International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13233-13240
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Reversible Data Hiding scheme using modified Histogram Shifting in Encrypted Images for Bio-medical images

Arunkumar S, Subramaniyaswamy V*, Sivaramakrishnan N
School of computing, SASTRA Deemed University, Thanjavur.
*Corresponding Author

Abstract

Existing Least Significant Bit (LSB) steganography system is less robust and the stego-images can be corrupted easily by attackers. To overcome these problems Reversible data hiding (RDH) techniques are used. RDH is an efficient way of embedding confidential message into a cover image. Histogram expansion and histogram shifting are effective techniques in reversible data hiding. The embedded message and cover images can be extracted without any distortion. The proposed system focuses on implementation of RDH techniques for hiding data in encrypted bio-medical images without any loss. In the proposed techniques the bio-medical data are embedded into cover images by reversible data hiding technique. Histogram expansion and histogram shifting have been used to extract cover image and bio- medical data. Each pixel is encrypted by public key of Paillier cryptosystem algorithm. The homomorphic multiplication is used to expand the histogram of the image in encrypted domain. The histogram shifting is done based on the homomorphic addition and adjacent pixel difference in the encrypted domain. The message is embedded into the host image pixel difference. On receiving encrypted image with additional data, the receiver using his private key performs decryption. As a result, due to histogram expansion and histogram shifting embedded message and the host image can be recovered perfectly. The embedding rate is increased in host image than in existing scheme due to adjacency pixel difference.

Key words : Steganography, Image encryption, Image decryption, Reversible data hiding

1.Introduction:

Data Security means maintaining the privacy of data. In order to provide data security, the technique of steganography was introduced. Steganography is a technique which hides one piece of data within another. It is a best method of secret communication when compare to Encryption, Digital Signatures since it maintains confidentiality, integrity and availability of data. It is an advanced method of cryptography where the structure of the message is not altered.

Figure 1 explains that a cover image (original image) along with the message is encrypted with encryption key and decrypted by using decryption key to get the cover image and message exactly. There are many types of steganography such as text, image, audio, video and so on. But in this article we focused on image steganography which means embedding data in an image.

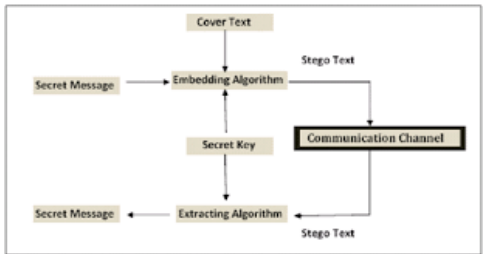


Figure 1 : Basic Steganography model

Image Steganography is widely used to secure private files and documents, hide passwords and encryption keys, transport highly private document between international governments,etc. There are many versions of steganography techniques in spatial domain methods like least significant bit(LSB) and so on. These techniques have problems like less image restoration property.

Reversible Data Hiding techniques such

as histogram expansion and histogram shifting are used to embed the message into image. Histogram expansion which is used to hide the data inside the image, by means of expanding the histogram of that image to make space for the data to be placed, each pixel gets doubled in the range of 0 to 255. On expansion spacing capacity of data to be inserted is increased. Histogram shifting is a technique which works by compute difference image, generate histogram bins for expansion then embedding and finally modification of pixels [17-25]. The benefits of using histogram shifting are better recovery image, less destruction ratio and high embedding capacity.

Homomorphic encryption which performs action on encrypted text and can check without decryption where the result will be same as that of the given original text. In that many Partially homomorphic cryptosystem is present that may be either homomorphic addition or multiplication [26-35]. To enforce more security, these algorithms like RSA and Paillier are used. Here, RSA is a multiplication and the Paillier is an addition homomorphism. These algorithms perform on their own homomorphic property which ensures the exact recovery of cover image on decryption [35-41].

The purpose of this article is to restore the image exactly on decryption and to keep hidden data secured. This is a system where Reversible Data Hiding(RDH) technique is used along with public-key encryption to keep the image in encrypted domain where RDH means restoring image and message as if it was sent. The main advantage of this article is that it ensures lossless data hiding and image is kept safely.

