Indian Journal of Science and Technology, *Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/98462, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Enhancing Security for Data Hiding in Radiographic Images using Burrows Wheeler Transform

B. Karthikeyan, M. Rajasekhar Reddy, V. Vaithiyanathan, D. Kannan, A. C. Kosaraju

School of Computing, SASTRA University, Thanjavur- 613401, India;
karthikeyan@it.sastra.edu, rajasekharmanyam04@gmail.com, vaithiya_nathan@hotmail.com,
dinesh_kannan@hotmail.com,ac.kosaraju@gmail.com

Abstract

Objectives: This paper proposes a new method to enhance security for data hiding in radiographic images through distortion of original data. **Method**: The process involves applying a Burrows-Wheeler Transform (BWT) to the original data, which groups and stores similar patterns in data, causing distortion. This distorted data is then further encoded in a safe format before hiding it in the cover image. The decoding process decoding from the safe format and applying Inverse Burrows-Wheeler Transform (IBWT) to retrieve the original data from the stego image. **Findings**: Thus, a 2-level security scheme is implemented. Cryptanalysis of the hidden data becomes difficult since the original data is distorted, thus enhancing the security of the hidden data. Nevertheless, the stego image obtained from this method is less deviated from the original cover image. This is shown from the satisfactory PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) obtained. **Application/Improvements**: This proposed method can be used wherever steganography or data hiding has its applications. This method can be used in commercial communication, military communication etc.

Keywords: Burrows-Wheeler Transform (BWT), Data Hiding, Inverse Burrows-Wheeler Transform (IBWT), Least Significant Bit (LSB), Radiographic Images, Steganography

1. Introduction

Security enhancement in communication and information exchange is one of the most explored domains in the field of Information Technology. Today in the world of universal electronic connectivity with diverse cyber threats, secure connectivity is indeed a very essential tool for information exchange. Steganographic techniques grant information exchange by hiding secret data into a carrier image, which facilitates the communication. Though other data encryption provides security to some extent, the cryptanalysis of cipher texts encrypted with outdated techniques and improved steganalysis can be performed with little effort. So, there has been a constant urge to introduce a more efficient cryptographic algorithm. The combination of both steganographic and cryptographic techniques could afford an optimum solution for this. A methodology, involving Burrows-Wheeler Transform (BWT), a non-linear transform[1] is presented in this paper. The input bits are first grouped using BWT. This is followed by storing the positions of the least occurring bit in the grouped order. The positions of the least occurring bit are only embedded in the cover image to form the stego image. Thus, two levels of distortion are added to the secret data which makes cryptanalysis difficult. Retrieval of the message is done by forming the grouped string; by using the positions of the least occurring bit in the entire bit sequence. This bit sequence represents the grouped string of bits. Inverse Burrows Wheeler Transform (IBWT) is applied to this string to retrieve the original message.

*Author for correspondence

A novel highly capable two-sided data hiding technique was suggested for JPEG compressed images[2], which involves altering the quantization table as well as quantized Discrete Cosine Transformation (DCT) coefficient. High embedding capacity can be achieved and the distortion pertaining to the embedding can be kept very low. This method yields better results in terms of image quality when compared with that of existing[3,4] methods and is plausible for image files which are stored and transmitted in the JPEG format.

A new data concealing method[5] was suggested, founded on the amalgamation of a secret divvying technique and a new steganography method utilizing Integer Wavelet Transform[6]. A confidential image is divided into n parts, using a secret sharing technique. And utilizing proposed wavelet based steganography method, the n parts and Fletcher-16 checksum of the n parts are concealed into n cover images. The suggested method is firm against serious attacks which includes RS (Regular Singular analysis) and other steganalysis methods involving super visionary efforts.

Previous research has focused on blind steganalysis of JPEG images through the process of dilation[7] which includes dividing the given image into Red Green Blue (RGB) components which is followed by the transformation of each component into three domains, viz., frequency, spatial, and wavelet. Extracted features from these domains are fed into the Support Vector Machines (SVM) classifier that classed the image as stego or clean. Overall Success Rate (OSR) was chosen as the performance metric of the suggested solution.

There exists an efficient steganographic technique[8] using LSB replacement on a scanned path image, this technique involves a random key which is generated using the cover image pixel values using raster scan. The secret data is converted to integers by means of Extended Binary Coded Decimal Interchange Code (EBCDIC). This is followed by permuting the plaintext with the key. The permutation thus obtained is exclusively NORed (XNOR) with the key and thus embedded in the image to form the stego image. Thus, security is increased by using a pseudorandom key generator and by the Raster Scan of the cover image for every plaintext.

Another new method was proposed[9] to embed a secret image in another image by modifying the hill cipher method[10–12]. In this approach, the secret image is transformed into n number of 2 X 2 images, which are individually multiplied with a key matrix of size 2 X 2 and modulo-256 operation is computed and a one-dimensional matrix is formed by rearranging the n resulting matrices. The matrixes values are then converted into its binary form. The least two significant bits of each pixel in the cover image are replaced with two bits from the binary matrix consecutively. The retrieval is done by considering the last two bits from each pixel in the stego image and forming an 8-bit sequence. This one-dimensional sequence is broken down to n 2 X 2 matrices. With these matrices, the inverse of the key matrix is multiplied to obtain the original matrix. The resulting matrices are then rearranged to yield a single whole matrix which is the secret image that was embedded.

