

Medical color image concealing for IoMT services

Salwa Mohammed Nijrs

Directorate of Private University Education

Ministry of Higher Education

Baghdad

Iraq

Abstract

Steganography (or Data Concealing, Data Masking, or Data Hiding) is the art of concealing information within other data, structures, or media to avoid detection or access by unauthorized users. Various domains and contexts can be used to hide data. By hiding sensitive data, you can prevent unauthorized access, tampering, or theft, protect your privacy, or even protect your intellectual property. Using images as cover media is the most effective method of steganography. A new method based on the modified technique described by the authors for grayscale images is presented in this manuscript for comparing the color images performance. Data can be hidden in color images by blocking them. Our calculation of the detail coefficients of the secret image uses an approximation of the blue, green, and red components of the cover image. As an alternative to block coefficients, we substitute approximation coefficients for root mean square errors. The best matching blocks are stored using a key. A single image hides a large amount of data, so the work is expected to be successful. A better peak signal-to-noise ratio is provided by Stego Medical Image (StMdIg).

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Stego medical image (StMdIg), Image concealing.*

1. Introduction

Data distribution has become easier and more affordable thanks to the Internet and multimedia processing technologies. With multimedia processing techniques, the data can be edited well with almost no loss. As a result, protecting sensitive data is a major concern. Several techniques that protect sensitive data can be implemented to resolve the problem. A significant amount of attention has been paid to digital steganography

E-mail: salwamn@uomisan.edu.iq

among them. Steganography, also known as digital cloaking, is a technique for obscuring secret data within carrier data for undetectable purposes. Embedding secret data in medical images, audio recordings, videos, and other files is possible[1][2].

Research communities are particularly interested in the use of digital medical images, since they are low bandwidth [3]. A digital image can be steganographic in two ways: spatially and frequency-wise. When the first method is used, the secret data is embedded in the pixels with the lowest significance. Spatial domains are mostly represented using least significant bits (LSBs). PVD and histogram shifting are also well-known techniques. Easy understanding and implementation are the main advantages of these techniques. Image-processing attacks can, however, compromise these systems[4][5].

The authors have proposed a similar study on grayscale medical images [9,10], but this manuscript intends to use color images. Blocking and secret key computation are two new concepts introduced in this study[16][6]. With the blocking concept, a secret medical image may be minimized in impact by embedding it within a cover color image. Neither the cover nor the secret medical images have overlapping blocks[8][1]. A cover color medical image consists of three planes embedded within a secret medical image block. For each plane block in the images of the secret and cover, the secret key computation procedure stores the address of the block with the least error[3][11]. Testing and comparing the proposed color medical image steganography with other recently proposed techniques has been conducted on a variety of medical images. The 2nd Section contains related works that relate to the rest of the manuscript. Steganography of images is presented in the 3rd Section using DWT. An explanation of the experiment's results can be found in the 4th Section. The 5th Section introduces the conclusions[7][2].

2. Related Works

There are numerous methods of watermarking images in the literature, which are categorized by their domain of insertion (spatial, frequent, multiple resolution, etc.). Different image representation spaces have different performance capabilities [12]. Consideration of the insertion domain is crucial when designing watermarking systems. Adding spatial data to an image is possible directly by modifying the pixel values. Real-time watermarking applications can be implemented using this domain due to its quick insertion and detection operations. It is however evident that the visual quality of the image deteriorates after integrating it. Attacks

can be easily mounted using these techniques. Frequency domain insertion can be accomplished by inserting the mark into the transformed domain rather than directly into the image. Frequency representations of images are obtained via DFT or DCT. One of the most challenging aspects of this type of scheme is choosing the coefficients to mark[13]. Best schemes offer a good compromise between robustness and invisibility by avoiding low frequencies and inserting them in the middle frequencies of an image. Inserting the mark at high frequencies would avoid compression or noise addition. While this domain is invariant to translations and scalings, it is unreliable and time-consuming for windowing and small local deformations. In spite of being translation- and scaling-invariant, this domain is unreliable and time-consuming for windowing and small local deformations[15]. As a result of this method, a low-frequency component is isolated from the other components of an image, which constitutes a less sensitive insertion space. Despite the multi-resolution transformation, however, the mark can still be located after it has been transformed spatially[6][16]. In Mohti & al. [18], visual cryptography and Wavelet Packet Transforms are combined. According to Anand & al. [19], medical images can be watermarked with a variety of watermarks. Watermarks are embedded in images and text. Devi & al [20][17] combine DWT and SVD to create a blind watermarking scheme [18][11, 14][19].

