Image steganography by homomorphic encryption with hybrid optimization

Marina A. Medvedeva [1], Al-Fariji Ahmed Hussein Hashem [2]

[1]Russia - Ural Federal University / marmed55@yandex.ru

[2]Russia - Ural Federal University / ahmedalfurijiit.109@gmail.com

ABSTRACT:

The image encryption scheme is easily broken by selected plaintext because of the abundance of image information data, high pixel correlation, and high redundancy. In order to improve security and performance, a modern treatment image encryption algorithm that incorporates genetic simulated annealing, particle swarm optimization and improved quantum chaos framework is suggested. Firstly, the key stream is produced using an enhanced quantum chaotic system. Then the plaintext picture is processed using the selection and cross operations of genetic algorithms. The image is scrambled using the ideal sequence created by the simulated annealing process. Furthermore, the simulated annealing method incorporates the hybrid technique. According to the beginning population's ideal fitness value, the starting temperature is determined. Inertial weight variables of hybrid algorithm are improved to prevent particles from slipping into local optimal during the optimization procedure and to speed up the algorithm's convergence. Global optimal position and Individual optimal position generation are optimized using Metropolis.

Keywords: Steganography , optimization, hybrid, key, homomorphic

DOI Number: 10.14704/nq.2022.20.13.NQ88365 Neuro Quantology 2022; 20(13):2930-2935

INTRODUCTION

The security of data has become one of the most crucial aspects of communication and information technology since the advent of the Internet. The purpose of cryptography is to protect the confidentiality of communications, and numerous techniques have been devised to encode and decode data in order to do so. Sadly, there are situations when keeping a message's contents hidden is insufficient and its existence must also be kept secret. Steganography seems to be the method utilised to carry this out [1–5].

Steganography is both the art and science of sending messages that can't be seen. This is done by concealing data in plenty of other information, which hides the fact that the information has been communicated. The word "steganography" comes from Greek words "*stegos*," which means "*cover*," and "*grafia*," which means "writing." This means that "steganography" means "*covered writing*." In image steganography, only images are used to hide the information. For a long time, people have thought about and done things to hide information.

Presently, most steganography is processed electronically, where digital data is used as the carrier and networks are used as rapid delivery channels. Steganography is different from cryptography in that it tries to hide the fact that a message exists, while cryptography tries to hide the message's contents. Steganography [8,13,14] and cryptography both are ways to hide data from users from the third parties, but neither one is ideal and therefore can be broken. Once it is known or even thought that information is there, steganography is no longer as useful [3,6,7,10,36]. Merging steganography with cryptography can make it even more powerful.

Watermarking and finger prints are two other innovations that are very close to steganography [15,42]. The main goal of such technologies is to protect intellectual property, so the requirements for the algorithms are different than for steganography. These are the things

that a good steganographic algorithm needs to do.

In watermarking, every case of an object is "marked" in the same way. When objects are watermarked, they usually have a signature that shows where they came from or who owns them to protect their copyright [41]. Fingerprinting, on the other hand, involves putting distinct, unique marks on each copy of the carrier object that is sold to a broad range of consumers. This lets the person who owns the intellectual property find clients who break their licencing agreement by giving the property to someone else without permission. In fingerprinting and watermarking, the fact that data is hidden within files may well be known to the public and might be visible. In steganography, however, the fact that the data can't be seen is the most important thing. A great attack on a steganographic framework is when an attacker notices that there is data hidden inside a file. On the other hand, a major attack on a fingerprinting or watermarking system would not be to find the mark, but to eliminate it [42].

Most of the work on steganography has been done because cryptographic systems are not strong enough. Many governments have passed laws that either limit how strong a cryptographic system can be or ban it outright [37], which forces people to look into other ways to securely send information. Businesses also have initiated to see how steganography could be used to share trade secrets or information about new products. If you don't talk through well-known channels, data is much less likely to get out while it's being sent [40]. With the discovery of steganography, it became impossible for anyone else to update the information that was being sent. This made transmission of data safer and more reliable.

1.1 Steganography

This word comes from the Greek words Steganós, which means "closed," and Graptos, which means "script," and together they mean "closed script" [30]. Most of the time, it is called "invisible" communication. It means to hide messages that are already in another medium (picture, sound files, video, communication). Today, these schemes use multimedia (image, video, sound file, etc.) as enclose media since people often send digital photos over text or distribute them via other communication apps. It's not the same as making sure the real meaning of a message stays safe. To put it simply, it is like hiding information in other information.