Researchers presented validity of medical image based steganography scheme[13], with a technique providing an effective mechanism to store and secure the digital images regarding medical fields. A feasible steganography proficiency involving Integer Wavelet Transform (IWT) for the protection of MRI medical images within a single container image is employed. The lineaments of the recovered image are of acceptable visual quality and the quality levels are ameliorated with satisfactory PSNR (Peak Signal to Noise Ratio) when compared with other existing algorithms.

A new methodology[14] was demonstrated to employ steganographic techniques in the construction of an access control model which provides to the data owners a complete control of their critical cardiac health information concealed in their own Electro cardiograms. The methodology includes a steganographic technique[15] instantly applicable to ECG. The proposed model effectively defends the privacy of users, maintains the confidentiality of user data, reduces storage requirements and provides an effective mechanism to upload and download data of large volume.

An adaptive blind and duple watermarking strategy[16] was introduced in the contour let knowledge domain, since the ROI (Region of Interest) is of high importance than RONI (region of non-Interest), in the interpretation of images pertaining to medical fields. Hence bits are embedded with different embedding strengths in ROI and RONI. Watermark bits are imbedded in the singular value vectors of the embedded blocks between low pass sub bands in contour let domain. The watermarked images possess high transparency and can be adapted to the DICOM (Digital Image and Communications in Medicine) format.

The proposed strategy shows that watermarked images in contour let field have higher hardiness against assaults than wavelet field and the qualitative examination of the proposed method shows it has good invisibility.

A modified histogram shifting algorithm[17] suitable for reversible medical image watermarking to ameliorate the hiding capacity was proposed. The technique involves hierarchical division of a cover image into smaller blocks for imbedding, utilizing the histogram shifting technique. A recursive technique for looking ahead estimation of the maximal data mass at the lowest level of the block division tree structure is employed to afford an optimal data concealment result and it also enhances PSNR value. Also, segmentation of medical images is performed to distinguish the region of interest, prior to block division to enhance the hiding capacity and the quality of stego image.

A new methodology[18] proposed for secret communications using cryptographic and steganographic techniques, where the cryptographic algorithm includes block cipher of length 128 bits and a key of length 256 bits. Two cipher text bits are imbedded in every pixel of the carrier image. The locations of embedding vary with respect to cipher text bits. This technique is termed as Dynamic steganography as the position of bits are decided while running the algorithm.

A lossless data hiding scheme[19] was introduced based on the quantized coefficients of DWT (Discrete Wavelet Transform) in the frequency domain. The secret data is embedded in the zero coefficients of the components in each block for a three-leveltwo-dimensional discrete wavelet transform of a cover image. This methodology includes three stages, embedding followed by extraction and then restoration. Acceptable image quality, data reversibility and high embedding capacity can be achieved by this technique.

A new blind steganalytic method[20] was suggested to identify JPEG stego images imbedded with various known steganographic programs. The proposed methodology includes a steganalytic method grounded on statistic results collected in both DCT and decompressed spatial domains for JPEG images. The collected statistics reflect even minute changes between a cover image and a corresponding stego image. Histogram Characteristic Function (HCF) and Center of Mass (COM) parameters are utilized to assess required statistics and compute features.

A new technique[21] was introduced for encrypting the data over network in less time and to make the retrieval of data difficult to any person other than the recipient. Their methodology is a culmination of RSA algorithm, Bit Rotation and Ex-Hill Cipher method, Bit Reversal method and Randomization utilizing permutation techniques. Visual distortions are used in encryption process and permutation technique is employed in the final stage to alter the whole file structure, which reduces the time taken for encryption.

There exists another technique[22] for secure data concealment by employing integer wavelet transform and genetic algorithm. The primary focus of the proposed work is to formulate an impregnable analysis-proof plan with highest imperceptibility. Optimal Pixel Adjustment Process is also adopted. The proposed technique is a semantic orientated security design, implemented on single computer system and the data hiding technique is limited only to image, and not suitable for video, speech and other biometrics.

An altered Hill cipher algorithm[23] inv1olving interweaving and iteration yields a strong cipher. A state-of-the-art study[24] about radiographic testing on weld inspection was presented. It consists of two stages, processing an image and recognizing a pattern. The techniques presented in this paper are concerned with the recognition of defects in continuous welds.

An elementary reversible data hiding technique[25] grounded on Integer Wavelet Transform (IWT) was proposed. Alterations of IWT coefficients in the proposed method efficaciously imbed data into IWT blocks with low distortion. Also, the stego images produced by the proposed methodology possess robustness to image processing techniques.

Recently, a steganography method using 9/7 Integer Wavelet Transform (IWT) was proposed[26]. This paper talks about a pixel adaptive embedding, which improves security by using a Least Significant Bit (LSB) method. The coefficients are selected randomly using Graph Theory. This method is proved to provide significantly high security and capacity.