3. Steganography Technique for Modified Color Images

This manuscript evaluates traditional steganography with color images by modifying it. Decomposition of the secret image and the cover image is also carried out using DWT. In addition to embedding, an extraction procedure is followed. Detailed descriptions of these procedures can be found below[19].

3.1 *A Process for Embedding*

Embedding is illustrated by the block diagram below. The planes of color cover images can generally be divided into three bands groups; (R-band, G-band, and B-band) as shown in Figure 1. A number of coefficients are used to multiply the three color planes, including the approximate, horizontal, and vertical detail coefficients, as well as the diagonal detail coefficients[20]. Four coefficients are calculated for approximated details, horizontal details, vertical details, and diagonal details. Coefficients with this value do not overlap. Color planes are the

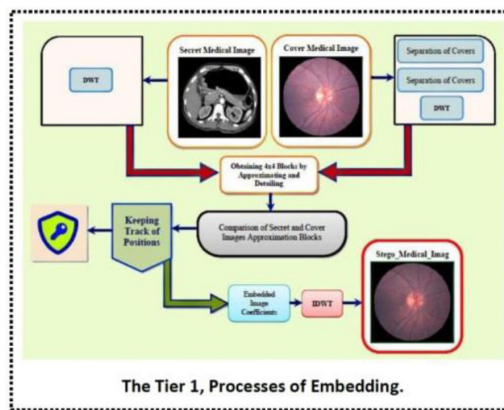


Figure 1

Tier (1), Process Proposed for Embedding

same on the cover images and secret images. Cover image now shows secret blocks instead of detail coefficient blocks. In order to obtain the StMdIg, one approximates and modifies the detail coefficients. Embedding is explained in detail below[18][20]:

(1) A secret image (S) can be read and a cover image (C) can be seen. Three planes can be distinguished between R, G, and B. Three planes can be distinguished between R, G, and B. (2) The RGB components of C are transformed with DWT. (3) Apply the blocking process to approximate C and S planes' R, G, and B planes. Using a 4x4 pixel grid, the approximation coefficients are decomposed. (4) Delete detail coefficients from the C plane's R. The coefficients are divided into four pixels by four pixels each. (5) The R plane of C has been blocked. The decomposition of pixels into coefficients is done pixel by pixel. (6) Blocking is done on C's B plane for detail coefficients. Each block of coefficients is composed of four pixels. (7) A block-by-block (BSA) image corresponds to R, G, and B of C. This image matches blocks based on root mean square error. There are three planes that hold the position of a minimum error block. Using Key K1, we store the blocks that are closest to each other. (8) C's R, G, and B planes should be approximated by a secret image. (9) An IDWT is used to pass a modified coefficient of the C plane. This process results in the StMdIg.

3.2 The Extraction Processing

This figure illustrates the extraction procedure through a block diagram as shown in Figure 2. In StMdIg, there are three color planes. By using DWT, four coefficients are derived from the three color planes. Each

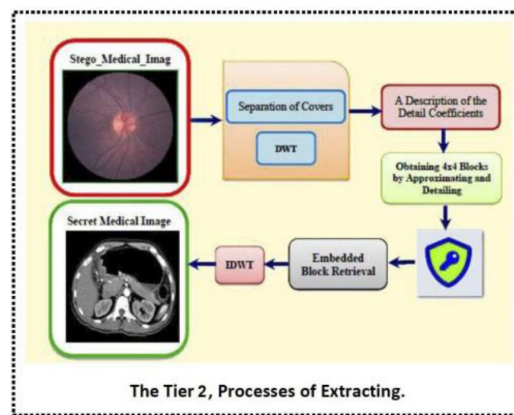


Figure 2

Tier (2), The Proposed Extraction Process

coefficient's blocks are not overlapped. By using detailed coefficients, the best-matching blocks are extracted. Extracting blocks creates secret images. The following instructions provide detailed information about extraction[21][7]: (1) Three color planes are defined for the StMdIg: R, G, and B. (2) On every color plane of StMdIg, R, G, and B, it should be processed using DWT. (3) The StMdIg's R, G, and B detail coefficients should be blocked. A block of 4x4 pixels is used to decompose all of these coefficients. (4) Based on the embedded blocks in K1 Key, a secret image approximation was derived. (5) IDWT applied to approximation blocks can be used to extract a secret image from StMdIg. From StMdIg, we get the secret image[22][4].

