VOL. 9, NO. 8, AUGUST 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

CRYSTOGRAPHY BASED MEDICAL IMAGE SECURITY with LSB-BLOWFISH ALGORITHMS

C. Deepak Naidu[1], Srinivas Koppu[1], V. Madhu Viswanatham[2], and S.L Aarthy[1]
[1]School of Information Technology and Engineering, VIT University, Vellore, India
[2]School of Computing Science and Engineering, VIT University, Vellore, India
E-Mail: srinukoppu@vit.ac.in

ABSTRACT

Medical image data protection is very important as medical image sharing has increased tremendously. Cryptography and image steganography are two important fields that help in medical data security. The security of the medical images has always been a concern. The method proposed could be used to securely transfer the medical images over the internet. An approach is proposed to combine both concepts of steganography and cryptography together to attain various medical image security attacks. In the proposed framework, the message is embedded in the image. Blowfish algorithm is used for encryption and decryption of image. LSB algorithm is utilized to embed the message into the image. The proposed approach mainly concentrates on the confidentiality of patient information during the transfer of medical images over the internet.

Keywords: steganography, Blowfish, noise signal.

1. INTRODUCTION

Steganography and cryptography are two very common methods used for ensuring the security of the medical image data passed over in the internet. Cryptography gives away the fact that some important data is present and is encrypted. But the attacker will have to find the proper algorithm out of so many, which could have been used for encrypting and then figure out the data from the cipher text. Steganography on the other hand hides the fact that the carrier has something hidden in it. Many algorithms based on the two are available for the same. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and the intended receiver, knows the existence of the message. This differs from cryptography is the art of secret writing, which is used to make message unreadable by a third party but does not hide the existence of the secret communication. A steganographic image can appear as a picture, a video, an audio file, an article etc. [1, 2].

A combination of the algorithms of both steganography and cryptography has previously been tried. But the main focus was on the encrypting the message and hiding the message. In this paper an attempt has been made to combine the most effective algorithms of steganography and cryptography to secure the medical images. The method used in this paper combines the image steganography algorithm, Least Significant Bit (LSB) and the cryptographic algorithm, Blowfish. Blowfish has been used to encrypt the stego-image. The selection of algorithms was done merely on the basis of their efficiency. Least Significant Bit algorithm offers very high PSNR value and very less MSE. It is also very fast and takes very less embedding time. Blowfish has been proved to be the best among the many cryptographic algorithms and has stood the test of the time. A combination of these too could offer a very powerful security method and the same has been experimented in this paper.

2. LITERATURE SURVEY

The transfer of data from one end to the other is now made possible by the use of internet. This gives users a chance to develop and modify the data which is remotely located. This has positive as well as negative effects depending on the person using it. A few users can take advantage of these services to retrieve confidential information. Hence this confidential information should reach the correct receiver without being intervened by any malicious users [3].

It is not possible to avoid the data from reaching malicious users. Hence the data should be encrypted so that even if it reaches the hands of the attacker he/she should not have a clue regarding the presence of data, even if by chance they found out, it should be encrypted so that making it a challenge for them to figure out the information [3, 4].

Steganography is much preferred than cryptography as people do not sense of the message's existence as the message is hidden and thereby providing a way to avoid the attackers to raise a suspicion regarding the existence of message. It is safer to hide information than to communicate in encrypted form. Different media's can be used out of which digital images are the most popular because of their wide existence over the internet. There exists a variety of stegano graphic techniques to choose from, some are more complex than others and all of them have respective strong and weak points [5].

Watermarking is the practice of adding information about media in an unnoticeable way. Steganography and watermarking are very different in the objects they use for communication. However, in watermarking, the communication is the carrier data and the protection lie in the hidden data in the form of copyright protection; in steganography communication is the secret and the carrier one is just a cover. In a steganographic communication, in order to prevent

detecting the existence of the information, the method used for steganography would have been already agreed upon by both the sender and the receiver and a secret key too. In particular, this key is shared between the sender and the receiver. This is utilized to control the message embedding and extraction [1, 3].

