International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Special Edition, Apr 2015, 21-30

HYBRID APPROACH FOR HIDING AN IMAGE USING VIDEO STEGANOGRAPHY

G. R MANJULA[1] & AJIT DANTI[2]

[1]Department of CSE, JNN College of Engineering, Shimoga , India

[2]Department of MCA, JNN College of Engineering, Shimoga , India

ABSTRACT

The paper presents a hybrid approach for concealing the existence of an image in a video file. Secret image is encrypted and embedded into cover video using a hybrid method that uses both hash based 3-3-2 LSB and index channel technique in spatial domain. Two metrics MSE and PSNR are measured and experimental results shows that the resulting stego video has less distortion and this stego system is more secure.

KEYWORDS: Cover Video, Stego Video, Stego Frame, Least Significant Bit, Hash Function, Index Channel

INTRODUCTION

In the present world, embedding data into a cover medium and concealing their existence is gaining more importance as safety and security of the data are major issues in communication and transmission field. Along with safety and security, another aspect that has to be taken into account is the quality of the secret data should be maintained. The word steganography comes from the Greek language where “Stegos” means covered and “Graphia” means writing. Steganography is a process of hiding secret data into a cover file such that the hidden data will not be noticeable to human naked eyes. The existence of the confidential data can be concealed effectively during transmission and it is not easy for the opponent to perceive that the information is being transmitted. This will reduce hacking possibilities as secret data transmission will not gain the attention of intruder.

Cover file and secret data can be text, image, video or audio. Video steganography is a technique where carrier file will be video in which the secret information can be hidden. When video is used as the cover file, there will be additional security [1] as structure of video file is quite complex compared to other types of media. Another important aspect in steganography is storage capacity of cover file. Larger the storage capacity of the cover file, greater the amount of data that can be hidden in it. Video files have more storage capacity than audio and image as data can be hidden in one or more frames of the cover video. If data is hidden in any of the one frame then that particular frame number can be used as stego key or password which is very essential for the receiver side to retrieve the secret data. In video steganography, it is essential to understand four different terminologies in order to keep the existence of the data unnoticeable. Figure 1 shows the block diagram and terminologies used in video steganography.

There are many kinds of steganographic techniques in which spatial domain technique [12] is the simplest one. Most commonly LSB substitution will be done where secret data will be inserted in the LSB bit positions. In this paper, a hybrid approach have been used which involves manipulation of secret data bits in the LSB bit planes of cover video.

