International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 502-506
Published Online July 2019 in IJEAST (http://www.ijeast.com)

INFORMATION SECURITY WITH SCAN PATTERNS AND CHAOTIC CRYPTOGRAPHY

Sankhya Nagesh Nayak
Department of CS&E
J.N.N.C.E, Shivamogga,
Karnataka, India

Nandish M
Department of CS&E
J.N.N.C.E, Shivamogga,
Karnataka, India

Chakrapani D S
Department of CS&E
J.N.N.C.E, Shivamogga,
Karnataka, India

Mohan H G
Department of CS&E
J.N.N.C.E, Shivamogga,
Karnataka, India

***Abstract*— A hybrid approach of data encryption and steganography is used in our work. Motivation behind this approach is to provide a simple and smart image steganographic technique which must be capable enough to provide good quality stego-image. Image steganography is a technique in which pixel intensities are used to hide the data. In this approach, the secret information is initially encrypted and then encrypted bits are embedded into an image. Logistic chaotic maps are used for Image Encryption, and LSB technique is used for embedding. To increase unpredictability, we employ different combinations of scan patterns for encryption and embedding. This approach is more secure against attack and its stego-image is indistinguishable from the original image by the human eye.**

Keywords— **Steganography, Logistic chaotic maps, Scan patterns**

I. INTRODUCTION

The main purpose of steganography is to provide imperceptibility to the secret, hidden in carrier file. Mahajan Palak et al. (2014), in their work used LSB inserting mechanism for steganography, substitution cipher for cryptography, JPEG-LS for Compression, image for hidden data. The proposed method uses compression, encryption and LSB embedding in order to hide and recover data. Applying compression in the first layer helped in reducing the size of secret data thereby providing high payload capacity. Encryption at inner layer results out to be an asset that increased the security of data against Steganalysis. S.N Rekha et al. (2016) in their work encrypted the secret data by using Hybrid encryption method i.e. AES [Advance Encryption Standard] and ECC [Elliptic Curve Cryptography] method to safe guard the secret communication. Then, Lempel Ziv Welch technique compresses the required amount of data to represent information quantity. Then Edge detection technique detects the sharp feature of image to hide secret data. Rani Pooja et al. (2015), in their work used pattern matching for steganography, blowfish encryption for cryptography, DWT compression for compression, image as hidden data. Sharma Lavisha et al. (2016), in their work have used Huffman coding technique to implement steganography. Encryption is implemented by using ECC (Elliptic Curve Cryptography) algorithm. To reduce the storage space used to store digital images, DWT (Discrete Wavelet Transform) technique is used along with EZW compression method. Jain Akshay et al. (2013), in their work used LSB for steganography, AES for cryptography, Vector quantization for compression, image/text as hidden data. To make the transmission and storage of digital data faster, lossy compression is used. On the compressed image, data hiding is done. The stego image is encrypted using AES to ensure user authentication. Nodes are selected randomly in data hiding stage. On the randomly selected nodes lossless LSB steganography is used. Xinyi Zhou et al. (2016), in their work used LSB for steganography, RSA for cryptography, image as hidden data. They have used an improved LSB information hiding algorithm of color image using secret key, combining information hiding and cryptography, increasing the human eye visual features, and the identity authentication based on digital signature and encryption technology to improve the security of information hiding. M Nandish et al. (2015) developed a new image encryption scheme based on SCAN, Dyadic permutation and Carrier image to encrypt and decrypt the image. Dyadic algorithm adds security by scrambling the image using key and placement of key in correlated image. SCAN algorithm adds security by scrambling the image using scanning pattern as key. Since carrier image is generated using pseudo random numbers based on DNA sequence, it is not possible to predict the numbers without knowing the seed. M.J Thenmozhi et al. (2016)], in their work compress the secret message image by SPIHT and convert in to a binary sequence, divide the binary sequence into a block, change the order of block using a key-based randomly generated permutation, concatenate the permuted blocks can be changed into a permuted binary sequence, and then utilize the Least-Significant-Bit (LSB) approach to embed the permuted binary sequence into image. After the completion of the pixel value changing all the images is placed in a sequential manner. Somaraj Shrija et al. (2017) in their work introduced new algorithm for image encryption using the scan method. Using SCAN language, it is possible to generate a wide range of scanning paths based on the spatial accessing methodology. They claim that with the increase in complexity of scan patterns, the encrypted image appears more distorted as compared with the single-level encryption. It has high processing speed. They use simple XOR operation and integer arithmetic for encryption. H T Panduranga et al. (2010)

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 502-506
Published Online July 2019 in IJEAST (http://www.ijeast.com)

proposed a hybrid technique for image encryption which employs the concept of carrier image and SCAN patterns generated by SCAN methodology. The carrier image is created with the help of alphanumeric keyword. Each alphanumeric key will be having a unique 8 bit value generated by 4 out of 8-code. The newly generated carrier image is added with original image to obtain encrypted image.