The basic model of steganography consists of a carrier and a message. Carrier is also known as cover object, to which the message is embedded into and serves to hide the presence of message.

Message is the data that the sender wishes to keep confidential. It can be a plain text, cipher text, or may be another image, or anything that can be embedded in a bit stream such as copyright mark, a covert communication, or a serial number. The cover object with the secretly embedded message is called the stego-object [6].

There are many promising carriers that can be used as the cover object. Some of them are audio that uses digital audio formats such as wav, midi, avi, mpeg, mpi and voc; file and disk that can hide and append files by using the slack space; text such as null characters, just like morse code including html and java; image files such as bmp, gif and jpg, where they can be both colour and grayscale [7].

A digital image is represented as a matrix of numeric values. These numeric values represent the intensities for various points and they are called pixels. The raster data of the image is made up by these pixels. The bit depth is referred as the amount of bits in a colour scheme, and is the amount of nits that is utilized for every pixel. The tiniest bit depth within the present colour schemes is 8, i.e., 8bits are utilized to provide a description of every pixel's color. The 8 bits for every pixel are made use by monochrome and gray scales and they have the ability to present a total of 256 (2^8) different colours or gray shades [5].

Compression techniques are always given primary concern while choosing suitable steganographic algorithms. Using lossy compression increases the chance of losing part of the secret message as excess image data will be eliminated during compression. On the other hand, lossless compression prevents the loss of even the slightest portion of message, but it cannot compress the file into smaller sizes. Various steganographic algorithms have been proposed for both compression types [5].

The commonly used steganographic methods today are embedding secret information into digital images. These methods exploit the Human Visual System's (HVS) weakness. By exploiting HVS we can embed any confidential information in a digital image. While embedding the secret information into an image, the pixels of the image are altered according to the information that is being embedded [5].

The different subsections of image steganography are spatial steganography and JPEG steganography. Spatial steganography include Least Significant Bit (LSB) based steganography, Multiple Bit-planes based steganography, Noise-adding based steganography, Prediction Error based steganography, Modulo Operation based steganography and Quantization based steganography. JPEG steganography includes JSteg/JPHide, F5, OutGuess, MB and YASS [8].

Algorithms in Cryptography are divided into Symmetric and Asymmetric key cryptography. If only one key is used to encrypt and decrypt data it is symmetric key encryption. Key plays a vital role in both encryption and decryption. If a weak key is used in the algorithm then cryptanalysis will be easy. The size of the key is directly proportional to strength of symmetric key encryption. There are two types of symmetric algorithms namely block and steam ciphers. Block ciphers are operating on data in groups or blocks. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish are the examples. Stram ciphers operate on a single bit at a time. An example of stream cipher is RC4. Asymmetric key encryption consists of two keys, public and a private key. Public keys are public used for encryption whereas private keys are private and are used for decryption [9].

RSA is a strong encryption algorithm which, implements a public-key cryptosystem which helps in secure communications. RSA is slower than certain other symmetric cryptosystems. RSA is mainly used to securely transmit the keys for another less secure, but faster algorithm. There are many drawbacks for RSA algorithm, which can affect the security of the data, such as timing attacks and problems with key distribution [10]. RC2 is a 64-bits block cipher and has a variable key size (8 to128 bits). Such block ciphers are usually resistant to attacks but RC2 is not resistant to related-key attack. AES is the new encryption standard that has been recommended by NIST to replace DES. Rijndaelalgorithm was selected in 1998 after a competition to select the best encryption standard. The only effective attack known against Rijndael algorithm is Brute Force attack. Both AES and DES is block ciphers [11]. DES was the first encryption standard published by NIST (National Institute of Standards and Technology). DES is a symmetric algorithm that uses a 64-bit key. Out of 64 bits, 56 bits make up the independent key, and the rest 8 bits are used for error detection. Six entirely different permutation operations are used by DES, in the key expansion part as well as in the cipher part. Decryption of DES algorithm is same as that of the encryption but, the keys have to be applied in reverse order. The output of DES will be a 64-bit block of cipher text [9].

