1. Introduction

The Health Insurance Portability and Accountability Act (HIPAA) were constituted to provide health insurance portability for individuals to protect the privacy and security of patient health information and to eradicate fraud and abuse. HIPAA standardizes claim submission so the sender and the receiver will have the same format. Consumers have demanded privacy and security of their patient health information to include all oral, paper and electronic notations. Healthcare information can be utilized to discriminate in employment settings and insurance buying. With wide-ranging implication, HIPAA is integral throughout the delivery of quality healthcare. With a variety of electronic medical records and healthcare software, transmitting information along the continuum of care within a healthcare system or between healthcare systems and providers necessitates that the sender and the receiver be able to communicate electronically with each other.

A simple data hiding system in the spatial domain is the Least Significant Bit (LSB) replacement method proposed. The LSB replacement method also called as LSB substitution directly embeds $k$ secret bits into $k$ Least Significant Bits (LSBs) of each cover pixel, where $1 \leq k \leq 8$. The LSB replacement method is inherently asymmetric i.e. the even value pixels will be either unchanged or incremented whereas the odd value pixels will be either
Selective Plane Replacement Watermarking and Cryptography (SPRWC)

unchanged or decremented. This asymmetric property is exploited for the steganalytic purpose. It is also known that the LSB-R method can be easily detected. In order to overcome this drawback, many data hiding schemes were proposed to improve the LSB-R method in terms of visual quality and hiding capacity.

To overcome the asymmetry of the LSB replacement method, LSB matching method was introduced. In this method, the cover image pixel is randomly either incremented or decremented when the secret bit does not match the LSB of the cover image pixels. Therefore, the asymmetry of odd and even valued pixels is eliminated. As a result, the detection of the LSB-M method by statistical detectors is difficult than the LSB-R detection method. Improved that LSB-M method has the same visual quality and hiding capacity as the LSB-R method. Introduced LSB Matching Revisited (LSB-M-R) scheme in which binary function and four embedding rules are used to embed two secret bits into a cover pixel pair at a time. From the results, it was proved that the visual quality and peak signal to noise ratio for an LSB-M-R scheme was better than the LSB-M method. Proposed to embed secret messages in the moderately significant bit of the cover image. Local Pixel Adjustment Process (LPAP) was introduced to improve the quality of the stego image. But the results were not optimal as the LPAP method considered only three least significant bits. As the LPAP process modifies the LSBs, the technique cannot be applied to data hiding schemes for LSB substitution. Proposed a data hiding scheme by simple LSB substitution with an Optimal Pixel Adjustment Process (OPAP). The method proved to be better than the LPAP method but extra computational complexity.

Cryptographic mechanisms such as encryption and Digital Signatures (DS) are commonly used for medical data protection. It mainly concentrates on confidentiality, integrity and non-repudiation services. Introduced a method in which the key used for the encryption of the cover image is embedded in the encrypted cover image. Here secret key is encrypted twice by the RSA algorithm before embedding process. Though the system provides high authentication, it is more computationally complex. Proposed a method for both record indexing and integrity protection of medical images wherein the ROI is generated by Message Digest 5 (MD5) algorithm and embedded along with EPR into the non-ROI parts of the medical image. But the algorithm was not tested for all types of attacks. Adapted error correcting codes to enhance reliability of transmission and storage of medical images interleaved with patient information. But this scheme does not satisfy requirements pertaining to security of the content transmitted. Proposed a method to embed the watermark information in non-region of interest. The data to be embedded is encrypted using Bose-Chaudhuri-Hocquengham (BCH) coding technique. The method is not successful with increased size of payload.

The paper is organized in such a way that the Section 1 gives detailed information of related works. Section 2 discusses the concept of bit plane slicing and Section 3 explains the RSA Image Encryption Algorithm. Section 4 gives the step by step process of the proposed algorithm. Section 5 shows the simulation results at every stage, the quality metrics that are used to determine the effectiveness of the proposed scheme are also presented. Section 6 presents the comparative analysis. Finally, Section 7 summarizes the paper and discusses the future work.

