Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.376 – 385

RESEARCH ARTICLE

An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography

Navita Agarwal[1], Himanshu Sharma[2]
[1]Assistant Professor, Moradabad Institute of Technology, Moradabad, India
[2]Assistant Professor, Institute of Foreign Trade and Management, Moradabad, India

[1] nvgrwl06@gmail.com; [2] cs.himanshu@gmail.com

Abstract— With fast growing network, many people utilize the internet to transfer digital image information. The need of the time is to implement an extremely securable, economic and perfect system of image encryption that can be well protected from unauthorized access. Also, the bulk size of the image data produces many problems in their transmission via internet. So, in this paper, a very new and combined approach for DCT based image compression, pixel shuffling based encryption, decryption and steganography is proposed for real-time applications and also comparison is done with the traditional lowly securable key-based encryption algorithm to show the effectiveness of the proposed algorithm.

Key Terms: - Image Security; DCT; Compression; Pixel Shuffling; Encryption; Decryption; Image Hiding; Steganography

I. INTRODUCTION

In today's scenario, Internet has become a crucial part of each and every aspect of society moulding the way how we live, work and communicate. But the security and the privacy of information especially the images data which is transferred via internet from unauthorized access is becoming a major concern. Large numbers of security approaches have been used in this regard like applying encryption and decryption which comes under the cryptography, steganography, etc.

A. Cryptography

Cryptography is derived from the Greek word κρυπτός [1] which means hidden. It is the art of procedures with the aim of securing the communication from the unauthorized access or the third parties. It also includes certain prospects of information security like confidentiality of the data, integrity of the data, authentication, and non - repudiation. There are two types of techniques which are involved in Cryptography – Encryption and Decryption.

1) Encryption: When the original data (Plain text) is changed into unreadable form (Cipher text), this process is known as encryption. Cipher text may not be understood by any unauthorized person. The process of encryption always occurs at sender's side.

Although encryption all alone can secure the information confidentiality, but it is the need of the time to use large number of complex security systems to maintain the secrecy of information. E.g. Confirmation of a Message Authentication Code (MAC) or a Digital Signature.

2) Decryption: When the encrypted data (Cipher text) is changed into original form (Plain text), this process is known as decryption. The process of decryption always occurs at receiver's side.

