Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

Embedding Image in Medical Images

Sayeedakhanum Pathan[1], Dr. Savadam Balaji[2]

Research Scholar, KoneruLakshmaiah Education Foundation, Hyderabad[1]
Professor, KoneruLakshmaiah Education Foundation, Hyderabad[2]
pathan.sayeeda@klh.edu.in[1], balajis@klh.edu.in[2]

Abstract

In recent years, telemedicine has been a preferred technique for hospitals. A doctor in one hospital may request more opinion from other doctors residing in any corner of the globe with the help of real-time transmission of medical image data. The location integration process plays a critical role here in medical applications. This causes the amount of space in the digital hospital database to be decreased. The two basic needs of an integration and retrieval system are invisibility and robustness. The main objective of this work is to make a suitable trade-off between the perceptual form of the embedded image and its effectiveness against different distortions. For this result, this paper examines two different embedding techniques in the complex contourlet transformation (CCT) domain. One is fusion based optimised embedding, and secondly, distributed spectrum based optimised embedding. Both of these approaches direct the robustness of embedding.

Keywords: medical image, cryptography, embedding, retrieving, security, digital, contourlet*;*

1. Introduction

1.1 IMAGE EMBEDDING TECHNIQUE

In confidential communication two methods are available for information security: cryptography and steganography. Cryptography is an ability in which information is scrambled so that, without a hidden key, unauthorised users can not extract the secret message (Channalli& Jadhav 2009, Aprajita& Ajay Rana 2013). As a covered script, steganography originated from Greek and traditionally means hiding in plain vision (Singla&Syal 2012). Anyone could discover that in cryptography, all parties interact secretly. However in steganography, the cover media containing hidden data would not be suspected at all by hackers. Hidden data such as a text file, an image file, an audio file, or a movie file may be inserted into a cover medium. In this job, two abilities are adopted. Three distinct aspects of the modern method of steganography are capability, safety (imperceptibility) and robustness (Sahraeian et al. 2008). Agriculture is an innovative idea focusing on the enhancement of agricultural development in rural areas [3]. It is essential to build security solutions by adopting a Security Framework for any organization to find solutions for majority of vulnerabilities and flaws [4].

Secure data transmission is the fundamental need for the users of internet community [6]. Generally speaking, there is a fundamental balance in all steganographic systems between capability and protection. In steganography, two types of methods are sometimes applied. One is based on the primary spatial domain, and the other is based on the domain of transformation. The most well-known steganographic technique in the spatial domain is Least- Significant-Bits (LSB) substitution (Gupta 2011), in particular. This technique is simple and fast, but, such as

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

JPEG compression, it is poor in robustness and compression (Juneja&Sandhu 2013). Since human eyes are not prone to small alterations in noisy data, it will not be detected when a hidden message is replaced with data in noisy regions. In the original domain-Bit-Plane Complexity Segmentation Steganography (BPCS) (Rudramath&Madki 2012), this is another well-known procedure. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Contourlet Transform (Do &Vetterli 2005) are also divided into the transform domain[36][38]. Many individuals trust that biometric frameworks can identify liveness in biometric tests [2][6][16][17][36].

Embedding's primary uses are to provide the degree of certainty of a document's authenticity or ownership (Sunesh& Harish Kumar 2011). The primary difficult issue in realistic implementation is embedding attacks. It has the ability to detach, discover and analyse, write or redo practical embedding bits for unauthorised users. "Assault" thus renders many of the existing algorithms ineffective, so invisible watermarks are designed to be imperceptible (Ashish&Bhadauria 2006). Invisible watermarks are therefore designed to be imperceptible. Therefore, embedding protection is linked to the secret key. To kill the algorithm, both the algorithm and the hidden security key should be known. We have performed fingerprint matching in two steps: i) point-wise match and ii) trim false matches with arithmetical constraints [1][11][12][13].