The superiority of the Blowfish algorithm over other algorithms in case of processing time has been proved time and again through various experiments. RC6 takes less time compared to all other algorithms, other than that of Blowfish. AES provides better time consumption and throughput than RC2, 3DES and DES. Compared to DES, since 3DES has to perform triple phase encryption, it performance is low in case of both power consumption and throughput. RC2 uses a key smaller than the ones other algorithms use, but still its performance and throughput are low [11].

A new LSB algorithm is proposed in the paper [12] which combines the idea of converting the original

message before embedding it in the cover-image and later changing the stego-image itself. Though not a proper encryption, the technique used for converting the original message and the stego-image serves it purpose of hiding the existence of the message well and fine. In the proposed method, a combination of Least Significant Bit (LSB) and Optical Pixel Adjusting Process (OPAP) techniques is used. The LSB method replaces the LSBs of the pixels with the bits of the message. In the proposed method, the original message is inverted before embedding it in the cover-image. The proposed method concentrates on the quality of the stego-image and hence before embedding the original message as such or the inverted message, the mean square error if calculated with each bit of the original message as well as the inverted image with the cover-image and whichever bit gives the least mean square error, is embedded into the cover-image. A bit string has to keep track of this embedding process to know which bit of which message (original or inverted) has been embedded. If the bit that has been embedded is from the original message, then the bit string will store 0 at the corresponding position and 1 if the bit is from the inverted message. This bit string can be called as a secret key that can be used to obtain the original message from the stego-image [12].

The improved LSB method explained above results in a good quality stego-image. It provides both encryption of the message as well a good quality image which is not possible by both the LSB and OPAP methods of steganography. The proposed method embeds the message very fast into the image and offers high capacity to hide data also. However, the secret key will be as big as the message and hence if the message is big then that is going to result in a big secret key [12].

An improvement to the Reversible Histogram Transformation Function (RHTF) has been proposed in the paper [13]. RHTF method was introduced to counter the RS steganalysis attack and to maintain the statistical features. But the vulnerabilities of RHTF method lie in the double-frequencies, zero pints and non-accurate detection problems. Hence RHTF is not very secure. In the proposed improvement, in order to solve the above mentioned vulnerabilities, cover selection, pixel grouping and dynamic secret-key adjustment schemes have been proposed. In the proposed method, the message is embedded into a properly chosen cover image that satisfies the proposed cover selection rules. Before embedding the message, the entire pixels of the cover image are grouped and each group has different secret key for embedding the message. The secret key is dynamically selected. In the process, after grouping the pixels, RHTF is applied to each group with their corresponding secret key. To the resultant image, the message is embedded using LSB and again RHTF is applied to the embedded image to produce the stego-image [13].

The stego-image produced thus has been proven to be very secure as it is impossible to figure out the dynamic secret keys without knowing the pixel grouping rules. Using the dynamic secret keys also diversifies the risk and hence the problems of double frequencies and zero points are nullified. The proposed method has been proved to be more resistant to the various steganalysis attacks than other methods. The PSNR (Peak Signal to Noise Ratio) value is average and close to LSB but better than RHTF method. However, recording secret keys in the stego-image is a concern [13].

The steganography method proposed in paper [14] encrypts the cover image itself before embedding the message. This encryption of cover image is done using scrambler. Scramblers are substitution ciphers that are less complex but very efficient. The encrypted cover image is then broken into bit planes and the message to be embedded is also divided into three variable length data vectors. The message is then embedded in the LSB plane and 2 subsequent ISB planes using three Pseudorandom Address Spaces (PAS). PAS is a collection of pseudo randomly generated addresses using a secret key. PAS has a Pseudo Noise (PN) Generator. In the proposed method, Linear Feedback Shift Register is used for generating PAS. Since the message is embedded using PAS, it ensures that the data is not embedded sequentially. To make the data extraction more difficult, Address Space Direction Pointer (ASDP) is used which determines the direction in which the address spaces are used for embedding the message. The stego-image has to be decrypted in descramble using the decryption key to obtain stego-image [14].