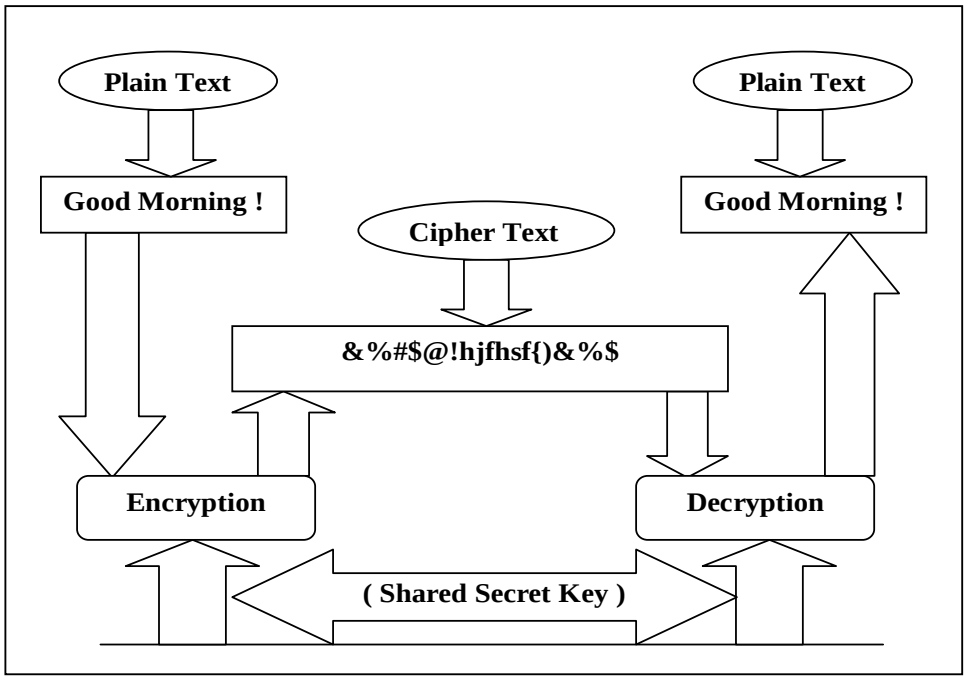

Fig. 1 Process of Encryption and Decryption

B. S*teganography*

In the past few years, the employment of Word Wide Web has increased tremendously. Along with this, many people start using the tools to work with multimedia information. Today, people prefer to employ the network as the important medium for transferring all their day to day confidential information. Here comes the Steganography which provides extensive security from the unauthorized access for the transmission of confidential information. The word steganography is derived from the Greek word "stegos" meaning "cover" and "graphia" meaning "writing", so in this way it has the full meaning "covered writing". In image steganography, the information is hidden exclusively in images. In today's world, there is a big requirement to secure the information from misusing by wrong hands because of many flourishing factors like electronic eavesdropping, electronic connectivity, electronic fraud, viruses and hackers. So, the need of the time is to bring into consideration the multimedia security [2] and disseminating the safety of digital information.

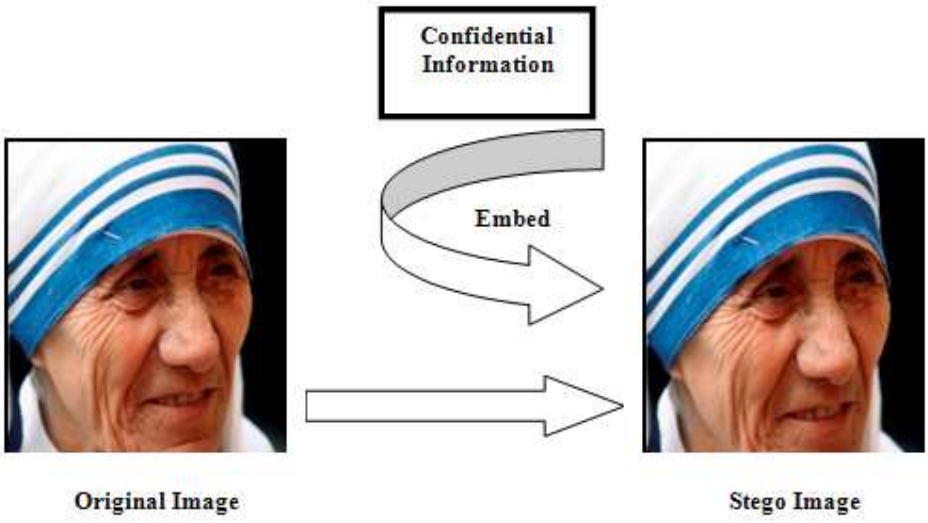

Fig. 2 Image Steganography

Fig. 2 Image Steganography

C. Compression

Many people on the internet have a great concern for secrecy and privacy of the information. Image steganography permit the two parties so that they can transmit their information confidentially. The size of the images increases very high in order to communicate them over secure channel when inputs are assumed to be the images of larger bit depth. Procedures must be used to reduce the size of the images in order to exhibit an image in very less time.

So, here comes the compression which acts as crucial phenomena in deciding which steganographic technique to employ. There are two types of compression - Lossy compression and Lossless compression. Lossy compression procedures are efficient in bringing down the size of the images with the condition that the engrafted message may be partly lost as the excess image data will not be there. On the other hand, Lossless compression maintains the originality of the images and not reduces the size of the images.

II. RELATED WORKS

The security of information system is directly related to the efficient working of the key management scheme that it follows. But the key management schemes that are available presently lack in their efficiency to avoid security threats and the flaws of the system. So, Xuanwu et al. [3] proposed a threshold key management scheme based on ECC (Elliptic Curve Cryptosystem). The proposed concept gained the threshold management of symmetric key and Public Key Certificate (PKC) by exchanging the secret key and using the encryption algorithm based on probability in key management. Suli Wu et al. [4] proposed a novel encryption algorithm based on shifting and exchanging rule of bi-column bi-row circular queue. This algorithm used the concept of random number for choosing the sub – matrix in a random manner and focused on the creation of a scrambling matrix from the plain text matrix which would avoid all the problems for decryption. However it still had some shortcomings. Firstly, a limited number of operations could be performed on the matrix by this algorithm. Secondly, it used the concept of key and its recording in the key file which could become its greatest weakness.