A proposed methodology[27] for blind integrity verification of medical images suggests blind forensics approaches for medical imaging. The technique involves comparison of two image features, HRBD (the histogram statistics of reorganized block-based discrete cosine transform coefficients), suggested for steganalysis purposes, and the histogram HRBT (statistics of reorganized block- based Tchebichef moments).

To ameliorate security, confidentiality and integrity in medical data a new watermarking technology was

proposed[28]. DICOM (Digital Image and Communications in Medicine) data is used as a watermark to imbed in medical images. The proposed methodology is robust to modifications in brightness and contrast. The algorithm suffers from degradation in water marked image and less accuracy in retrieved image.

A delicate image authentication technique[29] for DICOM (Digital Image and Communications in Medicine) images utilizing discrete wavelet transform was introduced. The proposed scheme deals with management of critical health information which also includes authenticating source, data and transfer of diagnosis details of patients. The robustness of method is ameliorated through hybrid coding technique.

A new methodology[30] for securing medical images in a Health Insurance Portability and Accountability Act (HIPAA) mandated Picture Archiving and Communication System (PACS) environment was suggested. The technique includes Digital Envelope (DE) concept with Digital Signature (DS) of the images for providing image integrity and to ensure security over an open network.

There exists an adaptive stego process[31] which encrypts secret data utilizing DES (Data Encryption Standard) and also randomizes the selection of block, utilizes an unsystematic walk in imbedding the secret data.This Adaptive Random method is carried out along with the Inverted Pattern approach, which is termed as Adaptive Random Inverted Pattern approach (ARIP).The proposed methodology improves security for the given payload.

A new method[32] was suggested to identify the hidden data imbedded in the least significant bits of a natural image. The proposed methodology specifically deals with tests designed for natural images and the statistical properties associated with the tests. The LRT (Likelihood Ratio Test) is computed from the known image elements and includes designing GLRT (Generalized Likelihood Ratio Test) for accurately estimating unknown parameters.

Previously, works were published[33] to exploit an equational reasoning for the derivation of the Burrows-Wheelers transform for the given specifications. There is another published paper[34] on computing the BWT for a given string and its inverse in parallel. The article also yields a good understanding of the relationship between a string and its inverse. A modified Burrows-Wheeler Transform was proposed[35] for standard edit operations, which includes an algorithm with time complexity O (|T |). This technique is also for updating a suffix array and compressed images. A syllable based BWT approach was introduced[36], which involves comparison of efficiency of BWT, in compressing letters, words utilizing XBW compression technique.

Application of BWT compression to practical problems have been explored[37] by researchers. In this published work, BWT is used along with other compression schemes like Huffman and run-length encoding to compress patterns for Very Large Scale Integration (VLSI) circuit tests. This approach seems to provide a better compression ratio compared to others in the literature for VLSI test vector compression.

The proposed method is an interdisciplinary of cryptographic and steganographic techniques, which suggests a two-level security scheme to increase the distortion in data as well as the difficulty level in decrypting the data. The cryptographic technique utilized in this methodology is Burrows-Wheeler transform.

2. Proposed Method

The proposed method consists of three steps in encryption and decryption algorithms as shown in Figure 1, 2, 3 and 4.

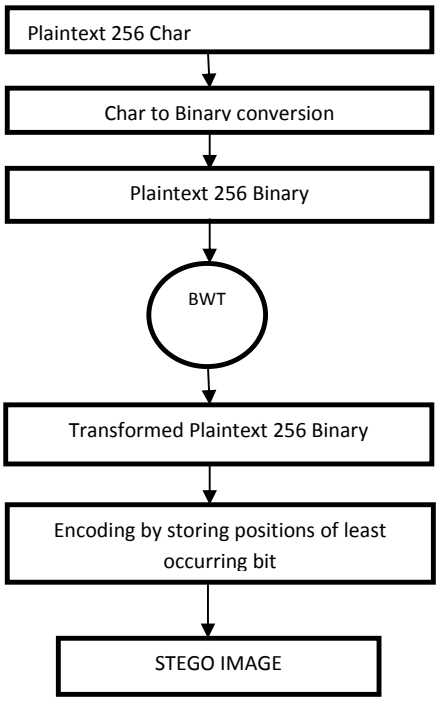

Figure 1. Encryption on sender's side.

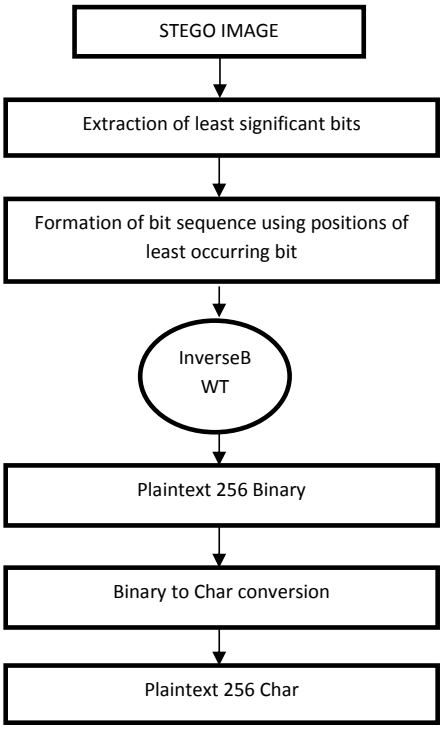

Figure 2. Decryption on receiver's side.