2. Existing System

2.1 Embedded Attacks

Four types of attacks are included in one categorization of the large class of current attacks: elimination attacks, geometric attacks, cryptographic attacks, and protocol attacks. We define these four forms of attack coarsely here and give some examples. (Voloshynovskiy 2001 &Hartung et al. 1999) can be found in more detailed explanations.

2.1.1 Removal Attacks

The goal of removal attacks is to delete the watermark information from the watermarked data completely without breaking the security of the watermarking algorithm, e.g. without the key used for embedding the watermark. That is, the watermark information from the pushed data can not be retrieved by any amount of processing, even prohibitively complex (Jayanthi et al. 2013). Denoising, quantization (e.g. for compression), demodulation, and collusion attacks are part of this group. Not all of these systems occasionally come close to their intention of simple extraction of watermarks; still they can significantly destroy the message of the watermark. Sophisticated removal attacks aim to optimise operations such as denoising or quantization in order to as often as possible impair the embedded watermark while keeping the consistency of the attacked document high enough. Under such a condition, transforming the information from the transmitter to the receiver requires more security.[7].

Usually, logical representations within the optimization are used for the watermark and the underlying data. Collision attacks are applicable when an attacker or a group of attackers can obtain several copies of a given data set, each signed with a key or different watermark. In such a scenario, by averaging all copies or taking only small sections from each separate text, a successful attack can be accomplished. Recent findings show that a small number of different copies in one attacker's hand, e.g. around 10, can lead to effective removal of watermarks.

2.1.2 Geometric Attacks

Geometric attacks do not remove the embedded watermark itself, unlike removal attacks, but attempt to distort the synchronisation of the watermark detector with the embedded details. When perfect synchronisation is restored, the detector can recover the embedded watermark information. However to be realistic, the complexity of the required synchronisation process may

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

be too high. The most well-known benchmarking software, Unzign and Stirmark, combine a number of geometric attacks for image watermarking. Unzign suggests confined pixel jittering and is useful in targeting designs for spatial domain watermarking. Stirmark incorporates geometric distortions that are global as well as local. However, owing to the use of precise synchronisation strategies, most novel watermarking methods survive these attacks.

Global geometric distortion robustness often depends on the use of either a transform invariant domain (Fourier-Mellin) or an additional template or specially built periodic watermarks that enable geometric distortion estimation with the Auto Covariance Function (ACF). The attacker can however, build dedicated attacks that exploit synchronisation scheme information. More or less, robustness to global affine transformations is a solved problem. However for most commercial watermarking instruments, resistance to the local random alterations incorporated with Stirmark remains an open issue. The so-called random bending attack in Stirmark takes advantage of the fact that the human visual system is not vulnerable to economic changes and is affine.

Alterations. Therefore without substantial optical distortion, pixels are locally modified, scaled, and rotated. It is worth noting, however, that some of the latest techniques can resist this attack.

2.1.3 Cryptographic Attacks

Recent years have seen a growing awareness of the need to improve information security [9]. Cryptographic attacks aim to break down authentication techniques in watermarking systems and thus find a way to delete information about embedded watermarks or to embed misleading watermarks. The brute-force search for embedded secret knowledge is one such strategy. The so-called Oracle attack, which can be used to generate a non-watermarked sign when a watermark indicator mechanism is available, is another attack in this section. Practically, because of their high computational complexity, the implementation of these attacks is limited.

2.1.4 Protocol Attacks

Protocol attacks are aimed at attacking the whole premise of the intent of watermarking. The design of invertible watermarks is based on one sort of protocol attack (Craver et al. 1997). The idea behind transposition is that from the watermarked data and rights, the spoiler deducts his/her watermark to be the owner of the watermarked data. It may create confusion about the exact possession of the details. It has been decided that watermarks need to be non-invertible for copyright protection purposes. The terms of the non-invertibility of watermarking technologies suggest that the removal of a watermark from a non-watermarked text should not be feasible. To make watermarks signal-dependent by practising one-way purposes is a clarification of this difficult intensity.