2. Bit Plane Slicing

Bit plane slicing is useful in image analysis to extract the details of an image. The gray level of each pixel in a digital image is stored as one or more bytes in a computer. Each pixel in a grayscale image is represented by 8 bits that means image is composed of eight 1-bit planes, ranging from bit-plane 0 which is the Least Significant Bit (LSB) up to bit-plane 7 which is the Most Significant Bit (MSB) as shown in Figure 1 each plane constitutes a collection of zeros and ones. The advantage of this technique is that it portrays the relative importance of each bit in a pixel and highlights the contribution made by these bits to the total image appearance. The last higher order bit planes contain the majority of visually significant data.

![Bit plane slicing](image-url)
The most image information is contained in the higher bits (i.e. MSBs), whereas the least significant bits contain some of the finer details and noise. Bit plane combining is the reverse of bit plane slicing. The planes can be recombined to reconstruct the image. For the reconstruction of the image with a lower data rate some bit planes can be ignored until the changes in gray level have an acceptable impact on the image. Bit plane slicing is most widely used for applications in the field of digital watermarking and image compression.

3. RSA Image Encryption Algorithm

The RSA scheme is a block cipher in which the plaintext and cipher text are integers between 0 and n. The scheme developed by in makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. The encryption of the plaintext M and the decryption of the cipher text C are as follows:

\[ C = M^e \mod n \]  
\[ M = C^d \mod n \]  

Both sender and receiver must know the value of 'n'. The sender knows the value of 'e' and only the receiver knows the value of 'd'. Thus, this is a public-key encryption algorithm with a public key of \( PU = \{e, n\} \) and a private key of \( PU = \{d, n\} \).

4. Proposed Algorithm: Selective Plane Replacement Watermarking and Cryptography

4.1 Embedding and Encryption Phase

The proposed embedding and the encryption process are depicted in Figure 2. The algorithm for the embedding and encryption process is as shown:

Step 1: The input cover medical image (M) is subjected to bit plane slicing. Plane 0 (LSB plane) contains all the lower order bits and plane 7 (MSB plane) contains all the higher order bits.

Step 2: Hospital logo is considered as the watermark image (H) that is encrypted before embedded into the cover medical image.

Step 3: Encryption is carried out using RSA as outlined in section 3. The watermark image is encrypted using a public key and the encrypted hospital logo is done as per (3)

\[ C = H^e \mod n \]  

Step 4: The encrypted hospital logo is embedded into the MSB plane of the cover image. The embedding is performed by replacing the bits in the MSB plane of the cover medical image with the bits of the encrypted hospital logo, the MSB Embedded Plane is obtained using the (4).

\[ MSB - E = \text{bitset} \left( \text{MSB Plane} , C \right) \]  

Step 5: The MSB embedded plane is replaced in position of the LSB plane of the Cover medical image as shown in (5). The watermarked encrypted cover medical image (\( M_6 \)) is reconstructed back before being transmitted over public networks.

\[ LSB \text{ Plane} = \text{Replace} \left( \text{LSB Plane}, MSB - E \right) \]  

Figure 2. Selective plane replacement embedding and encryption process.
4.2 Extraction and Decryption Process
The extraction and decryption process is depicted in Figure 3. The algorithm is as shown below:

Step 1: The watermarked encrypted cover medical image is transmitted over public network to the receiver end.

Step 2: At the receiver end, the watermarked encrypted cover medical image \( M_w \) is subjected to bit plane slicing.

Step 3: The LSB plane is extracted from the embedded medical image, which is then subjected to RSA decryption process from which the watermark hospital image can be obtained. The decryption process is done with a private key \( d \) with the multiplicand of two prime numbers \( n \):

\[
H = (MSB - E)^d \mod n
\]  

Step 4: The MSB plane of the cover medical image can be obtained after the extraction of the watermark. The plane is replaced in its original position and the cover medical image can be reconstructed.