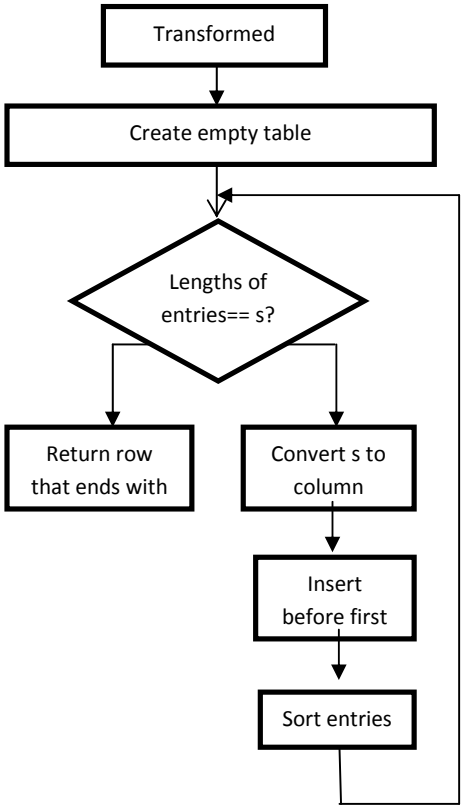

Figure 3. Procedure of IBWT.

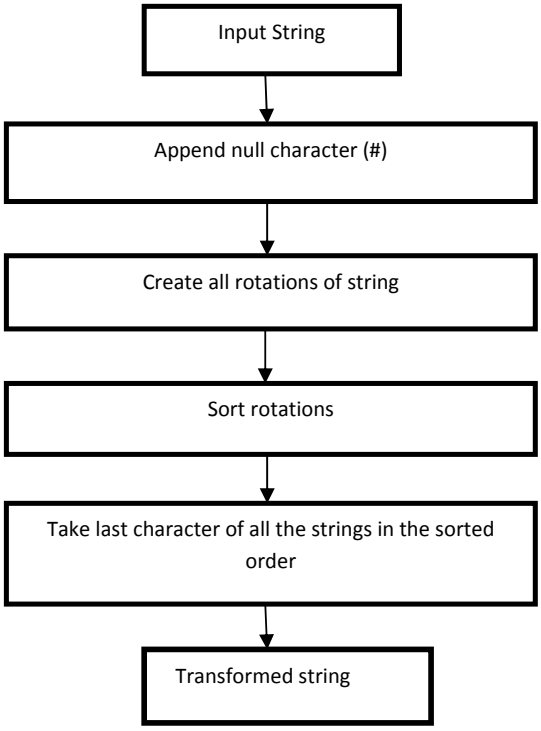

Figure 4. Procedure of BWT.

2.1 Encryption Algorithm

Step 1. Firstly, the message stream is converted into bit stream and the additional encryption method, BWT is applied to this bit stream.

Step 2. Then the bit stream is encoded into a more inviolable format by considering the positions of least occurring bits and the null character (#), which is appended to the bit stream in BWT. This provides an additional security layer and the result of this process would effectively convert a character into storable bits of 10-19 bits length.

Step 3. The bits obtained from Step 2 are stored in the cover image using LSB method, to form a stego image.

2.2 Decryption Algorithm

Step 1. First off, the embedded bits are extracted from the received stego image.

Step 2. The bits corresponding to a character of the original message are extracted. These bits contain the information regarding the position of least occurring bits and the null character (#) inserted in the BWT. These bits are further decoded to form a 9-bit sequence.

Step 3. Then the IBWT is applied to the 9-bit sequence obtained in the previous step. This operation yields the original embedded message.

2.3 Detailed Procedure

The following section contains the detailed procedure of the proposed methods for both encoding as well as decoding.

Step 1.The essential BWT is applied to each 8-bit character in the message.

Burrows-Wheeler Transform (BWT).

Burrows-Wheeler Transform (BWT), also known as block-sorting compression, rearranges a series of characters into groups, containing similar characters upon which other encoding techniques like run length encoding can be used. In this methodology, BWT is applied on a series of bits which is the binary form of 8-bit characters. Using BWT on the bits yield a unique arrangement of the bits where similar bits are grouped together efficiently to such an extent that it can also be reversed.

The transform is carried out by appending a null character (#) and rotating the positions of characters. Then the resultant strings are sorted in lexicographical order.

The output string is obtained by considering the last entity from each string in this order. Burrows-Wheeler Transform is a reversible transform- the original bit-sequence can be retrieved by the following method.

Inverse Burrows-Wheeler Transform (IBWT).