The rest of the paper is organized as follows. Proposed embedding and extraction algorithms are explained in section II. Experimental results are presented in section III. Concluding remarks are given in section IV.

II. PROPOSED ALGORITHM

The system include, pre-processing of the secret information (i.e. encryption), detection of pixels in cover image where the secret information can be stored and inserting the secret information in selected pixels to form a stego-image. At receiver end, the information is retrieved from stego-image and decrypted to get the secret information. Different scan patterns are used for both encryption and embedding to increase confusion and diffusion.

At Sender's end:

The proposed method allows user to

1. Choose the secret image.
2. Choose a suitable image as cover image from repository of images based on the size of secret.
3. Choose scan patterns for encryption and embedding.
4. Read the pixels according to chosen scan pattern and encrypt them using chaotic method.
5. Read pixels according to a different scan pattern than encryption and hide the secret using LSB method.
6. The stego-image is sent to receiver end.

At receiver's end:

The process of recovering data from stego image follows reverse procedure in comparison with sender side. Stego image is given as input to the decoding technique.

1. Extract information from the stego-image regarding scan patterns used for encryption and encoding and size of the secret image
2. Read the pixels according to chosen scan pattern and extract secret image in encrypted format from the cover image.
3. Read pixels according to a different scan pattern than recovery method and decrypt to recover secret image.

The proposed scheme uses the dual functioned process to encrypt the sequence of pixels of original image. Scan pattern is used to create the confusion in reading the pixels and the chaotic function is used to change intensity values of pixels. These functions together ensure confusion and diffusion operations required for encryption.

A. Chaotic Cryptography

Chaotic maps are simple unstable dynamical systems. They are highly sensitivity to initial conditions. Small deviations in the initial conditions lead to increased deviations making the long-term forecast for the chaotic systems intractable.

The proposed scheme uses the dual functioned process to encrypt the sequence of pixels of original image. Scan pattern is used to create the confusion in reading the pixels and the chaotic function is used to change intensity values of pixels. These functions together ensure confusion and diffusion operations required for encryption.

The chaotic function used is known as logistic map and it is given as:

$$Xn=Xn\text{-}1 * \lambda *(1- Xn\text{-}1)$$

where Xo is the initial seed. The chaotic behavior of the function depends on the value of λ. In both encryption and decryption side same scan pattern and same values for initial seed and λ is used . We used the values for these from work done by M Nandish et al.(2018).

Encryption:

Step 1: Read the input Buffered Image.
Step 2: Array of values is created using the logistic map matching the size of secret image.
Step 3: Modify each pixel from the image by XORing it with the corresponding seed value in the logistic map array.

$$Pi=Pi \text{ XOR } Xi$$

Step 4: Write the encrypted image.

Decryption:

Step 1: Read the Encrypted Image.
Step 2: Array of values is created using the logistic map matching the size of secret image.
Step 3: Modify each pixel from the image by XORing it with the corresponding seed value in the array.

$$Pi=Pi \text{ XOR } Xi$$

Step 4: Write the decrypted image.

B. LSB steganography

Steps in using LSB steganography:

At Sender's end,

a. Read the secret data which is needed to be hidden.
b. Read the cover image in which the secret data should be hidden.
c. Secret data is converted into array of pixels in case of image.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 502-506
Published Online July 2019 in IJEAST (http://www.ijeast.com)

d. Replace the least significant bit of pixel in the cover image with array content for image and directly in case of text.
e. Write the resultant stego-image.

At Receiver's end,

a. Read the stego-image.
b. Extract the least significant bit of pixel in the cover image and store in an array.
c. Reconstruct secret data.

C. Scan Patterns

Maniccam et al. (1999) presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language based two dimensional spatial accessing methodologies which can efficiently specify and generate a wide range of scanning paths or space filling curves. The wide range of sequential accessing patterns that are produced by the SCAN grammar, allows the consideration of a SCAN word as an encryption key bound to a given 2D image array. The application of this word on the initial array data produces the rearrangement to them into an encrypted final sequential representation, which is dictated by the accessing pattern that it represents.

"SCAN" refers to the different ways of scanning a 2D image. One can generate (n x n)! paths for an image of size n x n based on a 2-D spatial accessing method. A set of scanning paths are used for encrypting as well as embedding. Since the arrangement of the bits are secret, the level of security achieved is high. It is highly impossible to find scan path using currently available computational technologies. The SCAN model defines an extended set of hierarchical decompositions of an image into subregions.