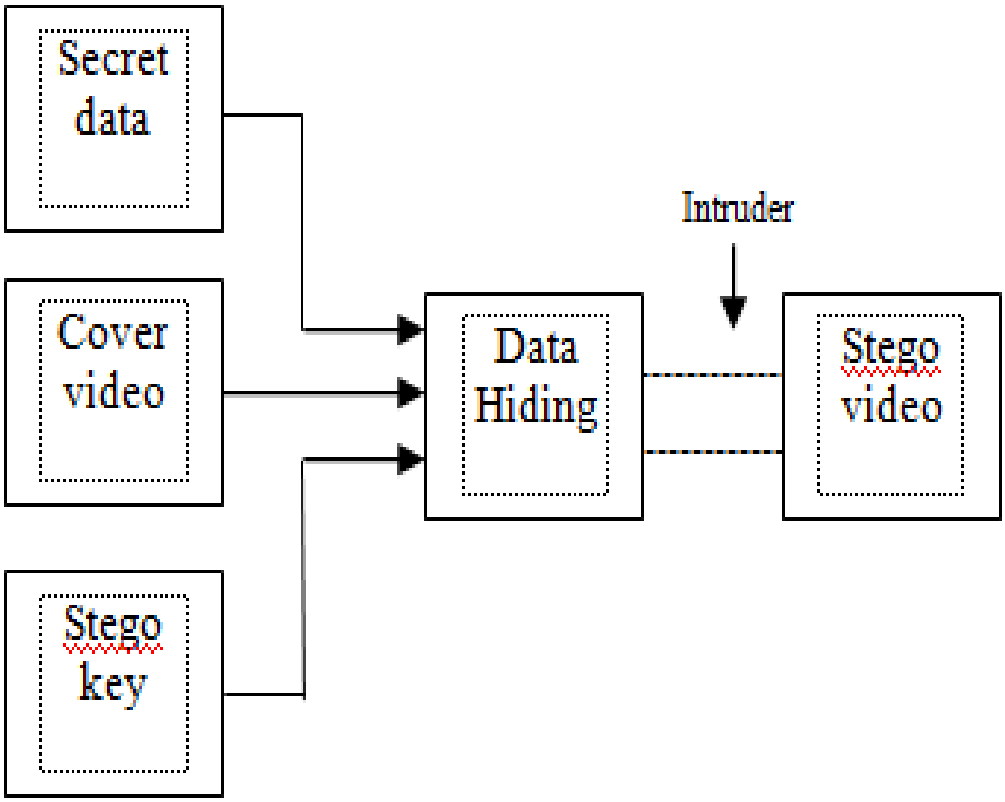

Figure 1: Video Steganography Block Diagram

The proposed approach is the combination of Hash based 3-3-2 LSB technique [8, 9] and Index channel technique [13, 14]. In the former technique, a hash function is used for determining the position to embed secret data bits in the least significant bit region of the RGB pixel. 8 bits of secret data will be inserted as 3, 3, 2 bits into red, green, blue pixel components respectively. The latter technique makes use of the index channel. An index channel is selected randomly and secret data bits is hidden in the last two LSB bit position of carrier channels based on the 3 bits (5, 6 ,7 th position) in the index channel. This hybrid approach will be implemented in MATLAB and secret data will be encrypted before embedding by which data is kept more secure while transmitting.

LITERATURE SURVEY

Video steganography is gaining the attention of researchers as there are many advantages of video steganography over other steganographic methods. Security is an important aspect in data transmission. Secure Video Data Hiding [1] embeds text message behind video file by using DCT for providing security and LZW for compression and decompression. It is highly secure steganographic system to send data using any channel over the network. Video steganography system [2] improves the protection of data by using DCT and LSB such that that the video does not lose its functionality. Reducing the extraction time while retrieving the data is also an important factor at the receiving side that must be taken into consideration. A new data embedding method in video steganography [3] is proposed for data embedding and data retrieving for high resolution AVI files. This technique effectively reduces the extraction time by placing the index in a frame of the video. Now a days major problem while communicating over th0e network is of hackers. To prevent hacking

of data, first and foremost criteria that must be strengthened is security. Video steganography using LSB based hybrid approach [4] has been proposed that deals with replacing one or two or three LSB bits of each pixel in video frame and apply Advance Encryption Standard (AES). It is not an easy job to predict that information is hidden in video as it is difficult for the intruder to analyse individual frames in a video.

In video steganography, secret data can be hidden either in still images(frames) or moving objects. In [5], a new technique for hiding messages using motion vector has been proposed. Rather than hiding messages in still images (frames), it hides secret data in horizontal and vertical pixel components of moving objects which increases quality of the video. In this video is compressed so that it can hold large quantity of data. Skin Tone based Steganography [6] in Video files exploits the *YcbCr* colour space which takes the advantage of human colour-response characteristics. This system outperforms S-Tools [10] and F5 [11] in many aspects and it considres face features as reference points to recover from any rotational distortion. A novel data hiding method in video [7] is proposed that hides data based on VQ videos and hide both video and key in color cover video using discrete wavelet transform(DWT) and genetic direct clustering based on Fuzzy C-means clustering. This proposed method provides flexibility in adjusting the data hiding capacity and bit rate which makes the method appropriate for many applications. Hash based Least Significant Bit(LSB) Technique for Video Steganography[8,9] deals with embedding secret bits into the LSB position of each pixel in the desired frame of video. The position in LSB region for inserting each secret bit is determined by computing a hash function which provides additional security for the hidden information from intruder. After decoding the secret data at the receiver side, retaining the quality of the information is a basic requirement in steganography. LSB 3-3-2 Technique in Spatial Domain using genetic algorithm [15] is proposed that embeds secret data bits into LSB region in the order of 3, 3, 2 bits to red, green and blue pixel components respectively. Secret image obtained in this method has less distortion and perceptual quality of the image is maintained.