The inverse of the transform IBWT is carried out by arranging the output string in a column and sorting it and then appending the bits in the corresponding positions of this sorted column to the output string column and sorting this newly formed column. This process is repeated until the length is reached to its maximum value (8-bits excluding the null character). Then the string with the null character at the end is the original string that has been transformed.

Algorithm 1: Burrows-Wheeler Transform

Function BWT (string s)

1: *create a table containing all possible rotations of s*
2: *sort the rotations lexicographically*
3: *take the last column from each of the sorted string.*

Algorithm 2: Inverse BWT

Function INVERSE - BWT (string s)

1: *create empty table*
2: *for i ⟵ 1 to length(s)*
3: *convert s to column vector*
4: *insert into table before first column*
5: *sort table lexicographically*
6: *return (string with null character '#' at the end)*

Step 2.

The resultant string of the BWT is encoded one at a time by the method given below.

Encoding:

The least occurring bit and the position of the null character in the BWT string are determined. The encoded string is formed as follows,

1. The first bit of the string is the least occurring bit. If there are equal number of zeros and ones, any one of them (0 or 1) can be taken.
2. The next three bits represent the frequency of the least occurring bit (0 – 4).
3. The next three bits represent the position of the null character (#) in the BWT string.
4. The next sequence of three bits represents the positions of the least occurring bits in the string.

A BWT string is thus encoded, and this encoded string is embedded in the cover image.

Decoding:

The decoding is done by following the steps below,

1. Identify the least significant bit. It is the first bit of the string.
2. Find the frequency of the least occurring bit from the next three bits.
3. Find the position of the null character (#) from the next three bits.
4. Find the positions of the least occurring bit from the next sequence of three bits. The limit of the sequence is indicated by the frequency of the least occurring bit computed earlier.
5. In a new string fill in the least occurring bit and the null character in their appropriate positions.
6. Fill in the rest of the positions with the compliment of the least occurring bit.

The algorithm for the encoding and decoding processes is as follows,

Algorithm 3: Encoding

1. *find count of least occurring bit (1 or 0)*
2. *create new string*
3. *least occurring bit is stored as first bit in the string*
4. *count of the least occurring bit in binary is the next three bits (1-3) of the new string*
5. *position of null character (#) in binary is the next three bits (4-6) of the new string.*
6. *positions of the least occurring bit is stored as sequences of three bits in the new string*

Algorithm 4: Decoding

1. *take first bit of string (least occurring bit-POSITION 0)*
2. *compute frequency of the least occurring bit from bits in position 1-3*
3. *compute the position of the null character (#) from bits in position 4-6*
4. *compute positions of least occurring bit from the sequence of three bits till the count (computed earlier) has reached.*
5. *create new string*
6. *fill in the null character (#) and least occurring bit in appropriate positions (as computed earlier)*
7. *fill the rest of the positions with the compliment of the least occurring bit*
8. *return new string*

3. Experimental Results and Discussions

The security for radiographic image based steganography has been enhanced by the proposed methodology, which yields much satisfactory results. The proposed algorithm is applied to various radiographic images. They are illustrated in Figure 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 1819. Each figure contains three images. The cover image (before embedding text message), the stego image (with embedded text message in it) and the retrieved image (after applying the proposed algorithm). The selected images vary in dimensions and in the file size. They are tabulated along with the MSE values, the PSNR values and the Structural Similarity Index (SSIM) values in Table 1, 2 and 3 respectively. It can be inferred from the tables (Table 1 and Table 2) that MSE values are low for the corresponding file size where the PSNR values are high, which are the two significant quantitative performance metrics for measuring the image distortion. The SSIM of the images, a reference metric, is also calculated to ensure the similarity between the images before and after embedding the secret data.

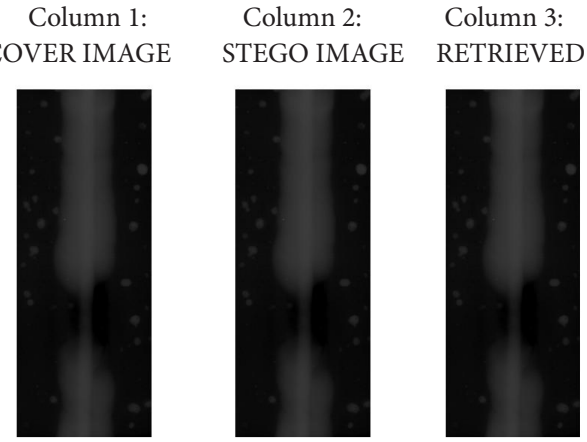

Figure 5. Sample Image1.

Figure 6. Sample Image2.

Figure 7. Sample Image3.

Figure 8. Sample Image4.