This is the cryptographic scheme for 2D encryption, and especially for picture data encryption, but we have used it for encryption as well as encoding. In general Z-pattern and B-pattern SCAN patterns are popular. We have used Scan pattern combinations for embedding and encoding and are shown in Fig.1 – Fig.4. Fig. 1(a) uses Continued Raster Scan pattern. Rest of the scan patterns are generated by us. Though we have showed some combinations, various combinations can be used to increase unpredictability.

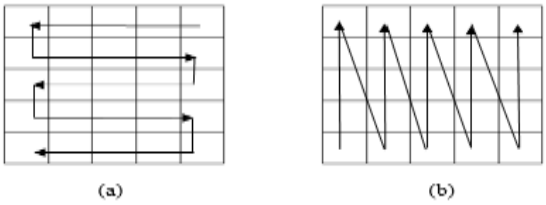

Fig. 1. Scan pattern 1 (a) encryption (b) encoding

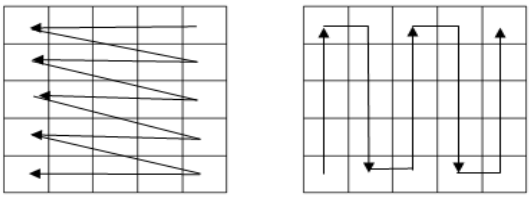

Fig. 2. Scan pattern 2 (a) encryption (b) encoding

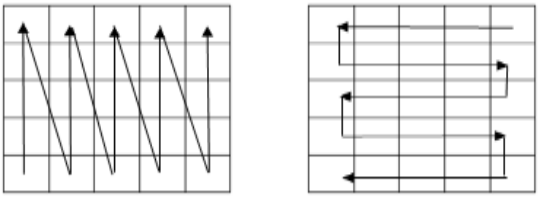

Fig. 3. Scan pattern 3 (a) encryption (b) encoding

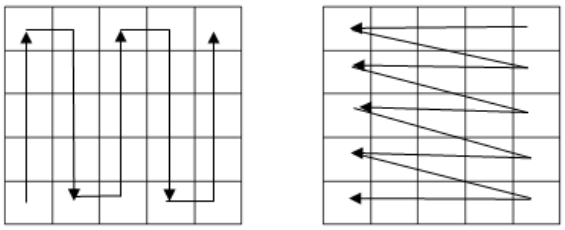

Fig. 4. Scan pattern 4 (a) encryption (b) encoding

The combinations used for encryption and encoding are decided earlier by both party involved in communication and is stored as look up table.

III. Experiment and Result

The test set for this evaluation of experiment is randomly selected from the internet. The method is implemented in Java. Scan pattern combination is selected by the user. Around 100 images are kept in the repository for secret and cover images and are used for analyzing the procedure. Two images and histogram is used to depict the method and is shown in Fig 5 and Fig 6. There are no visible changes observed in stego image that can disclose the information is hidden in it.

International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 502-506
Published Online July 2019 in IJEAST (http://www.ijeast.com)

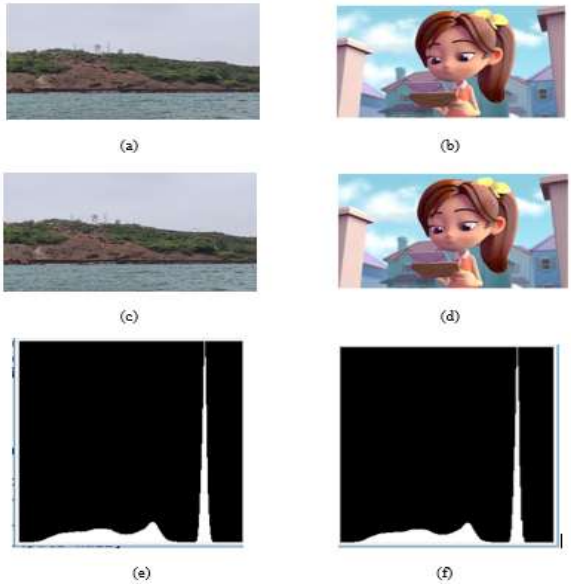

Fig. 5. (a)Cover image (b) Secret image (c) Stego-image (d) Extracted image (e) Histogram of cover images (f) Histogram of stego-images