PROPOSED HYBRID METHOD

The proposed hybrid approach is a combination of two techniques: Hash based LSB insertion and index channel technique. The flow of the proposed hybrid approach goes like this: First an image is chosen that should be kept hidden. After an image file is chosen, it must be encrypted using chaos algorithm [17] to provide more security. In the next stage a video file in the AVI format is selected for hiding the secret image. This video is nothing but cover video. Cover video will have some countable number of frames. These frames in cover video must be seperated and the frame in which we desire to hide the secret image must be selected (if needed one or more frames can be selected). Secret image is encrypted using chaos algorithm before embedding. In the next two stages, secret image is embedded into the desired frame using hash technique and index channel technique. After the image is hidden in the cover frame, frame obtained is called stego frame which is combined with other frames of cover video to generate stego video. On applying stego key at the reciever side secret image can be retrieved (extracted) from stego video. Figure 2 shows the flowchart for the proposed hybrid approach.

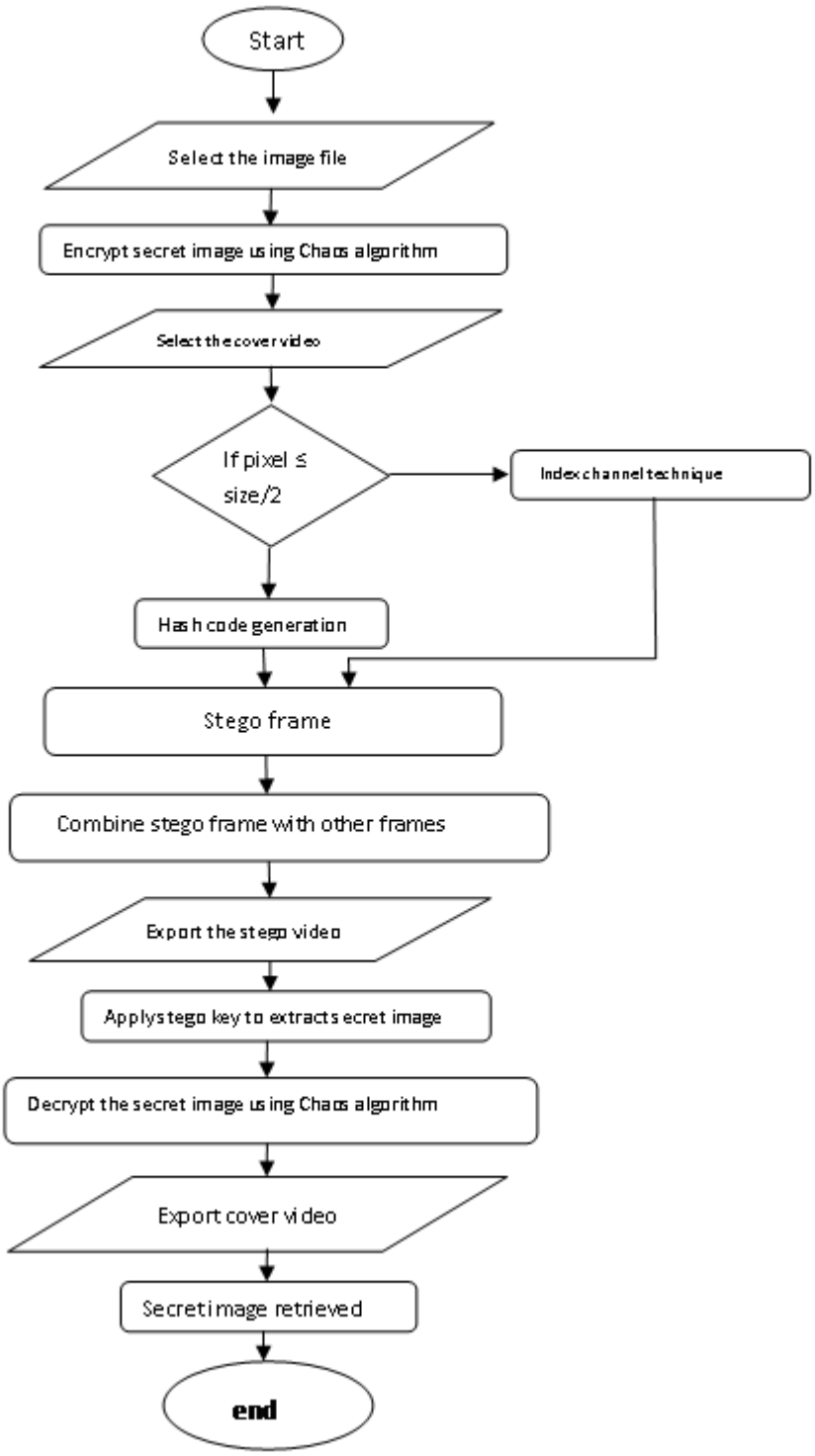

Figure 2: Flowchart of the Proposed Method

The proposed hybrid approach will have two processes one each for embedding and decoding the secret image. Before embedding the secret image, it is encrypted using chaos algorithm for security purpose. Video file in the AVI format is chosen as cover video. Frames in the cover video are separated and a frame is chosen in random in which we desire to hide the secret image. The frame number which is selected for embedding is used as password or stego key that is sent to the receiver along with the stego video. Embedding makes use of both hash based LSB technique and index channel technique.

First half of the pixels in the selected frame of cover video will be used for embedding secret image using hash based LSB insertion and remaining half of the pixels will be used for embedding using index channel method. If required more than one frame can be used. Using the stego key sent at the sender side, receiver will know about the frame in which secret image is hidden and can be decoded.

Hash Based Least Significant Bit Insertion Method