The use of PAS and ASDP make the method resistant to steganalysis attack and hence is secure. The image quality is good and the stego-image and the cover-image are very much similar. The method offers the stego images with a very good perpetual transparency. Hence the proposed method gives a high capacity and highly secure data hiding technique [14].

The method proposed in this study [15] uses Canny's Edge Detection and cat mapping to achieve security and safe embedding. Cat mapping is used to change the message prior to embedding it in the image. Cat mapping has a peculiar feature that we will get back the original message from the distorted message after a certain number of iterations. The steganography technique proposed consists of two phases. They are: Phase I - Payload Scrambling and embedding the message and Phase II - Extraction. During the payload scrambling, the original message is converted to distorted message using cat mapping. The required number of iterations for obtaining the original message back is found. The obtained distorted message is embedded into the cover image using a combination of matrix encoding and LSB matching. It uses edge adaptive LSB for embedding the message. The extraction process is the reverse of the said Phase I.

In the methodology explained in the above paragraph, the time taken to detect the edges raises proportionally with the increase in the number of pixels. The same happens in the case of memory space required as the image is stored as a matrix. The method is highly secure and provides high fidelity too. The distortion to the original image is negligible and cannot be identified easily

as it defies the Human Visual System and plays along its weaknesses. Though the proposed methodology offers lesser embedding time compared to other algorithms, LSB offers a better embedding time. The method is also resistant to steganalysis attacks. Though it has lots of advantages, the technique is not perfect as capacity is a shortfall for it and hence there is a scope for future work in the case of capacity as well as time complexity.

The proposed scheme in the paper [16] is an image encryption algorithm and it concentrates on removing the relationship of the geometry and statistical content in the image. The encryption part of the algorithm consists of sixteen rounds, each with a unique secret key. For each round the image is divided into blocks whose size is determined by the unique secret key of the corresponding round. As the authors of the paper believe that displacing the pixels of the image can break the relationship between the geometry and statistical content, during the diffusion process, they rearrange the pixels of each block in a zigzag path inside the same block itself. In substitution process, the properties of pixels of each block are changed by XOR-ing the pixel with its neighbour. The neighbour is chosen using an algorithm. Finally, during the mixing process, each pixel in the original image are replaced by a new pixel which is obtained by XOR-ing the current pixel, the previous pixel and the secret key for that particular round.

The proposed algorithm is highly secure, simple and easy to implement. Its uses lossless encryption and the encryption speed is fairly good. The key space is large and the encryption can be made stronger by increasing the number of iterations. As the encryption may fall apart during brute-force attack, a further improvement can be done based on that.

The steganographic technique proposed in this work [17] uses Tchebichef-based information hiding practise. The algorithm is based on three images, a carrier, a watermark and a hidden image. The watermark image is used to authenticate the hidden image. Both images are embedded in the carrier image. For the encryption purpose, all the three images are sub divided into equal number of blocks of size 4x4. Water image block and hidden image block are further scrambled before embedding to increase security. The Tchebichef moments of each block are then calculated and embedded in the same Tchebichef moments resulting in the stego-image. The extraction algorithm makes use of the watermark image to authenticate the hidden image. For this purpose, original watermark image is needed while extracting. The original watermark image is divided into blocks of size 4x4 and undergoes the same process mentioned above.

The proposed algorithm provides commendable security, high capacity, high imperceptibility, authentication and very good image quality. If tampered with, it can recover most of the data accurately and there is no actual loss of the data. Table-1 provides a summary of the methods described in this survey along with their advantages and drawbacks.

Table-1. Summary of literature survey.