Vinod Patidar G. Purohit et al. [5] proposed an image encryption technique through a novel permutation-substitution scheme based on chaotic standard map. In this technique, every round of encryption contained three stages namely permutation rounds, substitution rounds and again permutation rounds. The process of permutation and substitution were performed row-by-row and column-by-column instead of pixel-by-pixel in order to accelerate the speed of encryption. The controlling of permutation process was done by the usage of Pseudo Random Number Sequences (PRNS). On the other hand, In the process of substitution the attributes of pixels of rows and columns of various layers were merged with the PRNS created from the standard map. Huan Zhang et al. [6] proposed an image encryption algorithm based on bit-plane scrambling and multiple chaotic

system combination in which the compounding of transposition of position of pixels and the changing of pixel values was done. The outcomes proved that the proposed technique of image encryption algorithm achieved benefits of large key space, owing of excellent confusion attributes, good resistance capability from various types of attacks and a high level of sensitivity with regard to the original image and the secret key.

S V V Sateesh et al. [7] proposed an optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm which payed great emphasis in lowering down the arithmetic complexity. A new technique for concurrent image compression and encryption for increased level of security was implemented for real time applications. The outcomes displayed the compression ratio to be 66%. Lalitha G. et al. [8] proposed the secure transmission of information using image steganography. Actually, the security of confidential information was very difficult to preserve as organization contains extensive amount of data at one site. So, this technique was taken into consideration. The input messages of any digital format were taken and addressed as a stream of bits. Firstly, the image to be transmitted was compressed using the wavelet compression. Then encryption was done using RSA public key encryption algorithm. RSA was considered the simplest and easiest to implement encryption algorithm of all the public-key algorithms. Lastly, they were embedded in another image. The results were good but they involved very old cryptographic algorithm for encryption.

Nidhi Sethi et al. [9] proposed a new cryptology approach for image encryption. This algorithm was based on logistics and used Haar wavelet transform to disintegrate the image. It generated cipher of high quality having excellent diffusion and confusion attributes. The outcomes produced a securable system for the effective transmission of the images.

During signal transmission, encryption can be employed to forbid the third party organizations from realizing the raw data and misusing it. In the current era of violation of security and misuse of the confidential information, various encryption techniques can be used for raising the security of digital contents. So, Quist-Aphetsi Kester [10] proposed a new cryptographic image encryption algorithm for encryption of the images of size m * n by disordering the values of RGB pixels.

III. PROBLEM DEFINITION

In today's world, as the technologies related to network and internet is growing fastly, so the security of communication of information especially images is of prime concern. Furthermore, the security of images is a very hot topic of research in various areas like information security, secure communication and copyright protection. Image encryption all alone cannot be a perfect measure in this regard. This should be combined with more aspects of information security to increase the efficiency of the transmission and its protection from various attacks by the unauthorized parties. So, this approached is proposed that combine the image compression, image encryption, image decryption and image steganography in one system to achieve the highest level of security.

IV. PROPOSED METHODOLOGY

A. Image compression using Discrete Cosine Transform (DCT)

DCT is widely used for image compression as it provides very less computational complexity and minimizes the space required for data transmission. It can be very well used with large number of image standards like JPEG, CCITT, MPEG-2 and MPEG-4 and so on. So, here is a DCT [11] based algorithm that can perform image compression in a well manner.