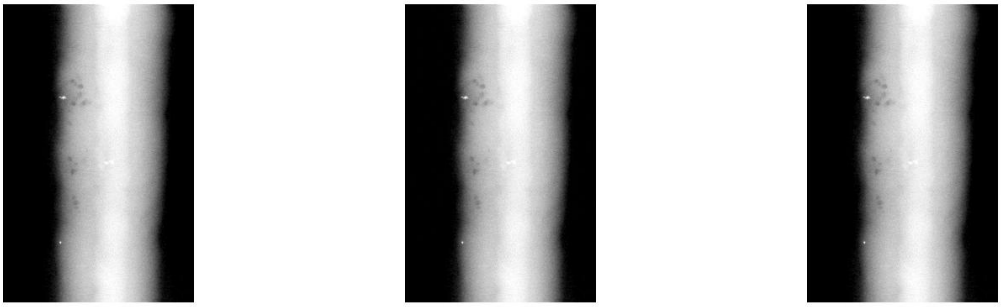

Figure 9. Sample Image5.

Figure 10. Sample Image6.

Figure 11. Sample Image7.

Figure 12. Sample Image8.

Figure 13. Sample Image9.

Figure 14. Sample Image10.

Figure 15. Sample Image11.

Figure 16. Sample Image12.

Figure 17. Sample Image13.

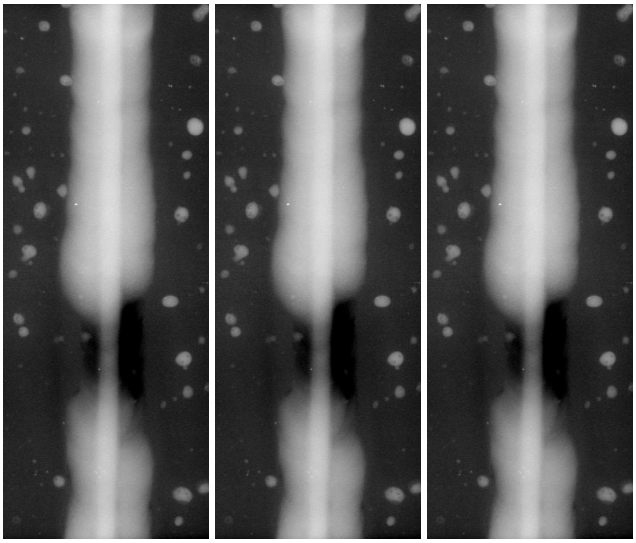

Figure 18. Sample Image14.

Figure 19. Sample Image15.

Table 1. Performance comparison of various test images

IMAGE	DIMENSIONS	SIZE OF FILE	MEAN SQUARE ERROR
Figure 5	345 X 552	1	0.004637
Figure 6	2410 X 1954	229	0.455081
Figure 7	1954 X 2410	234	0.924377
Figure 8	2410 X 1954	237	0.967263
Figure 9	227 X 355	4.03	0.543620
Figure 10	802 X 1000	19.9	0.9044
Figure 11	630 X 546	21.8	0.4331
Figure 12	610 X 610	23.6	0.8693
Figure 13	532 X 660	22.3	0.6995
Figure 14	2048 X 2048	265	0.4348
Figure 15	600 X 600	21.7	0.5376
Figure 16	204 X 247	3.00	0.4960
Figure 17	720 X 720	32.6	0.9313
Figure 18	931 X 359	4.03	0.4083
Figure 19	503 X 350	6.91	0.8054

Table 2. PSNR values of selected images and their dimensions

IMAGE	DIMENSIONS	PEAK SIGNAL TO NOISE RATIO
Figure 5	345 X 552	71.5028
Figure 6	2410 X 1954	51.5839
Figure 7	1954 X 2410	48.5063
Figure 8	2410 X 1954	48.3094
Figure 9	227 X 355	50.8118
Figure 10	802 X 1000	48.6010
Figure 11	630 X 546	51.7989
Figure 12	610 X 610	48.7733
Figure 13	532 X 660	49.7172
Figure 14	2048 X 2048	51.7815
Figure 15	600 X 600	50.8601
Figure 16	204 X 247	51.2099
Figure 17	720 X 720	48.4738
Figure 18	931 X 359	52.0546
Figure 19	503 X 350	49.1049

Table 3. SSIM values of selected images along with their dimensions and file sizes

IMAGE	DIMENSIONS	SIZE OF FILE	STRUCTURAL SIMILARITY INDEX
Figure 1	345 X 552	1	1.0000
Figure 2	2410 X 1954	229	0.9945
Figure 3	1954 X 2410	234	0.9967
Figure 4	2410 X 1954	237	0.9956
Figure 5	227 X 355	4.03	0.9966
Figure 6	802 X 1000	19.9	0.9980
Figure 7	630 X 546	21.8	0.9988

Figure 8	610 X 610	23.6	0.9929
Figure 9	532 X 660	22.3	0.9978
Figure 10	2048 X 2048	265	0.9992
Figure 11	600 X 600	21.7	0.9961
Figure 12	204 X 247	3.00	0.9952
Figure 13	720 X 720	32.6	0.9944
Figure 14	931 X 359	4.03	0.9962
Figure 15	503 X 350	6.91	0.9949

The observational results obtained from the proposed method are depicted in the pictorial plots. The plot in Figure 20, 21 and22 depicts the relation between MSE values and PSNR values of an image of a particular size.

