The Algorithm:

Step 1. Import data from secret fingerprint image (hide).

Step 2. Extract the secret image size (row, column).

Step 3. Determine the first pixel to read image.

Step 4. Determine the encrypt method, to encrypt the image from outside to inside (O2I), or an inverse (I2O).

Step 5. Determine the direction, to encrypt the image by clockwise or anticlockwise.

Step 6. Apply encryption algorithm (Apply Image2spiral).

Step 7. Import data from Landscape image (Cover).

Step 8. Resize the Landscape image (row, column) to the same size secret image.

Step 9. Apply LSB (Landscape image and the secret image).

Step 10. Finally the image will be converted into stego-image format.

The inverse of the algorithm will decrypt the encrypted image back into the secret fingerprint image.

VII. EXPERIMENTALRESULTS

In this research we would be obtaining our results by hide and encryption fingerprint image in simulating the image processing in MATLAB for better security. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) [38]. In proposed method, firstly we would be obtaining the matrix and pixels of the chosen image and then we would be encrypting the image using spiral algorithm. The result shows the fingerprint image, encrypted image and the decrypted image as shown in Table 1. We will clearly see that the decrypted image is same as the originalimage.

After enciphering the fingerprint image, these encrypted image are embedded in JPG image file by using LSB steganography technique. In order to minimize the visible effect of changes to pixel values, the value of PSNR of stego image must be as high as possible. The MATLAB code for the spiral algorithm was written and tested. They are used three landscape with three fingerprint images in simulation proposed method as in Table 2. From Table 3 cannot observation the change between cover image and stegoimage.

Table 1. Fingerprint Image before and after Encryption.

Finger rint Image	Finger print	Encrypted	Decrypted
Finger print Image 1			
Fingerprint Image 2			
Fingerprint Image 3			

To analyze the quality of the embedded texture image, with respect to the original, the measure of PSNR has been employed [38]. Generally speaking, when the payload increases, the MSE will increase, and this will affect the PSNR inversely [38]. So, from trade-off it was found that MSE decrease causes PSNR increase and vice- versa. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego- image should strive for 40 dB and above [39]. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR [39]. The obtained results of the experiments are summarized in the Table 2.

Fingerprint Image size (Before Encryption)	Fingerprint Image size (After Encryption)	MSE	PSNR
Fingerprint image 1 (62.1 kb)	Fingerprint image 1 (52.9 kb)	0.4212	55.7968
Fingerprint image 2 (58.3 kb)	Fingerprint image 2 (51.7 kb)	0.4150	55.8610
Fingerprint image 3 (79.5 kb)	Fingerprint image 3 (64.6 kb)	0.4384	55.6225

Table 2.MSE and PSNR values for the Cover and Stego images.

Table 3.Cover and Stego image.

Cover Image	Cover Image	Stego Image
Cover Image 1		
Cover Image 2		
Cover Image 3		

To measure the distortion introduced by the embedding in the cover-image, the PSNR after embedding was observed for some images. It was found that the PSNR is constantly above 55 dB as seen in Table 3 which means that the quality degradations could hardly be perceived by a human eye.

VI. CONCLUSION

Steganography is not a good solution to secrecy, but neither is encryption. But if these methods are combined, we will have two layers of protection. If a fingerprint image is encrypted by transposition spiral algorithm and hidden with a LSB steganography method thus we can hide large volume of data. In this paper, we described well known steganography techniques used to hide image in stego image that use the least significant bit insertion method. This paper presents a spiral algorithm for encryption fingerprint image and embeds in color image. The swapping of fingerprint image pixel has increased the security of the image against all possibleattacks available currently. The main focus of the paper is to develop a system with extra security features where a meaningful piece of image can be hidden by combining two basic data hiding techniques. The method can further be extended with taking into account other data hiding

and encryption techniques. The proposed method satisfies the requirements such as capacity, security and robustness which are intended for data hiding. The obtained experimental results show that, the proposedmethod will be a good and acceptable.

REFERENCES

[1] Raphael, A. J. and Sundaram, V. "Cryptography and Steganography – A Survey", Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630 ,ISSN:2229-6093

[2] S. Craver, On Public-key Steganography in the Presence of an Active Warden, IBM Research Report RC 20931, July 23,1997.

[3] Nicolas Courtois, JosefPieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT 2002.

[4] Younes, M.A.B. and Jantan, A. (2008), "Image Encryption Using Block-Based Transformation Algorithm" International Journal of Computer Science, Vol. 35, Issue.1,pp.15-23

[5] PiaSingh ,Karamjeet Singh "IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB", International Journal of Scientific & Engineering Research, Vol 4 (7), pp 150-154,July-2013.

[6] D.Stinson, "Cryptography: Theory and Practice", second edition, CRC Press, Boca Raton,1995.

[7] Abraham Sinkov, "Elementary Cryptanalysis: A Mathematical Approach", Mathematical Association of America, 1966. ISBN0-88385-622-0.

[8] Kester, Quist-Aphetsi. "A cryptosystem based on Vigenère cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1, no. 10 (2012):pp-108.