The copy assault is a separate protocol attack. In this state, the purpose is not to abolish or destroy the visibility of the watermark, but to evaluate and copy a watermark from watermarked data to some other data, called destination data. To achieve its imperceptibility, the computed watermark is adapted to the local peculiarities of the target data. The assault on copies is applicable when the original watermark may provide a non-algorithmic understanding of the watermarking technology or knowledge of the watermarking key in the target data. Again the force of signal-dependent watermarks is contrary to the copy attack.

3. Proposed System

3.1 PROPOSED MULTIMODAL MEDICAL IMAGE EMBEDDING USING OPTIMIZATION TECHNIQUE

The Updated Grey Wolf Optimization (MGWO) technique is the novel optimization used in the proposed process. Complex contourlet transformation is initially used to decompose the cover image and DCT is used to divide the images into blocks, then the clustering of k-means is used to separate the edges of the block. Edge preservation and directionality are thus the primary

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

property of Complex Contourlet Transform (CCT). RPM and TLA processing provide final results which are undoubtedly visible for health practitioner reviews for pre and post or even during surgical activities [10]. Therefore, after the edge separation in the blocks, the technique of grey wolf optimization is used to check for space by using the clustering centre k-means as the initial population (i.e.) to explore the misaligned edges in the block for more hiding potential and embedding for less time consumption. High hiding ability is the key benefit of the proposed image embedding techniques; sufficient space saves, less time consumption that enhances PSNR and MSE. As shown in Figure 4.1, the block diagram of the proposed scheme.

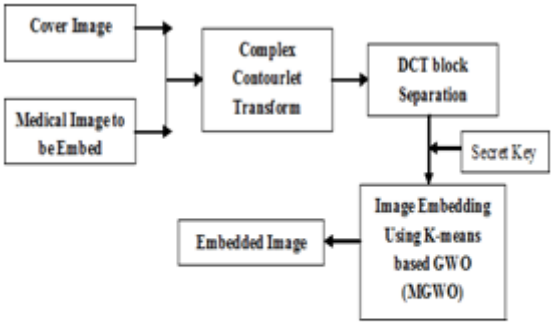

Figure 4.1 Block Diagram of Proposed Optimization Technique Based Image Embedding

5. Conclusion

Parameters such as Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) in the CCT domain are used to record the effects of image embedding. By measuring Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE), it is evaluated with different attacks and it is concluded from the study that the image embedding process using MGWO in the CCT domain provides better values than the other techniques. The suggested method of image embedding used for telemedicine applications that use MGWO in the CCT domain is therefore more accurate. It has the main features of high embedding capacity, imperceptibility (transparency, invisibility), attack robustness is less when it is transmitted for diagnosis. High PSNR 94.02816, minimum MSE 2.5e-06, broad embedding power, and less time consumption ~9 sec. are the important benefits of the proposed image embedding algorithm.

References

[1] Sahithi, S., Anirudh, A., Swaroop, B., Ruth Ramya, K. Biometric security for cloud data using fingerprint and palm print 2019 International Journal of Innovative Technology and Exploring Engineering863383432https://www.scopus.com/inward/record.url?eid=2s2.085069451595&partnerID=40&md5=6a4102e306106fd16731338b23028bd9

[2] Tarannum, A., Rahman, M.D. Multi-modal biometric system using Iris, Face and fingerprint images for high-security application 2019 International Journal of Recent Technology and Engineering 76314320 https://www.scopus.com/inward/record.url?eid=2-s2.085067962719&partnerID=40&md5=b1b1c2acd0ee967c767d7a35cad52cbc

[3] Puvvada, N., Prasad Babu, M.S.Semantic web based banana expert system 2018 International Journal of Mechanical and Production Engineering Research and Development 833643713 https://www.scopus.com/inward/record.url?eid=2-s2.085062992172&partnerID=40&md5=3579f6c1ea568fcc5ab66dc77cdd7dd1