Steganography [19] doesn't change the way a secret message is put together. Instead, it hides it inside a covert object. Later than hiding procedure, stego-object (moving information that has been hidden) and cover object are similar. So, cryptography, which hides data, and steganography, which hides information, are very different. Steganography [16–18] makes it difficult to enhance information without a known process because information is encoded. Steganalysis is a method for finding steganography.

It is a way to get secret information out in any kind of media. It is often confused with cryptography because both are used to protect secret information. The difference between the two is how the output looks. The result of a steganography methodology is not actually visible, while the result of a cryptography procedure is scrambled so that it can be used to draw attention. Steganlysis is the process of finding out if steganography is being used. Pictures are often used as a way to hide information.

1.2.1 Steganography Model

As depicted in Fig. 1.1, a steganographic system typically utilises a coverage file to conceal the original message and a steganography method to conceal the required item. The outcome is a file named stego-file that contains the concealed message. This stego file is subsequently transmitted to the recipient, who obtains the message via de-steganography. The objective of advanced steganography would be to conceal the message [24].

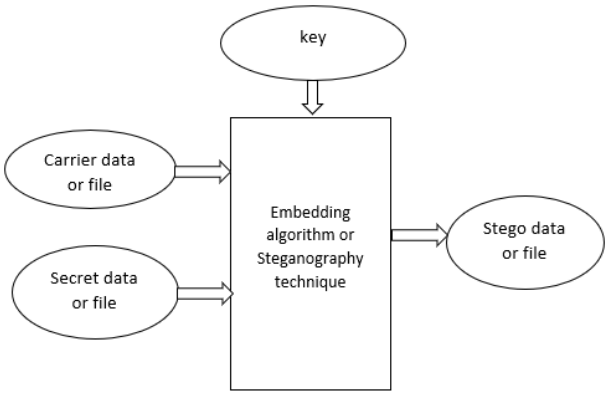


Figure 1.1: Model of Steganography

Subramanian, et.al [1] analyse and explain the various deep learning techniques used in the field of image steganography. CNN -based, general adversarial network-based, and classical methods comprise the three primary categories of deep learning methodologies utilised for image steganography. This paper also includes a detailed overview of the technique, datasets used, experimental setups taken into consideration, and regularly used evaluation criteria.

Lu, et.al [2] present a large-capacity Invertible Steganography Network (ISN). In order to take advantage of the image embedding and extraction issues, designers first describe the forward and backward propagation procedures of a single invertible network using steganography and the retrieval of hidden images as a set of inverse issues on image domain transformations. Designers are capable of effectively create both of the container image and the disclosed hidden image(s) with good quality by sharing all of the parameters of the single ISN architecture.

Pramanik, et.al [3] offer a cutting-edge method of image steganography that has been developed to convey private information using a cover image that generates a stego image. It is difficult for attackers to recover the confidential data using this combinational methodology to image steganography, which making this quite safe for transmitting sensitive data.

Mittal, et.al [4] concentrate on the use of steganography and homomorphic encryption to create safe banking transaction systems. Homomorphic encryption can indeed be utilised for NTRU data encryption, and steganography can be employed to embed a cover image in a QR code to obfuscate information.

Shah & Bichkar [5] present a genetic algorithm-based secret data modification-based high-capacity image steganography technique. To embed the secret data, a new method employs least significant bit (LSB) substitute steganography. Moreover, the hidden information is reorganised and revised before being embedded in the cover image's LSBs. GA controls the variables used to reorganize and update the secret information. A novel concept known as flexible chromosome is presented, allowing GA to define the chromosome value in a variety of ways. GA seeks the highest suitable parameter value that results in high visual quality stego images. The suggested methodology produces stego images with average PSNR values of 40.83 dB and 46.41 dB for 3 bpp data hiding capacity and 2 bit per pixel (bpp), respectively.

Voleti, et.al [6] have a description of what constitutes a decent steganographic algorithm and a short discussion of the best methods that are currently being used. Because ICT has grown, the knowledge is now processed electronically. So, security and privacy have been very important. It can also be used to encrypt messages that are hidden inside a digital host before they are sent to the network, making it hard to know if they exist or not. The way that sensitive data is hidden and encrypted could be used to guard the copyright of interactive media, video, audio, and images.

Ng, et.al [7] propose an enhanced picture steganography that conceals a grayscale secret image behind a grayscale cover image by utilising QR and RDWT decomposition. The proposed approach utilised the human visual system for information concealment. Both the cover picture and the hidden image are separated into identical, non-overlapping image blocks. Every picture block's generated entropy value would be ranked from lowest to highest. The embedding procedure begins with embedding the image block with the lowest entropy value into the image block with the least entropy value. The procedure continues till all image blocks are embedded.