Algorithm:

1. The original image is partitioned into blocks or groups of 8 x 8.
2. A black and white image has pixel values of range 0 - 255 and Discrete Cosine Transform is capable to act on pixel values having range -128 to 127. So, every block needs to be changed to act in the particular range.
3. Discrete Cosine Transform matrix is calculated by the equation -

$$C(u,v) = D(u)\, D(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} (x,y) \cos\left[(2x+1)u\pi / 2N\right] \cos\left[(2y+1)v\pi / 2N\right]$$

Where u, v = 0, 1, 2, 3… N - 1

4. Then multiply the changed block with Discrete Cosine Transform matrix on the left and the transpose of Discrete Cosine Transform matrix on the right by employing Discrete Cosine Transform to every block or group.
5. Now compress each and every block or group with the help of quantization.
6. Next perform the entropy encoding for the Quantized matrix.
7. Apply the reverse procedure to redevelop the compressed image.
8. Lastly apply the Inverse Discrete Cosine Transform for performing decompression of images which is given by the equation –

$$f(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} D(u)\, D(v)\, D(u,v) \cos[(2x+1)u\pi/2N] \cos[(2y+1)v\pi/2N]$$

Where $D(u) = (1/N)^{\wedge} 1/2$ **for** $u = 0$ **&** $D(u) = (2/N)^{\wedge} 1/2$ **for** $u = 1, 2, 3\ldots\ldots, (N-1)$

B. Image Encryption using Pixel-Shuffling

Considering an image of 8X8 where the values in the matrix represent the pixel values.

20	26	23	60	10	30	22	45
20	15	20	20	76	20	20	20
20	20	46	20	20	20	26	20
32	76	20	20	36	20	20	46
00	20	32	20	55	20	87	20
20	46	20	33	20	26	20	16
20	20	46	20	46	20	38	20
23	20	20	20	20	37	20	49

Fig. 3 Original Image

Algorithm:

1. Consider image to be divided into 2 columns like (1 column and 2column), (3 column and 4 column) and so on. Now perform swapping operation on the columns i.e. swap the values of 1st and 3nd columns.
2. Now swap values of 2nd and 4th columns.
3. In the similar manner, swap the 5th and 7th columns and then 6th and 8th columns. Follow the similar procedure for all the columns in the image.
4. Now increase the length column block to 4 and then swap the values in the similar manner as that for the column block size 2.
5. The procedure of incrementing the block size and the swapping of values is carried out according to the need or maximum it can be done up to the case till complete image is divided into 2 blocks. When complete processing is done column wise, then move on to process in the similar manner for the rows.
6. When processing the image row wise, firstly swap the pixel values of 1st and 3rd rows and then swap pixel values of 2nd and 4th rows.
7. In the similar manner, swap 5th and 7th rows and then 6th and 8th rows. Follow the similar procedure for all the rows in the image,
8. Now increase the length of row block to 4 and then swap the values in the similar manner as that for the row block size 2.
9. The procedure of incrementing the block size & swapping of values is carried out according to the need or the maximum it can be done up to the case till complete image is divided into 2 blocks of rows. When complete processing is done row wise, it marks up the end of the encryption process and the image is the final encrypted image.

38	20	46	20	46	20	20	20
20	49	20	37	20	20	23	20
87	20	55	20	32	20	00	20
20	16	20	26	20	33	20	46
26	20	20	20	46	20	20	20
20	46	36	20	20	20	32	76
22	45	10	30	23	60	20	26
20	20	76	20	20	20	20	15

Fig. 4 Encrypted Image

C. Image Decryption using Pixel-Shuffling

Now the process of decryption is performed on the encrypted image.

Algorithm:

1. The process of decryption is carried out in just reverse manner by applying decryption method on the encrypted image to obtain the original image.
2. Now apply column operation beginning from the largest block size and going to the smallest block size. In the example, the largest block size was 4, so firstly swap the 4 block size columns.
3. Now reduce the block size to 2 and swap 5^{th} & 7^{th}, 6^{th} & 8^{th} column.
4. Now swap 2^{nd} and 4^{th} column, 1^{st} and 3^{rd} column with block size 2.
5. As this process cannot be continued by reducing column block size, so stop here and now perform the same operation on rows. For this, firstly consider the image's largest block size 4 and swap the rows.
6. Now reduce block size to 2 and swap 5^{th} and 7^{th}, 6^{th} and 8^{th} rows.
7. Again swap 1^{st} and 3^{rd} rows and 2^{nd} and 4^{th} rows.
8. As no further reduction is possible in row block size, so stop here. This is the original image which was encrypted by the encryption algorithm.

D. Image Steganography

Image Steganography [12] provides more security to the encrypted image.