Author	Method	Drawbacks	Advantages	Result
Cheng-Hsing Yang	Inverted Pattern Approach in LSB Substitution	Secret-key is as big as the message	Good quality stego-image, embeds the message very fast, high capacity.	It has been proved that the stego-image quality is better than that of optimal LSB substitution and OPAP LSB substitution methods.
Der- ChyuanIou, Chen-Hao Hu	LSB Steganographic method based on RHTF	PSNR value is average, recoding secret keys in the stego-image is a concern	Highly secure, PSNR value is better than RHTF, immune to statistical attacks	Security of the stego-images is significantly higher than for other LSB steganography, especially under higher embedding rates.
Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz, G.M. Bhat	Double layer security data hiding technique	Very complex computations, time consuming	Highly secure, high capacity, good stego-image quality	Experimental results show that the system produces good quality stego images with high capacity and security
Ratnakirti Roy, Anirban Sarkar, SuvamoyChangder	Chaos based edge adaptive image steganography	Time taken to detect edges and storage space increases with increase in the number of pixels, low capacity	Highly secure, high fidelity, less embedding time, resistance to steganalysis attacks	Capacity is a shortfall hence future work can be done on it.
Narendra K. Pareek, Vinod Patidar, Krishan K Sud	Diffusion-substitution based gray image encryption scheme	Vulnerable to brute force attack.	Highly secure, simple and easy to implement	The experiments indicate that the proposed scheme is simple, easy to implement (Hardware and Software) has high security and good speed.
S.M. Elshoura, D.B. Megherbi.	Full-gray-scale-level multi-image information hiding	Tampered data is not always recoverable.	Commendable security, high capacity, high imperceptibility, authentication and good image quality	The scheme showed robustness towards various attacks and distortions.
Zhi Yuan An, Haiyan Liu	LSB Algorithm	Easily vulnerable to attacks	High capacity	LSB is not the best but is still important in the case of data hiding
Nadeem Akhtar, PragatiJohri, Shah Baaz Khan	Bit inversion with LSB algorithm	Third party will be able to detect the presence of message	Good image quality, improved security	Other combinations of bits in the cover image can be considered for future work
VikasTyagi, Atul Kumar, Roshan Patel, SachinTyagi, Saurabh Singh Gangwar	LSB substitution	Easily vulnerable to attacks	Easy to implement, high capacity	The method can be used for digital watermarking in future

3. ALGORITHM

In the proposed method, a combination of steganography and cryptography has been applied. The method consists of three phases:

Phase-I: Image Steganography - Least Significant Bit Algorithm

Phase-II: Cryptography - Blowfish Algorithm

Phase-III: Decryption

Image is chosen as the media for the steganography process in this paper. The message to be hidden is first embedded into the cover image using Least Significant Bit algorithm and then the stego-image obtained in further encrypted using Blowfish algorithm. LSB is a common algorithm used for steganography and is comparatively efficient than many other algorithms. Similarly, Blowfish cryptography algorithm is one among the best cryptographic algorithms and hence the same was

used for the process. Both the phases are explained separately in the following sections.

Phase-I: Image Steganography - This is the first phase of the process. In this process the inputted message and the cover-image are both converted into their binary equivalents. Each bit of the message is embedded into each pixel's least significant bit and hence the algorithm is named Least Significant Bit algorithm. This process continues until all the bits of the message are embedded into the cover image, thus obtaining the stego-image. The step by step algorithm is given below:

Step-1: Input the message and convert it into its binary equivalent.
Step-2: Input the cover-image and convert the same into it corresponding binary-equivalent.
Step-3: Take the first bit of the message and replace the least significant bit of the first pixel's binary equivalent with the same.
Step- 4: Repeat Step-3, until the whole message is embedded in the cover-image.
Step-5: The final image obtained is the stego-image.