Powar, et.al [8] provides a summary of various image steganography approaches. Every steganographic method has its own unique characteristics and limits. Image steganography enables the concealment of text, images, audio, and video within a cover image. This paper discusses steganography kinds and techniques, such as frequency domain, special domain, masking, spread spectrum, distortion, and filtering.

Shankar, et.al [9] suggested a wavelet-based approach for sharing secret photos with shadow images encrypted using the optimum Homomorphic Encryption (HE) algorithm. Discrete Wavelet Transform (DWT) is initially applied to the hidden image to generate sub bands. This procedure generates numerous shadows, which are then encrypted and

decrypted individually. The encrypted shadow can be reconstructed by selecting a subset of these 'n' shadows that are transparent and stack on top of one another. To increase the security of shadows, every shade is encoded and decrypted using the HE algorithm. For image quality concerns, the new Oppositional-based Harmony Search (OHS) algorithm was used to generate the best key.

PROPOSED APPROACH

A wavelet is a tiny wave (In Fourier analysis, longer-period waves, also known as sinusoids, are utilised). Or to put it another way, a wavelet is an oscillation that rapidly decreases [39,44,45]. The wavelet has the ability to simultaneously provide information about time and frequency. The family of functions serves as the foundation for wavelets. The mother wavelet, from which the smaller wavelets are created, serves as the primary function. The procedure of translation and dilations on the primary function known as the "mother wavelet" is used to create smaller wavelets ψ(t). The following equation defines them:

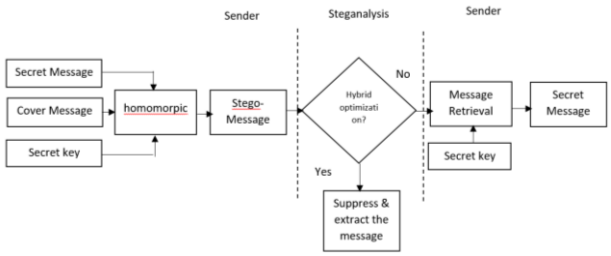
$$\varphi(t) = \frac{1}{\sqrt{c}}\varphi\left(\frac{t-d}{c}\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots (1.9)$$

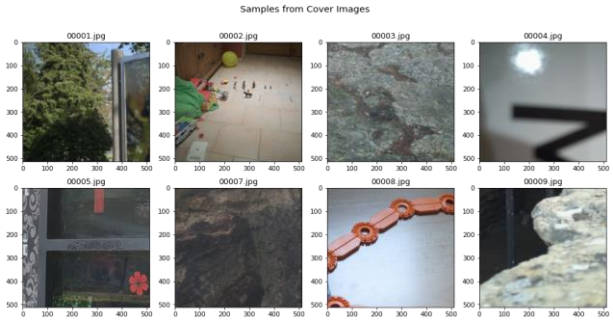
$$c, d \in R, c \neq 0$$

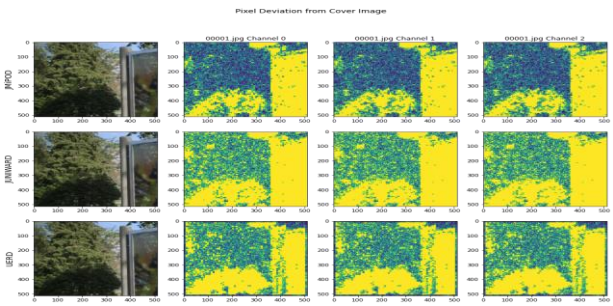
Where 'd' is the time-location shifting of a signal, 'c' seems to be the scaling factor that describes the degree or extent of compression. If the value of |c| is less than one, then the signal is in compressed form. If |c| is greater than one, then the wave $\varphi_{c,d}$ (t) has expanded with a longer time period but lower frequency than the mother wavelet $\varphi(t)$. If $\varphi(t)$ possesses 2n samples, she can produce n generations. Multiple fields such as Image Processing in JPEG 2000, Tide Forecasting, and Underwater Sonar analysis are used in wavelet applications in the real world [32].

- **Continuous Wavelet Transform:** The continuous wavelet transform (CWT) is indeed an alternative to the discrete wavelet transform (DWT) for overcoming resolution problems. The CWT separates a function that is continuous in time into wavelets. It is carried out in a manner similar to the STFT. It accurately depicts the signal or function in terms of time and frequency localization. Its analysis and synthesis [22] necessitate extensive computer processing. Therefore, the implementation of DWT, which really is easier and more effective, has begun.
- **Discrete wavelet transforms:** The DWT provides a potent algorithm for image processing [28]. Thus, DWT steganography become prevalent in the field of information concealment [33]. In STFT, the presence of a spectral component can only be determined for a specified time interval and not for a specific point in time.