Algorithm:

1. Add the encrypted image to win rar archive.
2. Apply DOS commands to hide the win rar file behind a new image.
3. Finally, the stego image is obtained.

V. ARCHITECTURAL SUMMARY OF THE PROPOSED APPROACH USING FLOW CHART DIAGRAM

A. Flowchart for DCT compression

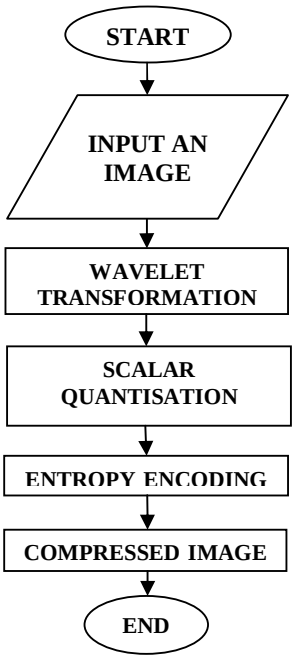

Fig. 5 Flowchart for DCT compression

B. Flowchart for pixel-shuffling encryption

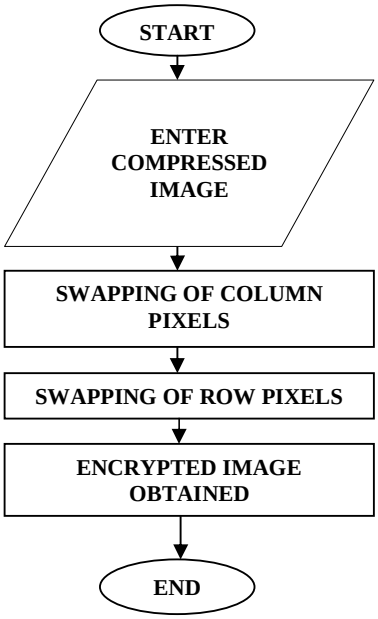

Fig. 6 Flowchart for pixel-shuffling encryption

C. Flowchart for pixel-shuffling decryption

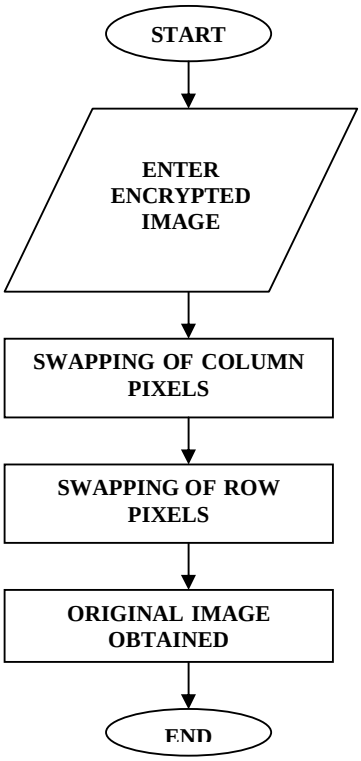

Fig. 7 Flowchart for pixel-shuffling decryption

D. Flowchart for steganography

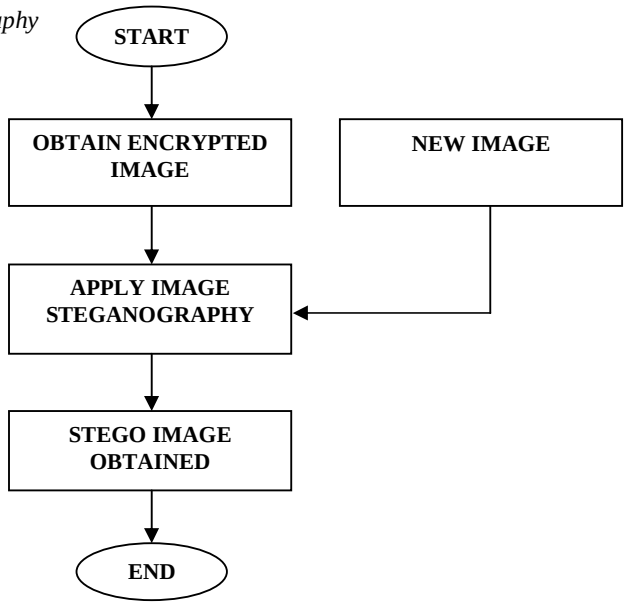

Fig. 8 Flowchart for steganography

E. Flowchart for complete work

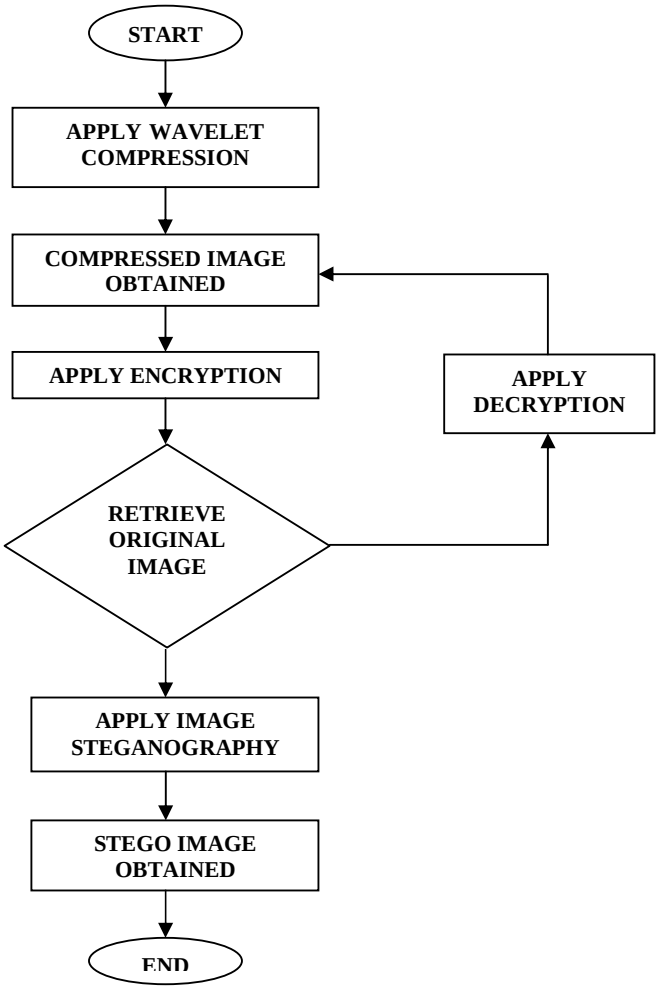

Fig. 9 Flowchart for complete work

VI. SIMULATED RESULTS AND DISCUSSIONS