Step 5: The extracted hospital logo helps in determining the integrity of the cover medical image.

5. Simulation Results and Analysis
In this Section, experimental results are demonstrated to show the effectiveness of the proposed Selective Plane Replacement Watermarking and Cryptography Technique. The proposed scheme is simulated using MATLAB R2014. As per the watermarking procedure, the cover medical image as shown in Figure 4 and the hospital logo as shown in Figure 5 (a) as the watermark image. The cover medical image is bit plane sliced as shown in Figure 6. The hospital logo is encrypted using RSA algorithm before being embedded into the cover medical image as shown in Figure 5 (b). The cover medical image is bit plane sliced in which the MSB plane is replaced with the bits of the encrypted watermark image. The watermark embedded MSB plane as shown in Figure 7 (a) is replaced with the LSB plane of the cover medical image. The cover medical image is reconstructed which is termed as Watermarked Encrypted cover medical image as shown in Figure 7 (b). Table 1 shows the entropy, NPCR and UACI values for the Watermarked Encrypted Medical Image.

![Figure 3. Selective plane replacement extraction and decryption process.](image)

![Figure 4. Cover medical image.](image)
the test medical images. The first row in the table gives the results of the test medical images without any attack. Additive noise (Salt and pepper noise) with varying density is considered as the first type of attack.

Figure 5. a) Hospital logo, b) Encrypted hospital logo.

Figure 6. Bit plane slicing of cover medical image.

Figure 7. a) Embedded MSB plane, b) Watermarked cover medical image.

| Image                          | Entropy | NPCR | UACI |
|-------------------------------|---------|------|------|
| Watermarked Encrypted Medical Image | 7.820   | 0.968 | 0.32 |

Table 1. ANALYSIS OF THE PROPOSED TECHNIQUE FOR VARIOUS PARAMETERS

| Attack                        | Attack level | PSNR (dB) for Watermarked Encrypted Medical Image |
|-------------------------------|--------------|--------------------------------------------------|
| No attack                     | -            | 43.3                                             |
| Additive Noise                | 0.005        | 43.1                                             |
| (Salt and Pepper Noise)       | 0.01         | 42.9                                             |
| JPEG 2000                     | 5:1          | 43.0                                             |
|                               | 10:1         | 42.6                                             |
|                               | 25:1         | 41.4                                             |
| Rotation                      | 5°           | 43.8                                             |
|                               | 30°          | 42.5                                             |
|                               | 50°          | 41.6                                             |
| Cropping                      | 5 %          | 42.9                                             |
|                               | 10 %         | 41.4                                             |
|                               | 20 %         | 40.8                                             |
| Median filtering              | 2 x 2        | 43.1                                             |
|                               | 3 x 3        | 42.7                                             |
|                               | 4 x 4        | 41.9                                             |
| Gamma corrections             | 0.25         | 43.0                                             |
|                               | 0.5          | 42.8                                             |
|                               | 1.5          | 39.8                                             |

The test is performed with a maximum density value of 0.05. JPEG compression is one of the most widely used compression algorithm for images and 25:1 is the maximum compression ratio applied to the test images.
Small angle rotation does not change the values of the image, but makes the watermark undetectable; the test is performed with a maximum rotation angle of 50 degree. Cropping of image tries to remove a portion of the watermarked medical image. The test is performed with a maximum cropping percentage of 20%. Median filtering belongs to the class of low pass filtering where the test is performed for varying mask sizes. Gamma correction is frequently used operation to enhance images and the test is performed for a maximum gamma value of 1.5. From the results, it can be observed the PSNR value reduces linearly for all the test medical images. It can also be stated that the proposed watermarking algorithm gives acceptable result even if the attack levels are increased as the encryption and watermarking techniques are combined.