4. An Evaluation of the Performance

For the purpose of evaluating the effectiveness of the presented technique, a variation of cover images, as well as secret images, are used. Four new steganography techniques are evaluated in our experiments.

4.1 Utilized Images

A grayscale secret image and a color cover image are used to evaluate the proposed approach's performance. Color images of the retina, Knee, Cervix, and Throat are shown. The cover images can be seen in Figure 3. Chest and Brain are the secret images[23]. These images are 256x256 pixels in size. In Figure 4, you can see the secret images. These two-color images contained images of the Chest and Brain. Using the proposed technique,

the StMdIgs shown in Figures 3 and 4 were embedded with the Chest and Brain secret images. StMdIg displays good visual quality as shown in Figures 5 and 6 [3].

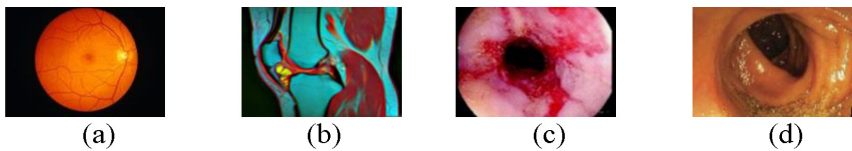


Figure 3

Image Source: Original Cover Image: (a) Retina Image, (b) Knee Image, (c) Cervix Image, and (d) Throat Image

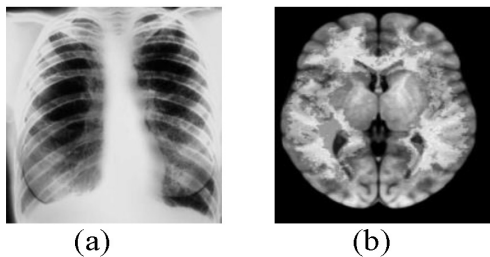


Figure 4

Image Source: Original Secret Image: (A) Chest Image, (B) Brain Image

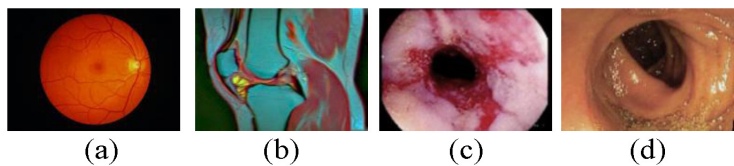


Figure 5

Chest Image Embedded, (a) Retina Image, (b) Knee Image, (c) Cervix Image, and (d) Throat Image

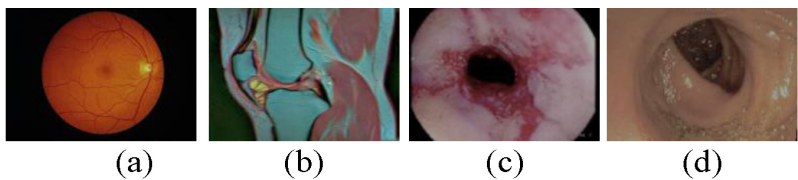


Figure 6

Brain Image Embedded in, (a) Retina Image, (b) Knee Image, (c) Cervix Image, and (d) Throat Image

4.2 Comparing algorithms

A comparison is conducted between this approach and five other popular steganography techniques, among them the DCT and DWT-based approaches [13], the smart pixels-based approaches [25, 26], PVD-based approaches, and the block-overlapping schemes based on PVD [20]. Every technique uses color images, and all have been tested. StMdIg and the extracted secret image are measured with PSNR[24].

5. Findings and Discussion

In this study, a PSNR analysis is performed on StMdIg and the secret images extracted from it. After encoding Chest and Brain as secret images, the StMdIgs PSNR values are shown in Table 1 and Table 2. Comparing experimental results between the proposed approach and the other four techniques developed recently, the presented approach provides a higher PSNR. Contrary to other approaches, the proposed approach embeds the secret image easily into the cover image's matched detail wavelet coefficient blocks. A high PSNR further confirms that the embedded image shows the least distortion during embedding based on the presented approach. Using the presented approach, it is proposed that the StMdIg be improved. The PSNR values for the extracted Chest and Brain images can be compared in Tables 3 and 4. PSNR values for the presented approach are higher than those of existing approaches based on the results. Moreover, the results indicate that the presented approach is relatively imperceptible.