The outcome of out-dated and very less securable key-based image encryption system is presented here in order to compare it with pixel-based encryption.

Fig. 10 Original Image

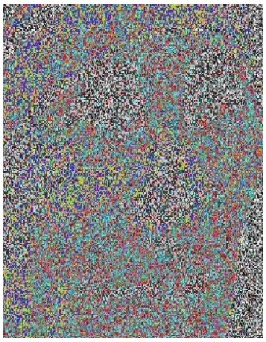

Fig. 11 Encrypted Image

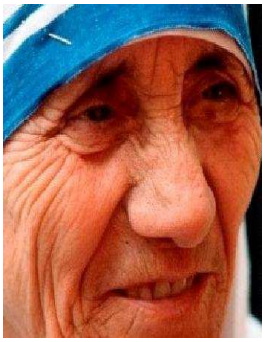

Fig. 12 Decrypted Image

The simulation of the proposed approach was performed on MATLAB version 7.8.0.347 to affirm the effectiveness of the proposed algorithm. The size of the input image was assumed to be m * n.

The output of the MATLAB code written and tested for the proposed approach is shown below-

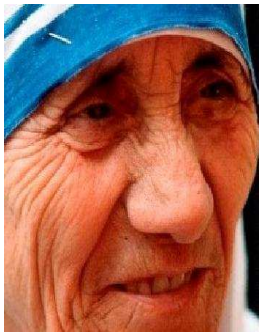

Fig. 13 Original Image

Fig. 14 Compressed Image

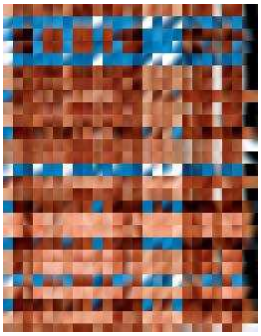

Fig. 15 Encrypted Image

Fig. 17 Decompressed Image

Fig. 16 Stego Image

On the basis of these results and the required data collected from the related works, a comparison can be done between the existing and proposed system on the basis of certain attributes and following values can be predicted.