In this article, we implement lossless data hiding technique using modified histogram shifting method for embedding patient details into DICOM image so that on decryption, image and patients can be recovered perfectly. The Radiologist gathers the patient details and the scan report. Those details are sent to the Steganographer by Radiologist. Then the Steganographer hide the patient details in the scan report and encrypt using public key which is made to be stored in DBserver. Finally, the end user on decryption using private key access the embedded data and DICOM image is as shown in the Figure 2

Remainder of the article is organised as follows, Section 2 gives the detailed literature survey, section 3 elaborates our proposed methodology and section 4 provides result and analysis of our proposed method and finally section 5 gives conclusion of our work.

2. Literature Review:

In Reversible data embedding, information is hidden in a digital image while decode the hidden information and original image will be restore[1]. In Novel pixel-based PVO(PPVO), sort the content of the pixels by predicting the pixels. It is used for data embedding [2].Alattar's method with location map concept improves the quality of the image embedded and provides payload of higher capacity[3]. Histogram shifting modulation which adaptively takes care of the local specifications of the image content[4].

The histogram shifting of reversible data hiding compresses codes of BTC increases the embedding capacity of secret data into image [5]. In medical images, there is a possibility of hiding the important data in a particular image and recovery of original image is easy[6].The encryption system and water marking provides authentication for the data transmission of a dependent key transformation. The security of the dependent key system is increased[7].The diffusion strategy in a random manner is used to hide the data. By the prediction of data embedding it improves the pixel measures [8].

Improves the measurement of block smoothness and further it decreases the rate of error of the bit extracted [9]. The encrypted image holds the hidden data and on decryption the respective image and the hidden data is recovered perfectly by using the encryption key[10].Asymmetric Encryption Algorithm (AES) is an example of Bench-mark encryption algorithm is used to concentrate on the remaining pixels of the image also used to encrypt estimated errors occurred. Thus, it

cannot guarantee to access the original image with perfection[11].The proposed RDH algorithm provides a best solution to achieve exact original image and the secret data [12].

The hidden data is embedded in the encrypted image without data expansion is the principle of designing the homomorphic cryptosystem. In addition, histogram shifting algorithm provides a real reversibility [13]. Encrypted image-based reversible data hiding (EIRDH) is same as the existing RDH techniques. But only difference the data is embedded in the encrypted domain [14].The cipher text pixel values include new data into least significant bit in order to providing the lossless data scheme [15]. Composite Residuosity Class Problem of public key cryptography is solved by additive homomorphic property of Pascal Paillier cryptosystem [16].

3.Methodology and Approach

We begin by extracting the pixels of DICOM image. Further, by introducing the histogram expansion, the pixel of the image is doubled by copying those pixel to its neighbouring pixel location. Each pixel and its corresponding copy of those pixel value and the message are encrypted by Paillier and RSA algorithms separately. Then the message is embedded into the encrypted image. As a result, an intermediate DICOM image is produced and is stored in the DB server. The end user access the encrypted image from the server and decrypt the image using private key to secure from unauthorized persons. Finally, the end user retrieve the original image and the hidden data. In this concept, Paillier algorithm performs histogram shifting to embed the message bits securely. Along with this, the multiplicative homomorphism of RSA algorithm enables the image to recover exactly. This concept ensures the lossless data hiding into the image.

STEPS TO BE FOLLOWED:

This article is mainly focused on medical application by hiding message in a medical image and is properly retrieved by the authorized person.

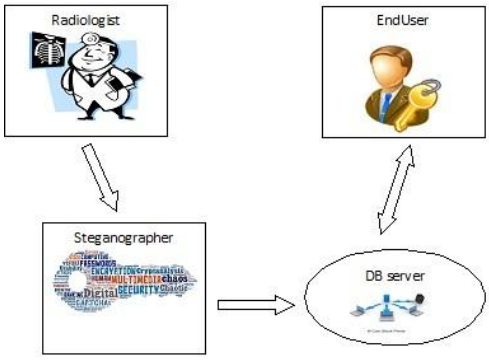


Figure 2 :Architecture of lossless data hiding and recovery

Step 1: Pixel Extraction

Take a DICOM image as an input image. DICOM means Digital Imaging and Communication in Medicine where we can store, print, transfer information in medicine. First step is to extract the pixels from DICOM image and finally generate the histogram for the input image.