Table 1
StMdIg PSNR values with Chest as a secret image

Cover images	DWT-Based Technique	Smart Pixel-Based Steganography	Steganography Based on PVD	Block-Overlapping PVD Steganography	Proposed
Retina	28.6762	29.0115	29.4013	29.8585	30.1671
Knee	34.8749	33.9431	34.9724	35.0539	35.1318
Cervix	25.4772	26.4449	26.6897	27.0288	27.7771
Throat	32.7636	33.0894	33.8681	33.9027	34.5086

Table 2
StMdIg PSNR values with Brain as a secret image.

Cover images	DWT-Based Technique	Smart Pixel-Based Steganography	Steganography Based on PVD	Block-Overlapping PVD Steganography	Proposed
Retina	28.8769	29.755	29.9888	30.8681	31.702
Knee	36.4949	36.5845	36.5883	36.6579	36.7935
Cervix	28.7445	28.8732	28.8953	29.0903	29.5911
Throat	34.1238	34.7317	35.0322	35.0668	35.7043

Table 3
The PSNR values of the medical image of the Chest that has been extracted.

Cover images	DWT-Based Technique	Smart Pixel-Based Steganography	Steganography Based on PVD	Block-Overlapping PVD Steganography	Proposed
Retina	12.4305	13.1272	13.5187	13.7521	13.9324
Knee	12.1239	12.4701	12.459	12.5283	12.6452
Cervix	12.8452	13.0238	13.3388	13.7321	14.4044
Throat	12.3534	12.4329	12.4332	12.4359	12.4379

Table 4
The PSNR values of the medical image of the Brain that has been extracted.

Cover images	DWT-Based Technique	Smart Pixel-Based Steganography	Steganography Based on PVD	Block-Overlapping PVD Steganography	Proposed
Retina	12.6328	13.7394	14.2583	14.5902	15.6111
Knee	12.368	12.8514	13.2617	13.7495	14.3499
Cervix	12.6027	12.5718	12.6045	12.6077	12.6089
Throat	13.2226	13.6521	14.0006	14.425	14.7197

Conclusions

Color image steganography is performed through modifications of the DWT-based approach. Computations using blocking and secret keys

are used in this approach. Using the least variation concept, the blocking concept is used. Calculated using the least error match criteria and the detail coefficient of the DWT, this secret key consists of 11 bits. According to the modified approach, StMdlg and secret images provide better PSNR than the original images. Our visual quality is improved as a result of it. In addition, the secret image is not required to be extracted using this approach.

References

- [1] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan, Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication, in: *Future Gener. Comput. Syst.*, Elsevier, 2018, <http://dx.doi.org/10.1016/j.future.2018.02.023>.
- [2] K. Rakesh, V. Parthasarathy, Secure fuzzy extractor based biometric key authentication scheme for body sensor network in internet of medical things, *Comput. Commun.* (2020) <http://dx.doi.org/10.1016/j.comcom.2020.01.077>.
- [3] Jigna. J, T. Sudeep, An exhaustive survey on security and privacy issues in Healthcare 4.0, *Comput. Commun.* (2020) <http://dx.doi.org/10.1016/j.comcom.2020.02.018>.
- [4] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, F. Titouna, A privacy-preserving cryptosystem for IoT e-healthcare, *Inform. Sci.* 527, 493–510 (2020).
- [5] J.A. Kaw, N.A. Loan, S.A. Parah, K. Muhammad, J.A. Sheikh, G.M. Bhat, A reversible and secure patient information hiding system for IoT driven e-health, *Int. J. Inf. Manage.* (2018) <http://dx.doi.org/10.1016/j.ijinfomgt.2018.09.008>.
- [6] T.C. Lu, C.Y. Tseng, J.H. Wu, Dual imaging-based reversible hiding technique using LSB matching, *Signal Process* 108, 77–89 (2015).
- [7] T.C. Lu, J.H. Wu, C.C. Huang, Dual-image-based reversible data hiding method using center folding strategy, *Signal Process* 15, 195–213 (2015).
- [8] S. Shastri, V. Thanikaiselvan, Dual image reversible data hiding using trinary assignment and centre folding strategy with low distortion, *J. Vis. Commun. Image R.* (2019) <http://dx.doi.org/10.1016/j.jvcir.2019.03.022>.