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

[4] Veerapanenic, S.S., Raja Sekhar, K. A systematic study of asset management using hybrid cyber security maturity model 2019 International Journal of Recent Technology and Engineering 76678683https://www.scopus.com/inward/record.url?eid=2s2.085065160274&partnerID=40&md5=ab47677f05cff6ca9f2834f94c41ac1e

[5] Aparna, Puvvadi; Kishore, PolurieVenkata Vijay Biometric-based efficient medical image watermarking in E-healthcare application IET IMAGE PROCESSING FEB 28 2019 13 3 421 428 10.1049/iet-ipr.2018.52886

[6] Sahu, Aditya Kumar; Swain, Gandharba Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis INTERNATIONAL JOURNAL OF ELECTRONIC SECURITY AND DIGITAL FORENSICS 2019 114458476 10.1504/IJESDF.2019.102567

[7] Biometric-based efficient medical image watermarking in E-healthcare application Aparna, P; Kishore, PVV IET IMAGE PROCESSING FEB 28 2019 10.1049/iet-ipr.2018.528864

[8] Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks Pradhan, A; Sekhar, KR; Swain, G SECURITY AND COMMUNICATION NETWORKS 2017 10.1155/2017/19246184

[9] A Dependency analysis for Information Security and Risk Management Krishna, BC; Subrahmanyam, K; Kim, THE INTERNATIONAL JOURNAL OF SECURITY AND ITS APPLICATIONS AUG 2015 10.14257/ijsia.2015.9.8.17

[10] Bangare, Sunil L.; Pradeepini, G.; Patil, Shrishailappa: a new computational technique for precise medical imaging INTERNATIONAL JOURNAL OF BIOMEDICAL ENGINEERING AND TECHNOLOGY 2018 27 1-2 76 85

[11] Yang, X.S., 2012, September. “Flower pollination algorithm for global optimization.” In International conference on unconventional computing and natural computation” (pp. 240-249). Springer, Berlin, Heidelberg.

[12] Jena, S. R., Lavanya, D. R., &Gadde, S. S. (2017). “Minimization of execution time over cloud computing environment using fuzzy technique.” Journal of Advanced Research in Dynamical and

Control Systems, 9(Special Issue 18)

[13] Phanikumar, V., &Satyanarayana, K. V. V. (2017). “Advanced data sharing and group scheduling procedure for dynamic resource allocation of cloud computing”. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 6), 396-409.

[14] Rathod, S. B., & Reddy, V. K. (2017). “Dynamic framework for secure VM migration over cloud computing”. Journal of Information Processing Systems, 13(3), 476-490. Doi:10.3745/JIPS.01.0015

[15] Krishna, P.V., . “Honey bee behaviour inspired load balancing of tasks in cloud computing environments”. Applied Soft Computing”, 13(5), pp.2292-2303.

[16] Jena, S. R., Lavanya, D. R., &Gadde, S. S. (2017). “Minimization of execution time over cloud computing environment using fuzzy technique.” Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 18) Retrieved from www.scopus.com

[17] Siva NageswaraRao, G., &Srinivasu, S. V. N. (2017). “Hybrid approach for task scheduling in heterogeneous cloud based systems”. Journal of Advanced Research in Dynamical and Control Systems

[18] Raghav, rs; amudhavel, j; dhavachelvan,P, “Enhanced artificial bee colony optimization for solving economic load dispatch” iioab journal 2017 1 994238

Potluri, S., &Rao, K. S. (2017). [19] SirishaPotluri,KattaSubbaRao ,”Quality of

service based task scheduling algorithms in cloud computing". International Journal of Electrical and Computer Engineering, 7(2), Vol. 7, No. 2, April 2017, pp. 1088~1095.