Step 2: Expansion

After extracting those pixel values from the image, double the pixel values by copying those pixel to its neighbouring pixel location. This process holds the histogram expansion by which we can embed the message along with pixel of the image. This mechanism provides space for embedding data in the image.

Step 3: Encryption (sender side)

Further, embedding the data, each pixel and its corresponding copy of those pixel value and the message are encrypted by Paillier and RSA algorithms separately as in Figure 3. Here Paillier is a homomorphic addition which performs histogram shifting to embed the message bits securely whereas RSA performs

multiplication which enables the receiver to recover the image exactly.

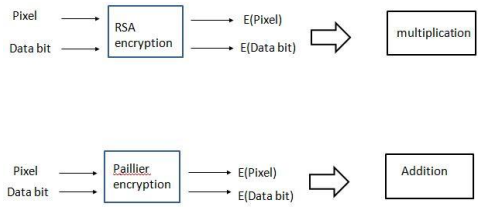


Figure 3 Server side encryption

Step 4: Generate intermediate image

After encryption, generate an intermediate (encrypted) image which is entirely different from the source image, retrieve the pixel values from the image and finally generate the histogram for the intermediate image.

Step 5: Decryption (Receiver side)

At last on the receiver side , encrypted image is decrypted using private key to secure from third person, also the exact image and data retrieved as if it was send and finally generate the histogram for the decrypted image. The Figure 3 and 4 merge to prove the homomorphic property.

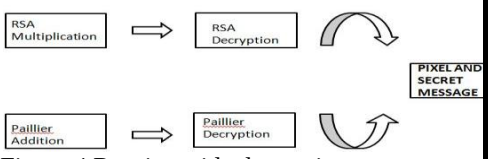
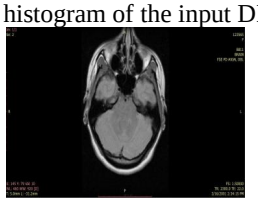


Figure 4 Receiver side decryption

4. Experimental Results

Doctor takes a patience medical image as shown in Fig 5 as a plain image and inferences from them as secret data. Figure 6 shows the histogram of the input DICOM image.



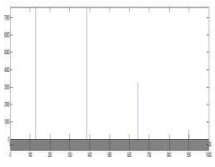
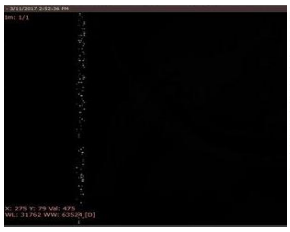


Figure 5 Input Image Figure 6 Input

The input image is subjected to encryption by histogram expansion and then secret data is embedded into it by means of histogram shifting as explained by the above steps. Fig 7 shows the encrypted image and fig 8 shows the histogram of the encrypted image.



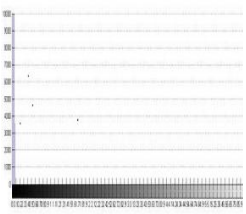
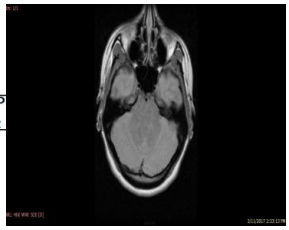


Figure 7 Encrypted Figure 8 Encrypted

Decryption is done on the Fig 7 as explained by the above method. Fig 9 shows the recovered original image and Fig 10 shows the histogram of the recovered image. Fig 6 and Fig 10 shows the same bin values for each pixel values of the input image and recovered image. From this, it is concluded that original image is recovered without any loss.