- [9] L.P. Chi, C.H. Wu, H.P. Chang, Reversible data hiding in dual stegano-image using an improved center folding strategy, *Multimed. Tools Appl.* 77, 8785–8803 (2018). <http://dx.doi.org/10.1007/s11042-017-4774>.
- [10] K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera and A. Mohand, Multiple watermarking technique for securing online social network contents using back propagation neural network, *J. Future Gen. Comput. Syst.* 25 (2016).
- [11] United States Department of Health and Human Services, HIPAA: Medical Privacy – National Standards to Protect the Privacy of Personal Health Information, Available at <http://www.hhs.gov/ocr/hipaa/>.
- [12] Zear, A. K. Singh and P. Kumar, A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine, *Multimed. Tools Appl.*, 1–20 (2016).
- [13] S. Kaihara, Realisation of the computerised patient record; relevance and unsolved problems, *Int. J. Med. Inform.* 49 (1998), 1–8.
- [14] H. K. Lee, H. J. Kim, K. R. Kwon and J. K. Lee, Digital watermarking of medical image using ROI information, in: *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry*, pp. 404–407 (2005).
- [15] B. Lei, T. E.-L. Tan, S. Chen, D. Ni, T. Wang and H. Lei, Reversible watermarking scheme for medical image based on differential evolution, *Exp. Syst. Appl.* 41, 3178–3188 (2014).
- [16] M. Li, S. Narayanan and R. Poovendran, Tracing medical images using multi-band watermarks, *Conf. Proc. IEEE Eng. Med. Biol. Soc.* 5, 3233–3236 (2004).
- [17] E. Maiorana, P. Campisi and A. Neri, Biometric signature authentication using random transform-based watermarking techniques, in: *IEEE Biometric Symposium*, pp. 1–6 (2007).
- [18] V. Mehan, R. Dhir and Y. S. Brar, Watermarking for health management system, *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 3, 224–228 (2013).
- [19] R. Pandey, A. K. Singh, B. Kumar and A. Mohan, Iris based secure NROI multiple eye image watermarking for teleophthalmology, *J. Multimed. Tools Appl.* 75, 14381–14397 (2016).
- [20] S. A. Parah, J. A. Sheikh and G. M. Bhat, Fragility evaluation of intermediate significant bit embedding (ISBE) based digital image water-

- marking scheme for content authentication, in: International Conference on Advances in Electronics, Computers and Communications (ICAEECC), pp. 1–6 (2014).
- [21] P. Rasti, S. Samiei and M. Agoyi, Robust non-blind color video watermarking using QR decomposition and entropy analysis, *Int. J. Sci. Direct* 38, 838–847 (2016).
- [22] R. Rodriguez-Colin, F.-U. Claudia and G. d. J. Trinidad-Blas, Data hiding scheme for medical image, in: IEEE 17th International Conference on Electronics Communications and Computers (CONIELECOMP'07) (2007).
- [23] A. Sharma, A. K. Singh and S. P. Ghrera, Robust and secure multiple watermarking technique for medical images, *Wireless Pers. Commun.* 92, 1611–1624 (2017).
- [24] A. K. Singh, Improved hybrid technique for robust and imperceptible multiple watermarking using medical images, *J. Multimed. Tools Appl.* 75, 8381–8401 (2016).
- [25] A. K. Singh, M. Dave and A. Mohan, Multilevel encrypted text watermarking on medical images using spread-spectrum in DWT domain, *Wireless Pers. Commun.* 83, 2133–2150 (2015).
- [26] Abdulbaqi, Azmi Shawkat, Muslim, Israa Falih, Al-Ameer, Asraa A. Abd & Obaid, Ahmed J. () Healthcare surveillance based on cloud computing utilizing mobile devices, *Journal of Discrete Mathematical Sciences and Cryptography*, 1-8, DOI: 10.47974/JDMSC-1566.

Received November, 2023