-data. It comprise of four bands and has excellent space-frequency localization property, which increases the impalpability and the hiding capacity, while implementing the Huffman Parity Coding Algorithm which acts as a lossless compression method so that the data should not get lost and lose its quality.

M. Senthil Murugan et al. in 2019, proposed the algorithm that is about hiding an audio file into video frame. A video file is chosen first. The video file is then divided into frames. A particular frame is selected and skin tone detection is performed on it using HSV color space model. The skin region is taken as the Region of Interest (ROI). An audio file is the secret message to be transmitted. It is embedded into the frame using Advanced Encryption Standard (AES) algorithm. The secret audio file encrypted on a particular frame is transmitted with a key. The receiver can extract the secret audio file only if he has the key.

Soria-Lorente A et al. in 2017, proposes a novel steganographic method based on the compression standard according to the Joint Photographic Expert Group and an Entropy Thresholding technique. The validation work of the algorithm consists of the calculation of the peak signal-to-noise ratio (PSNR), the difference and correlation distortion metrics, the histogram analysis, and the relative entropy, comparing the same characteristics for the cover and stego image. The proposed algorithm improves the level of imperceptibility analyzed through the PSNR values.

III. PROPOSED SYSTEM

In proposed system, the more advanced encryption standard for more advanced information standard process. Here we first hide the information behind the image by using steganography method. Then we converting the image data into binary image standard for provide the high standard cryptographic system. Here we use Asymmetric encryption standard for high encryption standard.

The scheme minimizes a novel flipping distortion measurement which considers both HVS and statistics. This measurement employs the weighted sum of crmiLTP changes to measure the flippability of a pixel. Further, the weight value corresponding to each crmiLTP is set according to that pattern's sensitivity to the embedding distortion. To estimate the sensitivity, a collection of generalized embedding simulators are organized to yield stego images with different distortion types and strengths. In the embedding phase, STC is employed to minimize the flipping distortion. To remove the unexpected flipping incurred by STC, the concepts of scrambling and superpixels are employed to guarantee that flippable elements occupy the majority in a cover vector.

However, the probability of pixels being "wet" (that is, pixels not suitable for flipping) is high in binary images. As a result, most finding of stego vectors in STC will fail. To deal with this problem, the cover image is divided into non-overlapped blocks first. Then image blocks suitable for embedding message bits are selected and the scrambling suggested is performed across all the selected blocks. Last, these scrambled blocks are further divided into superpixels, which are considered as the elements of cover vectors.

In this regard, the proposed measurement can be considered as the combination of DRD, ELD, and SCD. It simultaneously meets the above-mentioned two criteria, while ELD and SCD ignore the first criterion and DRD ignores the second one. The scrambling employed in both SHUFFLE and the proposed scheme is implemented by using the Matlab function randperm with a randomly selected seed. In all the testing, pseudorandom binary sequences are used as messages.

IV. METHODOLOGY

4.1 Image Steganography

Image steganography is the method of hiding secure information's behind the digital media like images. In the field of information secrecy, it was the high authentic method. In another two adaptive versions of perturbed quantization (PQ) steganography, i.e., texture-adaptive PQ (PQt) and energy-adaptive PQ (PQe) have been presented. Since the texture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

complexity and energy capacity, JPEG steganography with higher security performance can be accomplished. It have joined quantization step with quantization error in their distortion function to improve the security enactment of JPEG steganography. Besides the quantization step, Wang and Ni presented a new JPEG distortion function with consideration of the block entropy, and the experimental results demonstrate that this new distortion function may lead to less detectability of steganalyzers.

4.2 Image to Binary Conversion

The image to binary conversion method will involves for providing a cryptographic standard measures for the image data. In binary conversion module user image data converted into non-understandable binary format. By converting image into binary data, then it can be used for encryption and decryption.