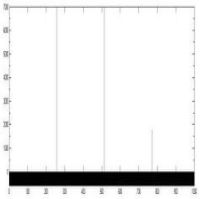


Figure 9 Output Image Figure 10 Output Histogram

5.Conclusion

Histogram shifting of the encrypted images and Reversible Data Hiding is achieved by histogram shifting using homomorphic properties. Data is embedded in a image to protect it from the unauthorized user. Data is expanded and encryption is done by RSA and Paillier algorithms. Embedded data and exact image is recovered easily. This article provides high security to the data and lossless image recovery after decryption. Comparing with

various available algorithms using homomorphic property it provides high security for the end user who access the data and the image without any loss and high authentication. Therefore, it can be applied across different applications such as hospital management system, military security and so on.

References:

[1] Tian, Jun. "Reversible data embedding using a difference expansion." IEEE transactions on circuits and systems for video technology 13.8 (2003): 890-896.

[2] Qu, Xiaochao, and Hyoung Joong Kim. "Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding." Signal Processing 111 (2015): 249-260.

[3] Hsiao, Ju-Yuan, Ke-Fan Chan, and J. Morris Chang. "Block-based reversible data embedding." Signal Processing 89.4 (2009): 556-569.

[4] Coatrieux, Gouenou, et al. "Reversible watermarking based on invariant image classification and dynamic histogram shifting." IEEE Transactions on Information forensics and security 8.1 (2013): 111-120.

[5] Chang, I-Cheng, et al. "High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding." Signal Processing 108 (2015): 376-388.

[6] Wu, Hao-Tian, Jiwu Huang, and Yun-Qing Shi. "A reversible data hiding method with contrast enhancement for medical images." Journal of Visual Communication and Image Representation 31 (2015): 146-153.

[7] Cancellaro, Michela, et al. "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain." Signal Processing: Image Communication 26.1 (2011): 1-12.

[8] Li, Ming, et al. "A modified reversible data hiding in encrypted images using random diffusion and accurate prediction." ETRI Journal 36.2 (2014): 325-328.

[9] Hong, Wien, Tung-Shou Chen, and Han-Yan Wu. "An improved reversible data hiding in encrypted images using side match." IEEE Signal Processing Letters 19.4 (2012): 199-202.

[10] Zhang, Xinpeng. "Reversible data hiding in encrypted image." IEEE signal processing letters 18.4 (2011): 255-258.

[11] Zhang, Weiming, Kede Ma, and Nenghai Yu. "Reversibility improved data hiding in encrypted images." Signal Processing 94 (2014): 118-127.

[12] Ma, Kede, et al. "Reversible data hiding in encrypted images by reserving room before encryption." IEEE Transactions on information forensics and security 8.3 (2013): 553-562.

[13] Li, Ming, et al. "Reversible data hiding in encrypted images using cross division and additive homomorphism." Signal Processing: Image Communication 39 (2015): 234-248.

[14] Chen, Yu-Chi, Chih-Wei Shiu, and Gwoboa Horng. "Encrypted signal-based reversible data hiding with public key cryptosystem." Journal of Visual Communication and Image Representation 25.5 (2014): 1164-1170.

[15] Zhang, Xinpeng, et al. "Lossless and reversible data hiding in encrypted images with public-key cryptography." IEEE Transactions on Circuits and Systems for Video Technology 26.9 (2016): 1622-1631.

[16] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 1999.

[17] Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Gao, X. Z., & Indragandhi, V. (2017). A hybrid quantum-induced swarm intelligence clustering for the urban trip recommendation in smart city. Future Generation Computer Systems, 83, 653-673.

[18] Subramaniyaswamy, V., & Logesh, R. (2017). Adaptive KNN based Recommender System through Mining of User Preferences. Wireless Personal Communications, 97(2), 2229-2247.

[19] Logesh, R., & Subramaniyaswamy, V. (2017). A Reliable Point of Interest Recommendation based on Trust Relevancy between Users. Wireless Personal Communications, 97(2), 2751-2780.