Hash based 3-3-2 LSB insertion method is implemented over the base 3-3-2 LSB technique. In 3-3-2 LSB technique, 8 bits of secret data is embedded as 3, 3, 2 bits into the red, green and blue components of each pixel in the cover frame. This base technique is extended by using hash function to provide additional security for the secret data. Because of the hash function used, intruder will not be able to predict the postion of the embedded secret bits unless he is able to compute hash code. Since insertion is done in LSB bit postion, difference between cover video and stego video will not be noticeable to human eyes. Flowchart for the hash LSB technique is given in [8]. Hash based LSB insertion method makes use of hash function [9]. Hash function gives the position in the LSB region within the pixel where it is appropriate to hide the secret bits there by making the data more secure.

Generally hash function is given by equation 1,

$$p=h\%n \quad (1)$$

Where h represents position of each hidden image pixel, n represents maximum number of bits in the LSB region (taken as 4) and p represents the position in least significant bit region within the pixel of cover frame.

For example, consider a RGB pixel from the desired frame of cover video. Each pixel from the true color image (frame) [16] will have 24 bits where they are distributed into 8, 8, 8 bits to red, green and blue components respectively. Let us choose a pixel for embedding the secret data in the desired cover frame. Let that pixel be 117. Binary representation is given by 01110101. This pixel is viewed as R, G, B components where each component is represented as

R: 01001001 G: 10001000 B: 10001110

Decimal values for the above components in the example are 73, 136, and 142. Let the secret data which is to be hidden be 36. It is represented in the binary form as 00100110.

Figure 3 shows how secret data bits is embedded into the three components of the pixel in the cover frame and arrow mark shows position of each bit in the pixel of cover frame after data embedding.

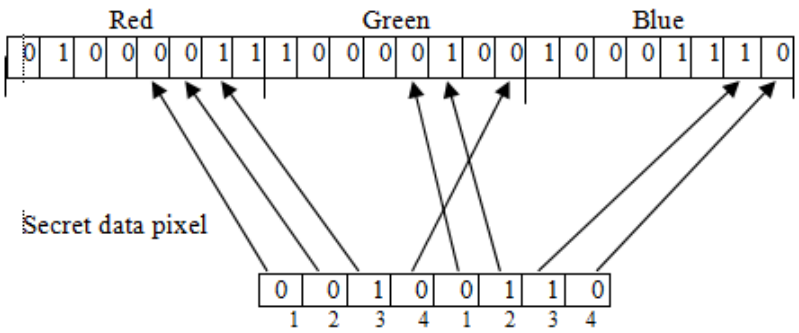

Figure 3: Example of Embedding Secret Data Bits

Process in the Figure 3 is repeated for first half of the pixels in the cover frame taking position of hidden image pixel into consideration. Hash function is applied and based on the output of the hash code 3, 3, 2 secret bits are distributed into the RGB components.