Steganography is a form of secure transmission, and steganalysis is the process of finding steganographic buried communications in digital data. The media and law enforcement have paid a lot of attention to steganalysis and steganography. Numerous effective and reliable steganalysis and steganography techniques have recently been disclosed in the literature. In this study, we categorise and describe the numerous steganalysis methodologies that have been put forth. Additionally, some interesting techniques for quantitative steganalysis have indeed been found.







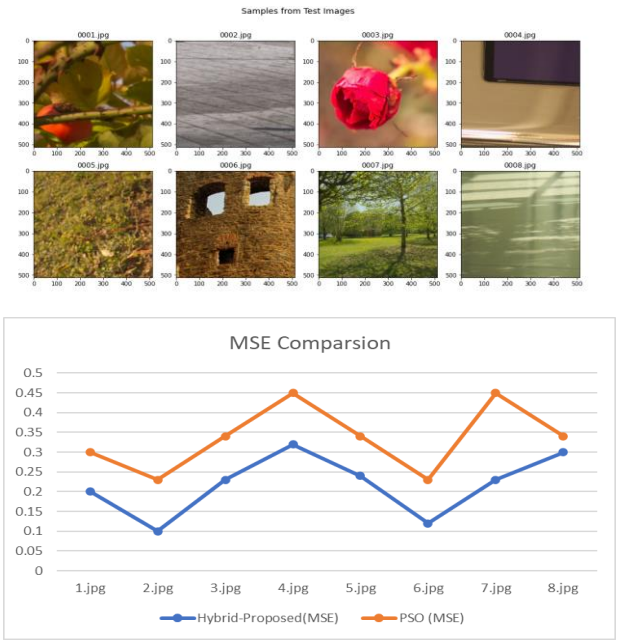


Figure 1.1: Comparison of MSE

The MSE-based comparison is explained in terms of PSO(MSE) and Hybrid-Proposed in Figure 1.1. (MSE). MSE assesses how much error is present in statistical models. At 1.jpg, the PSO (MSE) has an MSE of 0.3; at 2.jpg, the MSE acquired is approximately 0.23; at 3.jpg, the MSE acquired is around 0.34; and at 4.jpg, the MSE acquired is 0.45. (max). The MSE is then derived in a decreasing order starting with 5.jpg, where it is 0.34, continuing to 6.jpg, where it is 0.23, and so on. In contrast, the hybrid-proposed (MSE) has lower MSE values than the PSO(MSE), for example, at 1.jpg, it has an MSE of 0.2, which is significantly lower than the PSO at 1.jpg. The MSE found at 4.jpg is approximately 0.32, which is lower than the 0.45 (for PSO) at 4.jpg. The MSE achieved at 6.jpg is roughly 0.13, and so forth. This demonstrates that the Hybrid-Proposed (MSE) outperforms the PSO (MSE).

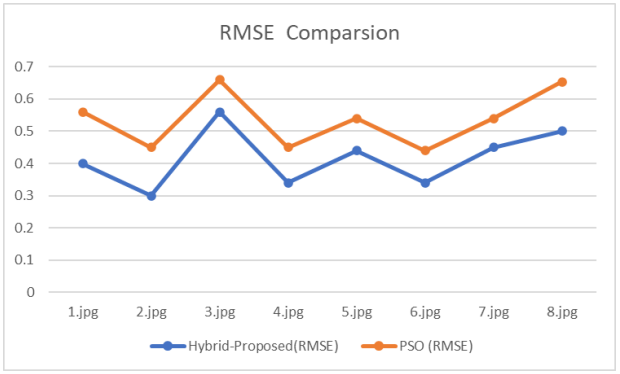


Figure 1.2: Comparison of RMSE

Figure 1.2 shows the RMSE-based comparison between the PSO(RMSE) and Hybrid-Proposed (RMSE) approaches. RMSE assesses the accuracy of image reconstruction by calculating the pixel-by-pixel difference between the original and reconstructed images. At 1.jpg, the PSO (RMSE) has an RMSE of 0.58, at 2.jpg, it is around 0.45, at 3.jpg, it is approximately 0.65, and at 4.jpg, it is approximately 0.45. At 5.jpg, the RMSE is 0.52, then at 6.jpg, the MSE is approximately 0.45, and so on. In contrast, the hybrid-proposed (RMSE) has lower RMSE values than PSO(RMSE); for example, at 1.jpg, it has an RMSE of 0.4, which is significantly less than the PSO at 1.jpg. At 4.jpg, the RMSE is approximately 0.35, which is less than 0.45 (for PSO) at 4.jpg. The RMSE for 6.jpg is approximately 0.35, and so on. This indicates that the Hybrid-Proposed (RMSE) works better than PSO (RMSE).