6. Comparative Analysis

The proposed algorithm is a combination of Watermarking and Cryptography techniques. The comparison is performed between the proposed algorithm and the algorithm performed without the encryption process. Table 3 depicts the results obtained by both the techniques. It can be stated that the proposed technique gives better result in terms of PSNR as the encryption of hospital logo generates a random image that is embedded into the MSB plane that causes less Mean Square Error when compared with embedding the hospital logo without encryption on the MSB plane. The PSNR value for the proposed algorithm varies with changes in the encryption key (p and q). Figure 8 presents the comparison chart in which the proposed technique with encryption gives a better result than without encryption.

| Watermarked Medical Images | Proposed Technique (Encrypted hospital logo) | PSNR (dB) | Proposed Technique (Hospital logo without Encryption) | PSNR (dB) |
|----------------------------|---------------------------------------------|-----------|--------------------------------------------------------|-----------|
| MRI 1                      | 44.4                                        | 43.9      |
| MRI 2                      | 45.3                                        | 43.1      |
| CT 1                       | 43.3                                        | 41.5      |
| CT 2                       | 45.9                                        | 44.8      |
| MRA 1                      | 45.4                                        | 44.2      |
| MRA 2                      | 45.6                                        | 44.8      |
| XRAY 1                     | 43.0                                        | 42.4      |
| XRAY 2                     | 45.8                                        | 44.3      |

7. Conclusion

The Selective Plane Replacement Watermarking and Cryptography algorithm presents a method that provides secure medical image transaction based on a hybrid algorithm involving bit plane slicing and RSA encryption. The hybrid algorithm explores a watermarking approach in spatial domain with hospital logo as the watermark. The encrypted hospital logo is embedded into the MSB plane of the medical image. The LSB plane of the medical image is replaced with the embedded MSB plane. The image is reconstructed before being transmitted over the public networks. The effectiveness of the proposed algorithm is verified against various attacks. The comprehensive simulation study of the proposed algorithm also demonstrates the improved security.

8. References

1. Turner LF. Digital data security system. Patent IPN. WO 89/08915. 1989.
2. Thanki RM, Borisagar KR. Experimental study of sparse watermarking techniques for multibiometric system. Indian Journal of Science and Technology. 2015 Jan; 8(1):42–8.
3. Chan CK, Cheng LM. Hiding data in images by simple LSB substitution. Elsevier Pattern Recognition. 2004 Mar; 37(3):469–74.
4. Bramara Neelima K, Saravanan T. Sample image watermarking study. Indian Journal of Science and Technology. 2015 Nov; 8(31):1–5.
5. Sharp T. An implementation of key based digital signal steganography. Proceedings of 4th International Workshop on Information Hiding, Springer LNCS. India. 2001 Oct; 2137:13–26.
6. Ker AD. Steganalysis of LSB matching in gray scale images. IEEE Signal Processing Letters. 2005 Jun; 12(6):441–4.
7. Mielikainen J. LSB matching revisited. IEEE Signal Processing Letters. 2006 May; 13(5):285–7.
8. Wang RZ, Lin CF, Lin JC. Hiding data in images by optimal moderately significant bit replacement. IEEE Electronic Letters. 2000 Dec; 36(25):2069–70.
9. Wang RZ, Lin CF, Lin JC. Image hiding by optimal LSB substitution and genetic algorithm. Elsevier Pattern Recognition. 2001 Mar; 34(3):671–83.
10. Puech W, Odrigues JM. A new crypto watermarking method for medical images safe transfer. Proceedings of the 12th European Signal processing conference (EUSIPCO’04); Vienna, Austria. 2004 Sep. p. 1481–4.
11. Cheng S, Wu Q, Castleman KR. Non-ubiquitous digital watermarking for record indexing and integrity protection of medical images. Proceedings of ICIP; Italy. 2005 Sep. p. 1062–5.
12. Acharya RU, Bhat PS, Kumar SLC. Transmission and storage of medical images with patient information. J Computers in Biology and Medicine. 2003 Jul; 33(4):303–10.
13. Memon NA, Gilani SAM, Ali A. Watermarking of chest CT scan medical images for content authentication. Proceedings of international conference on information and communication technologies; 2009 Aug. p. 175–80.