Phase-II: Cryptography - Cryptography is done using the Blowfish algorithm. Blowfish is a symmetric block cipher. It has a P-array which has 18 32-bit boxes (P1, P2,… P18). It also has S-boxes, which are 4 32-bit arrays (S1, S2, S3, S4) with 256 entries each. There are 16 rounds for this algorithm. The steps of the blowfish algorithm is given below
Step-1: The 64-bits data element is divided in two halves of 32-bits each (say L and R).
Step-2: L is then XOR-ed with P1 and the obtained 32-bits is passed to a function, say F.
Step-3: The function F, splits the 32-bit data into 4 8-bits and each are changed to 32-bits using the corresponding S boxes.
Step-4: The 4 32-bits obtained are again combined using XOR to finally obtain a 32-bit data.
Step-5: The thus obtained 32-bit data is XOR-ed with R and now L and R are exchanged. The process continues for another 15 rounds before the final encrypted data-element is obtained.

Phase-III: Decryption - Decryption process is always the reverse of the encryption process. Here, the encrypted image must be first decrypted using the Blowfish algorithm and then, the hidden message can be obtained from the stego-image.

4. SYSTEM ARCHITECTURE

The proposed system consists of two main modules for encryption and decryption and each has two sub-modules implementing image steganography using Least Significant Bit algorithm and cryptography using Blowfish algorithm. The first sub-module in the encryption module, takes in the input message and the cover image. It then embeds the message in the cover-image. The output from this module will be the stego-image. The stego-image produced by the first sub-module is used as an input by the second sub-module. It encrypts the stego-image using Blowfish algorithm to produce the encrypted image.

The first sub-module of the decryption module, take the encrypted image as the input and decrypts it using Blowfish algorithm. The stego-image thus reproduced is inputted into the second sub-module. Least Significant Bit algorithm is applied on the same to retrieve the hidden message from the stego-image. The system architecture is shown in the Figure-1.

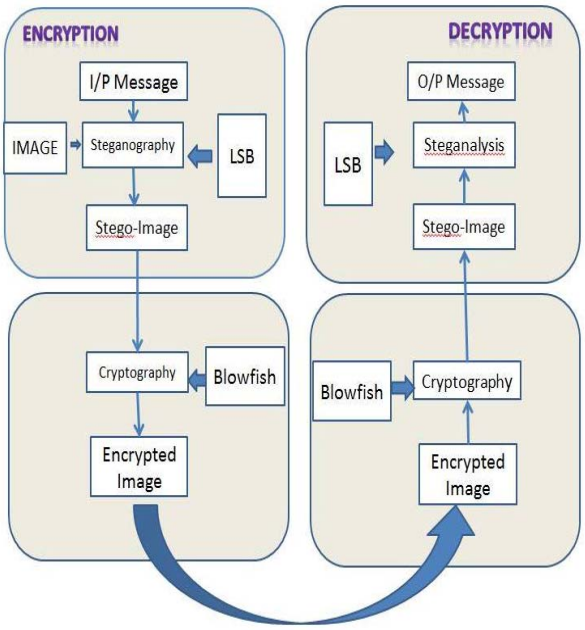

Figure-1. Proposed system architecture.

5. EXPERIMENTAL RESULTS

The experimental test was conducted on the processor, Intel Core i7-3610QM CPU, with a RAM of 6 GB. The experiment conducted has used 512x512 images. The message hidden in the images is 'Data Security using Cryptography and Image Steganography'. The Peak Signal to Noise Ratio and Mean Square Error values of the original image and the finally obtained image after decryption have been given in the table and the time taken in seconds for encryption process is also given in the Table. The Table-2 gives the PSNR and MSE values of the images given in the Figure-2 and the Table-3 shows the PSNR and MSE values of the images given in the Figure-3.

$$PSNR = 10log\frac{(2^n-1)^2}{MSE} = 10log\frac{(255)^2}{MSE}$$

$$MSE = \frac{1}{PQ}\sum_{j=1}^{P}\sum_{k=1}^{Q}(C_{j,k} - S_{j,k})^2$$

Table-2. The PSNR and MSE value for medical images.