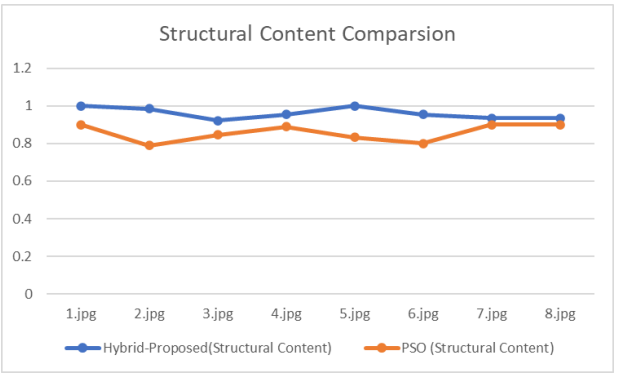


Figure 1.3: Comparison of Structural Content

Figure 1.3 provides a comparison of the structural content of the PSO and Hybrid-Proposed methods. The structural content values of Hybrid-Proposed approaches are close to or equivalent to 1 when compared to structural content values of PSO approaches, showing a favourable response of the proposed method in comparison to other current methods.

CONCLUSION

This paper offers an optimum multi-key homomorphic encryption with steganography approach for hybrid homomorphic methodology for environment. Principally, the singular value decomposition (SVD) paradigm is used to separate cover images into RGB components. In addition, a coyote optimization algorithm (COA) is used for the optimal pixel selection procedure. Concurrently, hidden

images are encrypted with poor and rich optimization (PRO) and multikey homomorphic encryption (MKHE) techniques with hybrid optimization . Finally, the cypher picture is placed within the selected pixel values of cover image to produce stego image. Numerous experiments were conducted in order to evaluate the successful results of proposed suggested model is superior to the rennet techniques in terms of several metrics.

REFRENCES

1. Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE access*, *9*, 23409-23423.
2. Lu, S. P., Wang, R., Zhong, T., & Rosin, P. L. (2021). Large-capacity image steganography based on invertible neural networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 10816-10825).
3. Pramanik, S., Samanta, D., Bandyopadhyay, S. K., & Ghosh, R. (2021). A new combinational technique in image steganography. *International Journal of Information Security and Privacy (IJISP)*, *15*(3), 48-64.
4. Mittal, S., Kaur, P., & Ramkumar, K. R. (2021, September). Achieving Privacy and Security Using QR-Code through Homomorphic Encryption and Steganography. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1-6). IEEE.
5. Shah, P. D., & Bichkar, R. S. (2021). Secret data modification-based image steganography technique using genetic algorithm having a flexible chromosome structure. *Engineering Science and Technology, an International Journal*, *24*(3), 782-794.
6. Voleti, L., Balajee, R. M., Vallepu, S. K., Bayoju, K., & Srinivas, D. (2021, March). A secure image steganography using improved LSB technique and Vigenere cipher algorithm. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)* (pp. 1005-1010). IEEE.
7. Ng, K. H., Liew, S. C., & Ernawan, F. (2020, February). An improved image steganography scheme based on RDWT and QR decomposition. In *IOP Conference Series: Materials Science and Engineering* (Vol. 769, No. 1, p. 012069). IOP Publishing.
8. Powar, S. K., Dinde, H. T., & Patil, R. M. (2020). A Study and Literature Review on Various Image Steganography Techniques.
9. Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., & Yuan, X. (2020). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. *Journal of Ambient Intelligence and Humanized Computing*, *11*(5), 1821-1833.
10. Pramanik, S., Singh, R. P., & Ghosh, R. (2020). Application of bi-orthogonal wavelet transform and genetic algorithm in image steganography. *Multimedia Tools and Applications*, *79*(25), 17463-17482.
11. Duan, X., Liu, N., Gou, M., Wang, W., & Qin, C. (2020). SteganoCNN: image steganography with generalization ability based on convolutional neural network. *Entropy*, *22*(10), 1140.
12. Yin, S., Liu, J., & Teng, L. (2020). Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. *Int. J. Netw. Secur.*, *22*(3), 419-424.
13. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.
14. Wu, X. (2019). An algorithm for reversible information hiding of encrypted medical images in homomorphic encrypted domain. *Discrete & Continuous Dynamical Systems-S*, *12*(4&5), 1441.
15. Zou, Y., Zhang, G., & Liu, L. (2019). Research on image steganography analysis based on deep learning. *Journal of Visual Communication and Image Representation*, *60*, 266-275.