Randomized Index Channel Method

The Bits of the encrypted secret image is embedded into the remaining half of the pixels of cover frame using randomized Index channel method. In this method, one channnel will be used as indicator for embedding and other two channels are used as carrier channels. Selection of the index channel is constant instead it is ranomized here. If secret bits are available to embed then default index channel in the beginning will be red, followed by green which is followed by blue and this order repeats until secret data bits are available. On the basis of the bits in the 5^{th}, 6^{th}, 7^{th} position of index channel secret bits are embedded into the carrier channels (one or two) of cover frame. Bits in 5^{th}, 6^{th}, 7^{th} position of index channel are calculated and stored in S. The S number of bits from the secret image pixel will be embedded into each of the carrier channels. Get the bits in the last two position of LSB of index channel and depending on those bits it is decided whether to hide the S number of bits into one or two channels or not. Algorithm for embedding and extraction randomized index channel technique is given in [14]. Table 1 shows the idea of embedding the data based on the index channel.

Table 1: Secret Bits Embedding Based on Index Channel

LSB Bits of Index Channel	Channel 1	Channel 2
00	No hidden bits	No hidden bits
01	Hidden bits = *S*	No hidden bits
10	No hidden bits	Hidden bits = *S*
11	Hidden bits = *S*	Hidden bits = *S*

ANALYSIS AND RESULTS

In evaluation of a steganographic technique, it is always expected that the perceptual quality of the resulting stego file should be good. Greater the PSNR value better the quality of the stego video which makes the embedded data imperceptible. The perceptual imperceptibility of the embedded data can be obtained by comparing the cover video to its stego counterpart so that their visual differences can be determined. Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied. To measure perceptual quality of stego video, two metrics are commonly used.

The perceptual quality of stego video is can be measured using the equation 2 below

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^{H} \big(P(i,j) - S(i,j)\big)^2 \quad (2)$$

H × W represents the Height and Width.

The distortion in the stego video is measured using the equation 3 below

$$\text{PSNR} = 10 \log_{10}\left[\frac{L^2}{MSE}\right] \quad (3)$$

Here MSE is mean square error, PSNR is Peak Signal to Noise Ratio and P (i, j) and S (i, j) are pixel in original frame and stego frame respectively and L is peak signal level (255).

The proposed method is tested using three secret images and one cover video (Rhinos.avi). The experimental results are shown in Table 2.

Table 2: Comparison between HLSB, Index Channel and Proposed Method

Secret Images	HLSB		Index Channel		Hybrid Method	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena.jpg	8.0205	39.1228	7.8298	39.2273	20.7256	34.9997
Pic.jpg	5.4278	40.8185	7.0566	39.6788	19.6650	35.2279
Animal.jpg	9.7960	38.2543	7.7113	39.2935	20.8176	34.9805

The output samples for the secret images in the table 2 is as shown below

Lena.jpg




Figure 3: Secret Image **Figure 4: Cover video** **Figure 5: Stego Video** **Figure 6: Recovered Image**

Pic.jpg




Figure 7: Secret Image **Figure 8: Cover Video** **Figure 9: Stego Video** **Figure 8: Recovered Image**

Animal.jpg




Figure 9: Secret Image **Figure 10: Cover Video** **Figure 11: Stego Video** **Figure 12: Recovered Image**

CONCLUSIONS

An efficient hybrid approach for concealing the existence of an image has been presented in this paper. Experimental results of the proposed technique are compared with base techniques (HLSB and index channel) and we infer that even though the results are comparatively less in terms of MSE and PSNR as in Table 2. Quality of the retrieved image and stego video is good in the proposed method. As in hybrid approach more than one embedding techniques are used to

hide the secret image there will be confusion for the attackers. So this method is robust against attacks. The proposed approach is strengthened in security aspect which is the major requirement in communication stream. The proposed approach is a combination of two techniques that can be used to effectively hide a secret image in a cover video. Only AVI files can be used as cover video. However, other video formats can be used with some modification. This work hides an image in a video, the same work can be extended for hiding video in a video.