Name of image	PSNR	MSE	Time
image 1	83.29	3.052e-4	0.624
image 2	82.77	3.433e-4	0.519
image 3	83.18	3.128e-4	0.910
image 4	82.79	3.413e-4	0.468
image 5	83.17	3.127e-4	0.680
image 6	83.18	3.128e-4	0.444
image 7	83.23	3.089e-4	0.572

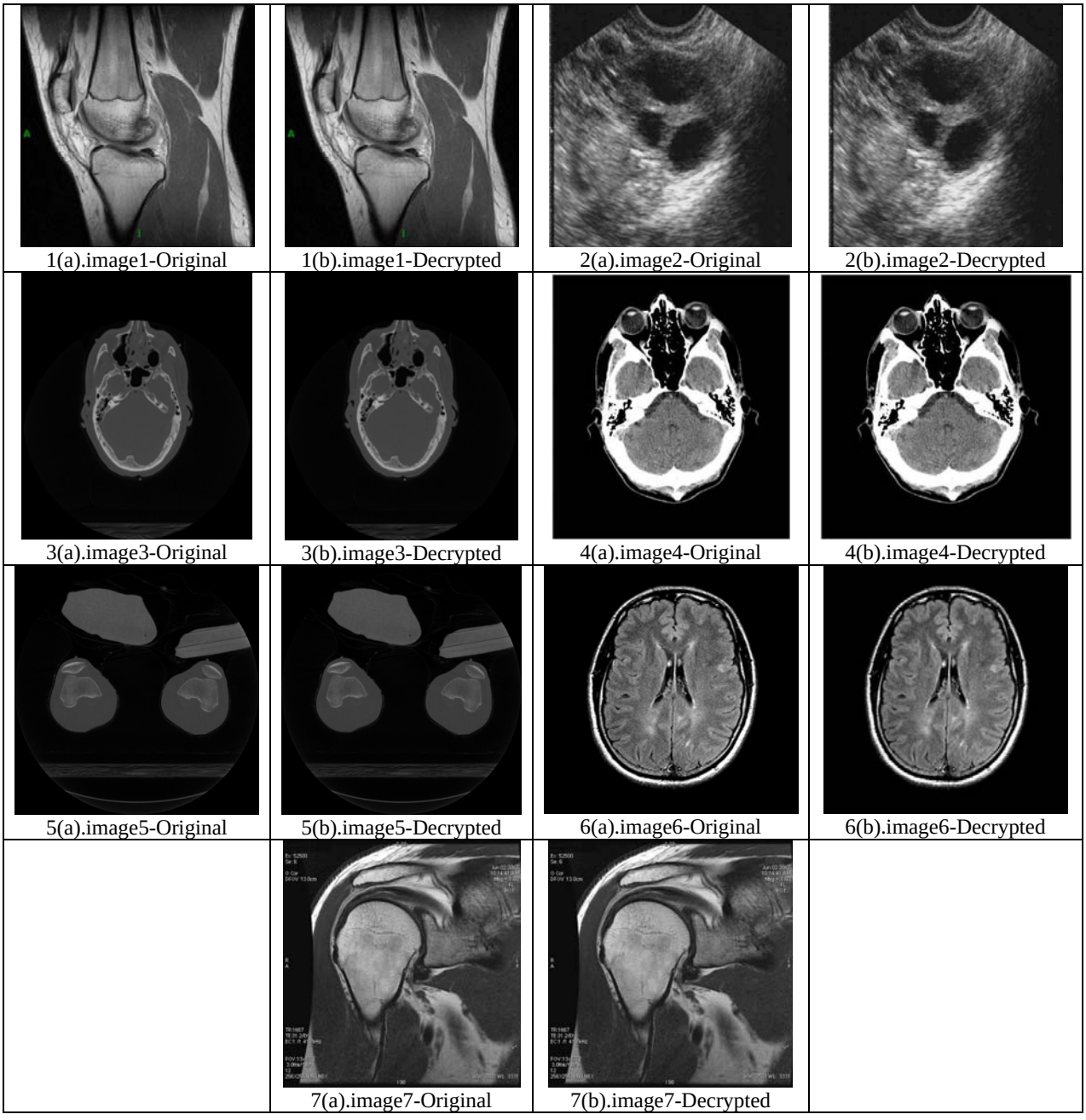

Figure-2. Experimental images before encryption and after decryption.