[9] Visual cryptography retrieved from:http://en.wikipedia.org/wiki/Visual_cryptography.

[10] M. Salleh, S Ibrahim and I.F. Isnin, "Image encryption algorithm based on chaotic mapping", JurnalTeknologi, 39(D) Dis. 2003: 1–12 UniversitiTeknologiMalaysia

[11] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) "Information Hiding -A Survey", Proceedings of the

IEEE, Special issue on Protection of Multimedia Content, vol. 87, no. 7,pp.1062-1078

[12] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal v 35 no 3-4 (96) pp313-336.

[13] Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of Sscience and Technology, Vol.9, No.II, pp.83-103, ISSN:0975-2773.

[14] Samer H. Atawneh, "A New Algorithm for Hiding Gray Images using Blocks", the proceedings of ICTTA '06: IEEE - 2nd International Conference on Information & Communication Technologies: From Theory to Applications, Damascus, Syria, 24-28 April, 2006, ISBN:0-803-9521-2.

[15] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series: 9in x 6in,pp.1-31.

[16] Chandramouli, R. and Menon, N. (2001), "Analysis of LSB based image steganography techniques", IEEE Proceedings on Image Processing, Vol.3,pp.1019-1022.

[17] Tiwari, N. and Shandilya, M. (2010), "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", International Journal of Computer Applications (0975 – 8887) Vol. 6,no.2,pp.1-4.

[18] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), "Implementation of LSB steganography and Its Evaluation for Various Bits", 1st International Conference on Digital Information Management, pp.173- 178.

[19] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose,CA,2003.

[20] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Fall 2003 Volume 2, Issue2.

[21] R., Chandramouli, and NasirMemon.(2001), "Analysis of LSB based image steganography techniques." In Image Processing, 2001. Proceedings. 2001 International Conference on, IEEE, vol. 3, pp.1019-1022.

[22] Karen, Bailey, and Kevin Curran.(2006)

"An evaluation of image based steganography methods" Multimedia Tools and Applications, Springer Vol.30, no. 1, pp.55-88.

[23] E. Franz, A. Jerichow, S. Moller, A. Pftizmann, I. Stierland, "Computer Based Steganography", in Information Hiding, Springer Lucture Notes in Computer Science v 1174 (1996) pp7-21.

[24] B. Pfitzmann, "Information Hiding Termonology", Proc. First Int'l Workshop Information Hiding. Lecture Notes in Computer Science No. 1,174, Springer-Verlag, Berline, 1996, pp.347-356.

[25] MamtaJuneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Inssertion and Encryption", 2009IEEE.

[26] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy, " Implementation of LSB Steganography and its Evaluation for Various File Formats", Int.J.Advanced Networking and Applications, Volume: 02,2011

[27] Neha Sharma, Mr.J.S.Bhatia, Neena Gupta, "An EncryptoSetgo Technique based secure data transmission system", PEC, Chandigarh, May,2005.

[28] Krishnan, G.S.; Loganathan, D.; , "Color image cryptography scheme based on visual cryptography," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on , vol., no., pp.404-407, 21-22 July2011

[29] Christy, J.I.; Seenivasagam, V.; , "Construction of color Extended Visual Cryptographic scheme using Back Propagation Network for color images," Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on , vol., no., pp.1101-1108, 21-22 March2012.

[30] Kester, Quist-Aphetsi; ,"A public-key exchange cryptographic technique using matrix," Adaptive Science & Technology (ICAST), 2012 IEEE 4th International Conference on , vol., no., pp.78-81, 25-27 Oct.2012.

[31] ShujiangXu,YinglongWang,YucuiGuo,Cong Wang, "A Novel Image Encryption Scheme based on a Nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68,2010

[32] RuisongYe,Huiqing Huang, "Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking", IJIGSP, vol.2, no.1, pp.19-29,2010.

[33] AmneshGoel,NidhiChandra,"A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement", IJIGSP, vol.4, no.2, pp.16- 22,2012.

[34]   Sokouti, M., Sokouti, B. and Pashazadeh, S. (2009), "An approach in improving transposition cipher system", Indian Journal of Science and Technology, Vol.2 No. 8, pp. 9-15, ISSN: 0974-6846.

[35]   Giddy, J.P. and Safavi- Naini, R. (1994), "Automated Cryptanalysis of Transposition Ciphers", The Computer Journal, Vol.37, No.5, pp. 429-436.

[36]   Mathworks, 2014 Website: http://www.mathsworks.com.

[37]   Kahate, A. (2008), "Cryptography and Network Security", 2nd Edition, TataMcGraw-Hill.

[38]   Kaur, R., Singh, B. and Singh, I. (2012), "A Comparative Study of Combination of Different Bit Positions In Image Steganography", International Journal of Modern Engineering Research, Vol.2, Issue.5, pp-3835- 3840.

[39]   Ulutas, G., Ulutas, M. and Nabiyev,V. (2011), "Distortion free geometry based secret image sharing", Elsevier Inc, Procedia Computer Science 3,pp.721–726.