TABLE I

Image Encryption Techniques /Characteristics	Requirement of Bandwidth (%)	Level of Security (%)	Efficiency (%)
Key-Based Image Encryption	100	Approx 50	Approx 60
Pixel-Shuffling Based Image Encryption	Approx 50	Approx 90	Approx 95

VII. CONCLUSION

In this paper, we have presented a technique for the image data to be transmitted securely. Our applied technique reduces the requirement of bandwidth by image data when transmitted over the network. Pixel – Shuffling Based Encryption has been applied over the image so that it can be safely transmitted from the sender to the receiver end, protecting the secret image from an unauthorized access. Image steganography technique hides the secret image that have to transmit to the receiver end behind another image securely. So, this combined approach hides the existence of secret image making it almost impossible to snoop in the network, provides extremely high security and consumes very less space as compared to the traditional key-based encryption techniques.

VIII. FUTURE DIRECTIONS

In future, two or more functionalities can be added to the proposed approach which will allow performing many more operations and thus more securing the confidential data from unauthorized access while it is being transmitted over the internet. By increasing the compression ratio, the size of the image which is being transmitted over the network can further be reduced and thus the image will occupy lesser bandwidth of the network. By adding the functionality of conversion of text or audio data, firstly it needs to be converted into image and then applying all the procedures presented in our thesis work.

REFERENCES

[1] (2001) The Wikipedia website. [Online]. Available: http://en.wikipedia.org/wiki/Cryptography
[2] Dr. Gabriel Cristobal, Prof. Dr. Peter Schelkens, Prof. Hugo Thienpont, Bing Qi, Li Qian and Hoi-Kwong Lo, "Optical and Digital Image Processing: Fundamentals and Applications," Canada: Wiley-VCH Verlag GmbH & Co. KGaA, 29 April 2011
[3] Xuanwu Zhou, Ping Wei, "Key Management Scheme Based on (t, n) Threshold Cryptosystem," Intelligent System and Knowledge Engineering, IEEE Proceedings of 3rd International Conference on, 2008, pp. 1288-1293.
[4] Suli Wu, Yang Zhang, Xu Jing, "A Novel Encryption Algorithm based on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue," Computer Science and Software Engineering, IEEE International Conference on, 2008, pp. 841-844.
[5] Vinod Patidar G. Purohit, K. K. Sud, N. K. Pareek, "Image encryption through a novel permutation-substitution scheme based on chaotic standard map," Chaos-Fractal Theory and its Applications, IEEE International Workshop on, 2010, pp. 164-169.
[6] Huan Zhang, Ruhua Cai, "Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic Systems Combination," IEEE Journal, 2010, pp. 113-117.
[7] S V V Sateesh, R Sakthivel, K Nirosha, Harish M Kittur, "An optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm," Signal Processing, Communication, Computing and Network Technologies (ICSCCN), IEEE Proceedings of International Conference on, 2011, pp. 442-447.
[8] Lalitha G, Ashish Jain, U. Raja, "Secure Transmission of Compound Information Using Image Steganography," International Journal on Computer Science and Engineering (IJCSE), vol. 3 no. 4, April 2011, pp. 1645-1648
[9] Nidhi Sethi, Deepika Sharma, "A New Cryptology approach for Image Encryption," Parallel, Distributed and Grid Computing, IEEE 2nd International Conference on, 2012, pp. 905-908
[10] Quist-Aphetsi Kester, "A cryptographic Image Encryption technique based on the RGB Pixel shuffling," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, issue 2, January 2013, pp. 848-854
[11] (2008) Cardiff School of Computer Science and Informatics Website. [Online]. Available: http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html
[12] The Hacking Tutorial Website. [Online]. Available: http://www.hacking-tutorial.com/tips-and-trick/hide-secret-file-inside-an-image-steganography/