4.3 RSA Cryptography

RSA is grounded on the fact that it is challenging to factorize a large integer. The public key consists of two figures where one number is a addition of two large high figures. And private key is also deduced from the same two high figures. So if notoriety can factorize the large number, the private key is compromised. thus encryption strength completely lies on the crucial size and if we double or triple the crucial size, the strength of encryption increases exponentially which can be illustrated in fig.1

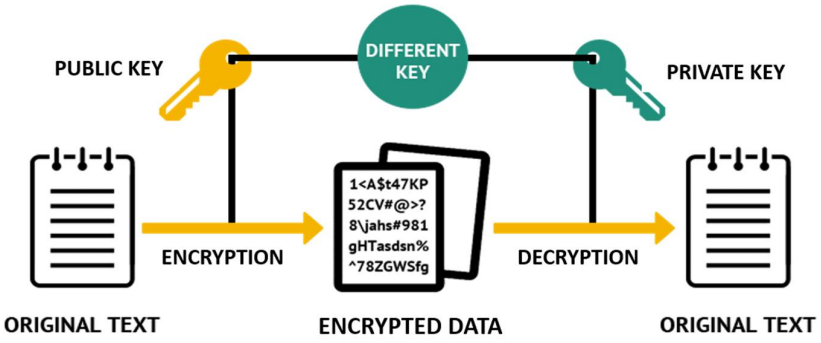

Fig.1. Process of Asymmetric Encryption algorithms

4.4 Key Generation

Need to generate public and private keys before running the functions to generate your ciphertext and plaintext. They use certain variables as follows

Choose two large prime numbers (p and q)

Calculate n = p*q and z = (p-1)(q-1)

Choose a number e where 1 < e < z

Calculate d = e-1mod(p-1)(q-1)

Bundle private key pair as (n,d)

Bundle public key pair as (n,e).

4.5 Asymmetric Encryption and Asymmetric Key Decryption

In asymmetric encryption, use the two types of keys public key and private key. The sender encrypting the message with sender private key and receiver public key. In asymmetric decryption, use the two types of keys public key and private key. The Receiver Decrypt the message with sender public key and receiver Private key

V. CONCLUSION

The system has proposed the more advanced encryption standard for more advanced information standard process. The most successful approach today avoids estimating the cover source distribution because this task is infeasible for complex and highly non-stationary sources. Therefore, the proposed flipping distortion measurement is set with the weighted sum

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, February 2023
Impact Factor: 7.301

of crmiLTP changes, where the weight is empirically assigned according to the discrimination power of the crmiLTP histogram. By comparing with HVS-based approaches, it can be seen that the proposed measurement accomplishes well on both image quality and security.

REFERENCES

[1]. Q. G. Mei, E. K. Wong, and N. D. Memon, "Data hiding in binary text documents," Proc. SPIE, vol. 4314, pp. 369–375, Aug. 2001.

[2]. Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Trans. Commun., vol. 50, no. 8, pp. 1227–1231, Aug. 2002.

[3]. M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," IEEE Trans. Multimedia, vol. 6, no. 4, pp. 528–538, Aug. 2004.

[4]. H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," IEEE Trans. Multimedia, vol. 9, no. 3, pp. 475–486, Apr. 2007.

[5]. H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal data embedding for binary images in morphological transform domain—A high-capacity approach," IEEE Trans. Multimedia, vol. 10, no. 3, pp. 339–351, Apr. 2008.

[6]. M. Guo and H. Zhang, "High capacity data hiding for binary image authentication," in Proc. Int. Conf. Pattern Recognit., Aug. 2010, pp. 1441–1444.

[7]. H. Cao and A. C. Kot, "On establishing edge adaptive grid for bilevel image data hiding," IEEE Trans. Inf. Forensics Security, vol. 8, no. 9, pp. 1508–1518, Sep. 2013.

[8]. F. Huang, W. Luo, J. Huang, and Y. Q. Shi, "Distortion function designing for JPEG steganography with uncompressed side-image," in Proc. 1st ACM Workshop Inf. Hiding Multimedia Security, 2013, pp. 69–76.