Table-3. The PSNR and MSE values of the test images given in Figure-3.

Image name	**PSNR** (dB)	**MSE**	**Time** (s)
Baboon	82.82	3.395e-4	.499
Barbara	82.97	3.281e-4	.494
Boat	83.45	2.937e-4	.552
Cameraman	83.23	3.089e-4	.559
Lake	82.63	3.547e-4	.513
Lena	83.34	3.014e-4	.487
Man	82.68	3.509e-4	.495
Peppers	83.51	2.899e-4	.484

Figure-3. Experimental images before encryption and after decryption.

6. CONCLUSIONS

In this paper an attempt was made to combine both steganography and cryptography. The method proposed uses the Least Significant Bit algorithm to embed the message in the image and the stego-image is encrypted using the Blowflow algorithm. The method enhances the security of the data. Experimental results show that the method offers high quality images and the MSE value is very less. However, the encrypted image when displayed shows an 'invalid image' which makes it obvious that the image has been tampered with and hence in future, enhancements can be made on this.

REFERENCES

[1] www.scribd.com/doc/54600936/.

[2] Hiding Plain Sight: Steganography and the Art of Covert Communication.

[3] Zhi Yuan An and Haiyan Liu. 2012 Research on digital watermark technology based on LSB algorithm. 4th International Conference on Computational and Information Sciences.

[4] Nadeem Akhtar, PragatiJohri and Shah Baaz Khan. 2013. Enhancing the security and quality of LSB based image steganography. 5th International Conference on Computational Intelligence and Communication Networks.

[5] SamerAtawneh, AmmarAlmomani and Putra Sumari. 2013. Steganography in digital images: Common approaches and tools. IETE journals.

[6] Keeping Secrets Secrets: Steganography with .NET.

[7] VikasTyagi, Atul Kumar, Roshan Patel, SachinTyagi and Saurabh Singh Gangwar. 2012. Image Steganography using Least Significant Bit with cryptography. Journal of Global Research in Computer Science.

[8] Bin Li and Junhui He. 2011. A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing.

[9] PratapChnadra Mandal. 2012. Superiority of Blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering.

[10] 2009. The RSA algorithm, EvgenyMilanov.

[11] Gurjeevan Singh, AshwaniSingla and K S Sandha. 2011. Cryptography algorithm comparison for security enhancement in wireless intrusion detection system. International Journal of Multidisciplinary Research.

[12] Cheng-Hsing Yang.2008. Inverted pattern approach to improve image quality of information hiding by LSB substitution. Pattern Recognition

[13] Der- ChyuanIou, Chen-Hao Hu. 2012. LSB Steganographic method based on reversible histogram transformation function for resisting statistical steganalysis. International Journal Information Science.

[14] Shabir A. Parah, Javaid A.Sheikh, Abdul M. Hafiz and G.M. Bhat.2014. Data hiding in scrambled images: A new double layer security data hiding technique. Computers & Electrical Engineering

[15] Ratnakirti Roy, Anirban Sarkar and SuvamoyChangder.2013. Chaos based Edge Adaptive Image Steganography. First International Conference on Computational Intelligence: Modeling Techniques and Applications.

[16] Narendra K. Pareek, Vinod Patidar and Krishan K Sud.2013.Diffusion-substitution based gray image encryption scheme. Digital Signal Processing

[17] S.M. Elshoura and D.B. Megherbi.2013.A Secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments. Signal Processing: Image Communication