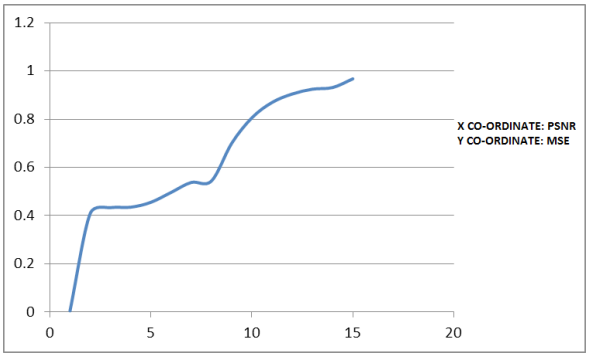

Figure 20. No.of pixels versus message file size plot.

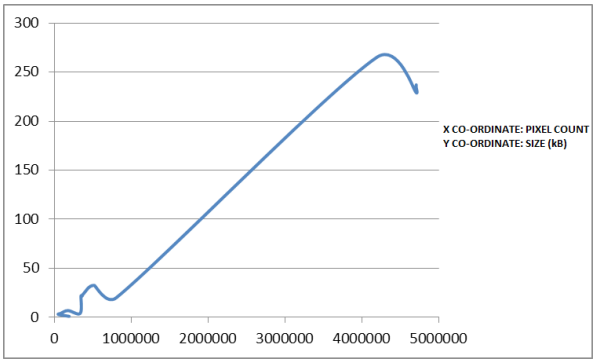

Figure 21. PSNR versus pixel count plot.

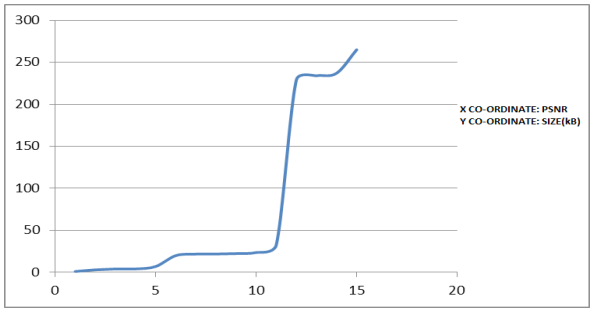

Figure 22. PSNR versus message file size plot.

It is evident from the results that the proposed methodology results in securing information transmission through images with acceptable tradeoffs in performance metrics of the corresponding images.

4. Conclusion

This paper deals with strengthening the security by distorting the original data using a known reversible transform. Further distortions are added by encoding in an efficient format, thereby making cryptanalysis difficult and ultimately increasing security. The reversible transform employed in this process is Burrows-Wheeler Transform (BWT), which when applied on the plaintext yields a bit sequence from which, only the positions of the least occurring bit is stored instead of the entire sequence. The reverse of this operation is carried out during retrieval, where the bit sequence is formed by filling the least occurring bit in its corresponding positions. The entire sequence is formed by filling the rest of the positions with the compliment bit of the least occurring bit. Performing an Inverse Burrows-Wheeler Transform (IBWT) on this bit sequence yields the original plaintext.

5. Acknowledgments

The authors would like to convey sincere thanks to SASTRA University for providing the necessary infrastructure and for IGCAR for providing the radiographic images.

6. References

1. Kurtz S, Balkenho B. Space Efficient Linear Time Computation of the Burrows and Wheeler-Transformation. Numbers, Information and Complexity. 2000;375–83.
2. Wang K, Lu ZM, Hu YJ. A high capacity lossless data hiding scheme for JPEG images. Journal of Systematic Software 2014. 86(7):1965.
3. Chang CC, Chen TS, Chung LZ. A steganographic method based upon JPEG and quantization table modification. InformSciences. 2002; 141(1–2):123–38.
4. Xuan GR, Shi YQ, Ni ZC, Chai PQ, Cui X, Tong XF. Reversible data hiding for JPEG images based on histogram pairs. Lecture Notes of Computer Science. 2007;715–27.
5. Khosravi MJ, Naghsh-NilchiA R. A novel joint secret image sharing and robust steganography method using wavelet. Multimedia System. 2014; 20(2):215–26.