ACKNOWLEDGEMENTS

Authors would like to thank the principal and staff of JNNCE for their support in this work.

REFERENCES

1. Kumbhar Shraddha, Rokade Varsha, Sukre Mayuri, "Secure Video Data Hiding Using DCT and LZW", International Journal of Computer Science Trends and Technology (IJCST) , Vol. 3, Issue 1, pp. 24-26, Jan-Feb 2015.
2. Poonam V Bodhak, Baisa L Gunjal, " Improved Protection In Video Steganography Using DCT & LSB", International Journal of Engineering and Innovative Technology (IJEIT) Vol. 1, Issue 4, pp. 31-37, April 2012.
3. Pritish Bhautmag, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 1, pp. 1641-1644, January - February 2013.
4. Hemant Gupta, Dr. Setu Chaturvedi, " Video Steganography through LSB Based Hybrid Approach", International Journal of Engineering Research and Development Vol. 6, Issue 12, pp. 32-42, May 2013.
5. P.Paulpandi1, Dr.T.Meyyappan, "Hiding Messages Using Motion Vector Technique In Video Steganography", International Journal of Engineering Trends and technology,Vol. 3, Issue3, pp. 361-365, 2012 .
6. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Skin Tone Based Steganography In Video Files Exploiting The Ycbcr Colour Space", *School of Computing and Intelligent Systems, Faculty of Computing &* Engineering University of Ulster, Londonderry, BT48 7JL, Northern Ireland, United Kingdom 2008.
7. Roshani Patidar, Kamlesh Patidar, "Steganography Method Hiding Data in Video", *International Journal of* Computer Science and Information Technologies (IJCSIT), Vol. 6 , pp. 237-239, 2015.
8. Prof. Dr. P. R. Deshmukh , Bhagyashri Rahangdale, " Hash Based Least Significant Bit Technique For Video Steganography ", International Journal of Engineering Research and Applications, Vol. 4, Issue 1(Version 3), pp. 44-49, January 2014.
9. Kousik Dasgupta, J.K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit TechniqueFor Video Steganography(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, pp. 1-11, April 2012.
10. Westfield A and Pfitzmann, "Attacks on Steganographic Systems Breaking the Steganography Utilities EzStego, Jsteg, Steganos and S-Tools and Some Lessons Learned", Proc of 3rd International Workshop on Information Hiding, IH'99. LNCS 1768. pp. 61- 76, 1999.

11. Westfeld, "F5-steganographic algorithm: High capacity despite better Steganalysis", *LNCS 2137, pp. 289-302, 2001*.
12. Rakhi, Suresh Gawande, "A Review On Steganography Methods", International Journal of Advanced Research in Electrical, Electronics And Instrumentation Engineering, Vol. 2, Issue 10, pp. 4635-4638, October 2013.
13. Emad T. Khalaf, Norrozila Sulaiman, "Segmenting and Hiding Data Randomly Based on Index cahannel", *IJCSI* International Journal of Computer Science Issues, Vol. 8, Issue 3, May 2011.
14. Ajit Danti, G. R. Manjula, R. B. Sushma,"Steganography using Randomized Index Channel with Arnold Cat Map Encryption", Proceedings in the second international conference on Emerging research in computing, information, communications and applications, Elsevier Publications 2014.
15. Kousik Dasguptaa, Jyotsna Kumar Mondal, Paramartha Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", international Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013.
16. Iman Thannoon Sedeeq, "Steganography in Colored Images", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 11, No. 4, pp. 87-92, April 2013.
17. Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 3, No 1, pp. 11-22, February 2014