[20] Logesh, R., & Subramaniyaswamy, V. (2017). Learning Recency and Inferring Associations in Location Based Social Network for Emotion Induced Point-of-Interest

Recommendation. Journal of Information Science & Engineering, 33(6), 1629–1647.
[21] Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment Analysis of Tweets for Estimating Criticality and Security of Events. Journal of Organizational and End User Computing (JOEUC), 29(4), 51-71.
[22] Indragandhi, V., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Siarry, P., & Uden, L. (2018). Multi-objective optimization and energy management in renewable based AC/DC microgrid. Computers & Electrical Engineering.
[23] Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2018). An ontology-driven personalized food recommendation in IoT-based healthcare system. The Journal of Supercomputing, 1-33.
[24] Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2018). Hybrid Transform based Adaptive Steganography Scheme using Support Vector Machine for Cloud Storage. Cluster Computing.
[25] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Resources, configurations, and soft computing techniques for power management and control of PV/wind hybrid system. Renewable and Sustainable Energy Reviews, 69, 129-143.
[26] Ravi, L., & Vairavasundaram, S. (2016). A collaborative location based travel recommendation system through enhanced rating prediction for the group of users. Computational intelligence and neuroscience, 2016, Article ID: 1291358.
[27] Logesh, R., Subramaniyaswamy, V., Malathi, D., Senthilselvan, N., Sasikumar, A., & Saravanan, P. (2017). Dynamic particle swarm optimization for personalized recommender system based on electroencephalography feedback. Biomedical Research, 28(13), 5646-5650.
[28] Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., & Logesh, R. (2018). Meta-data based secret image sharing application for different sized biomedical images. Biomedical Research, 29.
[29] Vairavasundaram, S., Varadharajan, V., Vairavasundaram, I., & Ravi, L. (2015). Data mining-based tag recommendation system: an overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 5(3), 87-112.
[30] Logesh, R., Subramaniyaswamy, V., & Vijayakumar, V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. Electronic Government, an International Journal, 14(1), 90-113.
[31] Vijayakumar, V., Subramaniyaswamy, V., Logesh, R., & Sivapathi, A. (2018). Effective Knowledge Based Recommeder System for Tailored Multiple Point of Interest Recommendation. International Journal of Web Portals.
[32] Subramaniyaswamy, V., Logesh, R., & Indragandhi, V. (2018). Intelligent sports commentary recommendation system for individual cricket players. International Journal of Advanced Intelligence Paradigms, 10(1-2), 103-117.
[33] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Topological review and analysis of DC-DC boost converters. Journal of Engineering Science and Technology, 12 (6), 1541–1567.
[34] Saravanan, P., Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2017). Enhanced web caching using bloom filter for local area networks. International Journal of Mechanical Engineering and Technology, 8(8), 211-217.
[35] Arunkumar, S., Subramaniyaswamy, V., Devika, R., & Logesh, R. (2017). Generating visually meaningful encrypted image using image splitting technique. International Journal of Mechanical Engineering and Technology, 8(8), 361–368.
[36] Subramaniyaswamy, V., Logesh, R., Chandrashekhar, M., Challa, A., & Vijayakumar, V. (2017). A personalised movie recommendation system based on collaborative filtering. International Journal of High Performance Computing and Networking, 10(1-2), 54-63.
[37] Senthilselvan, N., Udaya Sree, N., Medini, T., Subhakari Mounika, G., Subramaniyaswamy, V., Sivaramakrishnan, N., & Logesh, R. (2017). Keyword-aware recommender system based on

user demographic attributes. International Journal of Mechanical Engineering and Technology, 8(8), 1466-1476.
[38] Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated Message Filtering System in Online Social Network. Procedia Computer Science, 50, 466-475.
[39] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Unstructured data analysis on big data using map reduce. Procedia Computer Science, 50, 456-465.
[40] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Intelligent travel recommendation system by mining attributes from community contributed photos. Procedia Computer Science, 50, 447-455.
[41]Vairavasundaram, S., & Logesh, R. (2017). Applying Semantic Relations for Automatic Topic Ontology Construction. Developments and Trends in Intelligent Technologies and Smart Systems, 48.