[20] Praveen, SP; Rao, KT; Janakiramaiah, B "Effective Allocation of Resources and Task Scheduling in Cloud Environment using Social Group Optimization" Arabian journal for science and engineering AUG 2018 10.1007/s13369- 017-2926

[21] Lavanya, K; Reddy, LSS; Reddy, BE, "Distributed Based Serial Regression Multiple Imputation for High Dimensional Multivariate Data in Multicore Environment of Cloud" international journal of ambient computing and intelligence apr-jun 2019 10.4018/IJACI.20190401051

[22] Dey, NS; Gunasekhar, T "A Comprehensive Survey of Load Balancing Strategies Using Hadoop Queue Scheduling and Virtual Machine Migration", IEEE ACCESS 2019 10.1109/ACCESS.2019.2927076A

[23] Babu, K.R., Samuel, P, "Enhanced bee colony algorithm for efficient load balancing and scheduling in cloud". In: Innovations in Bio-Inspired Computing and Applications, pp. 67–78. Springer,New York (2016).

[24] Nagesh P, Srinivasu N, Ranganadh N" Optimal vm placement using particle swarm optimization", et al. International Journal of Scientific and Technology Research (2020)

[25] Akhila B, Srinivasu N, Varalakshmi A, et al. "Energy efficient scheduling of virtual machines in cloud data center",International Journal of Recent Technology and Engineering (2019)

[26] SumitGangwal, Dr. V P Singh, 08-10-2015, International Conference on Soft Computing Techniques & Implementation, ICSTI 2015 IEEE, Faridabad, India, "Intrusion detection system using machine learning models".

[27] Radhika Rani Chintala, NarasingaRao M R, SomuVenkateswarlu, IJPAM, 2015, "Implementation & Performance Analysis of Security in Human Sensor Networks".

[28] Chintala R R, Narasingarao M R, Venkateswarlu S, IJET (UAE), 2018, "Review on the Security issues in Human Sensor Networks for Health Care Applications".

[29] Leena A Deshpande, M R NarasingaRao, Journal of Engineering Science and Technology, 2019,"Addressing Social Popularity in Twitter Data Using Drift Detection Technique".

[30] K Swetha, M R NarasingaRao, Asian Journal of Information Technology, 2016, "Dynamic Searchable Encryption over Distributed Cloud Storage"

[31] A Seenu, M R Narasingarao, U S SPadmajyothi, International Journal of Advance Research in Computer Science, 2014, "A System for Personal Information Management Using an Efficient Multidimesional Fuzzy Search".

[32] GaikwadKiran P, Dr. C M Sheela Rani, International Journal of Scientific & Technology Research, 2020, "Regression Model with Modified Linear Discriminant Analysis Features for Bimodel Emotion Recognition".

[33] Mr.PrashantMininathMane, Dr. C M Sheela Rani, IJPAM, 2018, "Triple Data Encryption Algorithm based Multiple Authority Access Control in Cloud System Using Optional Threshold".

[34] D V Manasa, M R NarasingaRao, A S Lalitha, International Journal of Applied Engineering and Research, 2014, "Analyzing the Services and Privacy Conflict Resolutions of Shared Data in OSNs".

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 3922 - 3928
Received 25 April 2021; Accepted 08 May 2021.

[35] SwathiKarkarlapudi, M R NarasingaRao, International Journal of Science and Advanced Technology, 2011, “A Novel Facial Recognition Model Using an Artificial Neural Networks”.
[36]Kshirsagar PR, Akojwar SG, R. Dhanoriya, “Classification of ECG-signals using Artificial Neural
Networks”, https://www.researchgate.net/publication/317102153_Classification_of_ECGsignals_using_Artificial_Neural_Networks, International Conference on Electrical, Computer and Communication Technologies. 2017 .
[37] P. Kshirsagar and S. Akojwar, "Classification & Detection of Neurological Disorders using ICA & AR as Feature Extractor", *Int. J. Ser. Eng. Sci. IJSES*, vol. 1, no. 1, Jan. 2015.