6. Huang HY , Chang SH. A Lossless Data-hiding Technique based on Wavelet Transform. Conference on Machine Vision Applications. MVA Japan. 2011;316–9.
7. Pathak P, Selvakumar S. Blind Image Steganalysis of JPEG images using feature extraction through the process of dilation. DigitInvest. 2014; 11(1):67–77.
8. Karthekeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M. An improved steganographic technique using LSB replacement on a scanned path image. International Journal of Network Security 2014. 16(1);–8.
9. Karthikeyan B, Chakravarthy J, Vaithiyanathan V. An enhanced Hill cipher approach for image encryption in steganography. International Journal of electronic Security and Digital Forensics. 2013; 5(3-4): 178–87.
10. Sharma N, Chirgaiya S. A Review of Modern Hill Cipher Techniques. JSRD. 2013; 1(10):2198–202.
11. MokhtariM, Naraghi H. Analysis and Design of Affine and Hill Cipher. Journal of Mathematics Research. 2012; 4(1): 67–77.
12. NordinM, Rahman A, Abidin AFA, Yusof MK, Usop NSM. A New Approach of Classical Hill Cipher. International Journal of Security and Its Applications. 2013; 7(2):179–90.
13. Prabakaran G, Bhavani R, Rajeswari PS. Multi Secure and Robustness for Medical Image Based Steganography Scheme. International Conference on Circuits, Power and Computing Technologies, ICCPCT, India. 2013. p.–1188–93.
14. Mai V, Khalil I, Baida A . Steganography-based Access Control to Medical Data Hidden in Electrocardiogram. 35th Annual International Conference of the IEEE EMBS. 2013.p–1302–5.
15. Ibaida A, Khalil I, Al-Shammary D. Embedding patient's confidential data in ECG signal for healthcare information systems. Conference Proceeding of IEEE Engineering Medical Biology Society 2010. p.3891–4.
16. Rahimi F, Rabbani H. A dual adaptive watermarking scheme in contourlet domain for DICOM images. Biomedical Engineering Online. 2011;10–53.
17. Kumar VC, Natarajan V, Bhogadi D . High Capacity Reversible Data hiding based on Histogram shifting for Medical Images. International conference on Communication and Signal Processing, ICCSP,India. 2013.–730–3.
18. Swain G, Lenka SK. A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography. International Journal of Security and Its Applications 2012. 6(4):1–12.
19. Huang HY, Chang SH. A Lossless Data-hiding Technique based on Wavelet Transform. Machine Vision Applications. 2011; 66(2):8–15.
20. Li Z , Lu K, Zeng X , Pan X . A Blind Steganalytic Scheme Based on DCT and Spatial Domain for JPEG Images. Journal of Multimedia. 2010; 5(3):200–7.
21. Sapra K, Kapoor S. Modified Image Encryption Technique. SSRG International Journal of Electronics and Communication Engineering. 2014; 1(6):36–40.
22. Shamimunnisab S, Cauvery NK. Empirical Computation of Rs-Analysis for Building Robust Steganography Using Integer Wavelet Transform and Genetic Algorithm. International Journal of Engineering Trends and Technology. 2012; 3(3):448–56.
23. Sastry UV, Shankar RN, Bhavani DS. A Modifed Hill Cipher Involving Interweaving and Iteration. International Journal of Network Security. 2010; 11(1):11–16.
24. Ricardo R, Silva D, Mery D. State-of-the-Art of Weld Seam Inspection by Radiographic Testing: Part i-Image processing. E-Journal of Nondestructive Testing and Ultrasonics. 2009;12(9):1–9.
25. Yang CY, Lin CH, Hu WUC . Reversible Data Hiding for High-Quality Images Based on Integer Wavelet Transform. Journal of Information Hiding and Multimedia Signal Processing. 2012; 3(2):142–50.
26. Thanikaiselvan V, Bansal T, Jain P, Shastri S. 9/7 IWT Domain Data Hiding in Image using Adaptive and Non Adaptive Methods. Indian Journal of Science and Technology. 2016 Feb; 9(5):1–7.
27. Huang H, Coatrieux G, Shu HZ, Luo LM, Roux CH. . Blind Integrity Verification of Medical Images. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2012;16(6):1122–26.
28. Raúl RC, Claudia FU , de JTBGD. Data Hiding Scheme for Medical Images. 17th International Conference on Electronics, Communications and Computers, Mexico.2007.
29. Kannammal A, SubhaRani S. Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet Transform Domain. IJCSI International Journal of Computer Science . 2011; 8(6):1.
30. Cao F, Huang HK, Zhou XQ. Medical image security in a HIPAA mandated PACS environment. Computer Medical Imaging Graphing. 2003;185–96.
31. Amirtharajan R, Rayappan JBB. An intelligent chaotic embedding approach to enhance stego-image quality. Information Sciences. 2012;193:115–24.
32. Cogranne R, Zitzmann C, Retrainty F, Igor V, Nikiforov N, Cornu P, Fillatre L. A Local Adaptive Model of Natural Images for Almost Optimal Detection of Hidden Data. Signal Processing. 2014; 100:169–85.
33. Bird R, Shin-Cheng MU. Functional Pearls Inverting the Burrows-Wheeler Transform. Journal of Functional Program. 2004;14(6):10–11.

34. Ohlebusch E ,Beller T, Mohamed I, Abouelhoda A. Computing the Burrows–Wheeler transform of a string and its reverse in parallel. Journal of Discrete Algorithms. 2013; 25:–243–56.
35. Salson M, Lecroq T, L´eonard M, Mouchard L. Dynamic Burrows-Wheeler Transform. Prague Stringology Conference, India. 2008.p.13–25.
36. L´ansk´y, J ChernikK ,Vl˘ckov´a Z . Syllable-Based Burrows-Wheeler Transform. CEUR Workshop Proceedings. 2007; 235:1–10.
37. Asokan A, Anita JP. Burrows Wheeler Transform Based Test Vector Compression for Digital Circuits. Indian Journal of Science and Technology. 2016 Aug; 9(30):1–5.