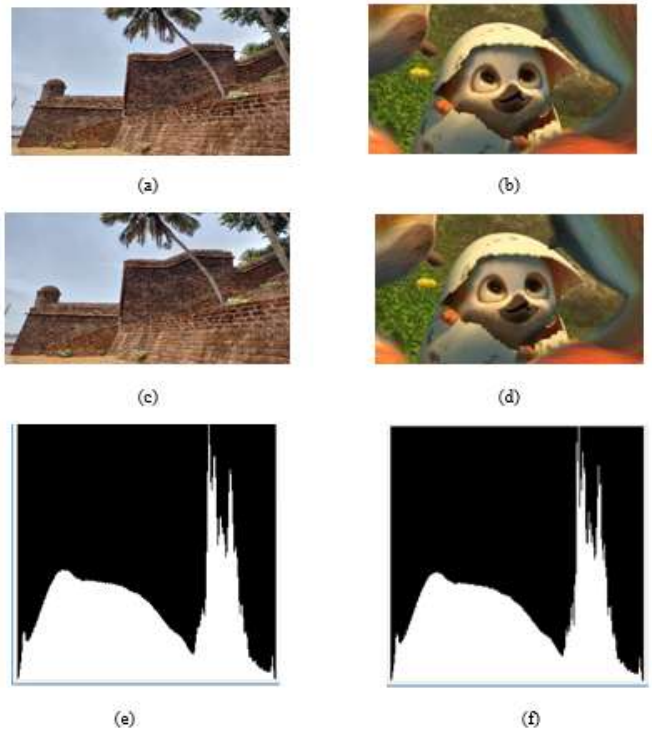

Fig. 6. (a)Cover image (b) Secret image (c) Stego-image (d) Extracted image (e) Histogram of cover images (f) Histogram of stego-images

Different size of cover image and secret image is chosen and MSE and PSNR values are calculated for them. The comparison for one cover image and secret image in various sizes is given in Table 1. As the size of secret image is increased for constant cover image, we observed that the values of MSE and PSNR are 0 and infinity respectively. From and above the size 648 x 1152 secret image embedding was found inefficient.

Table 1: List of cover image, secret image, MSE, PSNR

Cover image in MxN	Secret image in MxN	MSE	PSNR
4970 x 4000	87 x68	0	infinity
4970 x 4000	150 x 180	0	infinity
4970 x 4000	188 x 268	0	infinity
4970 x 4000	640 x 619	0	infinity
4970 x 4000	537 x 837	0	infinity

The information entropy of some outcomes are shown in Table 2.

Table 2: Information entropy

Matrix of Secret image in MxN	Encrypted image
373 x 208	7.63
350 x 466	7.63
388 x 228	7.63
640 x 619	7.63

The entropy we obtained after encrypting the image is 7.63. The ideal entropy of an image is 8 and the obtained entropy is close to the ideal value.

Correlation between cover and stego image is shown in Table 3. By observing the table, we can infer that there is negligible change in the cover and stego image.

Table 3. Correlation between cover and stego image

Matrix of cover image in MxN	Difference in percentage
3648 x 2736	0.01855
4608 x 3456	0.01162
4608 x 3456	0.01161
3840 x 2160	0.02234

IV. CONCLUSION

The proposed LSB method-based steganography is an effective way to hide sensitive information secretly. This method is efficient and offers good imperceptibility. The robustness of secret information embedded in the cover medium shows that the method is very effective. The image persistence does not change much and is negligible when embedding the secret information into the image. The secret information is chaotic encrypted to increase the security.

To further increase the security, we have used four different scan patterns in both encryption and embedding process so that the encrypted image is more distorted than the original one and it is more difficult for intruder to get back the secret image. By observing the correlation information, embedded image has negligible difference compared to cover image and hence, we can say that it is more difficult to detect the actual information.

V. REFERENCES

[1]. Mahajan Palak, Koul Ajay (2014), "CEET: A Compressed Encrypted & Embedded Technique for Digital Image Steganography ", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, e-ISSN: 2278-0661, p- ISSN: 2278-8727, (pp. 44-52).

[2]. S. N. Rekha, Y. Manjula, M.Z. Kurian(2016) , "A secured lsb image steganography system using edge detection, lzw compression and hybrid encryption methods", International Journal of Advanced technology in Engineering and Science, Vol.No.4, ISSN 2348-7550, (pp. 197-208).

[3]. P. Rani, Arora Apoorva (2015), "Image Security System using Encryption and Steganography", International Journal of Innovative Research in Science, Engineering and Technology, Volume 4, ISSN: 2319-8753, (pp. 3060-3869).

[4]. Sharma Lavisha, Gupta Anuj (2016), "Image Encryption Using Huffman Coding for Steganography, Elliptic Curve Cryptography and DWT for Compression", International Journal of Advanced research, Idea and innovation in technology, Volume 2, ISSN: 2454-132X, (pp.1-10).

[5]. Jain Akshay, Pawar Dipak (2013), "Encrypted Reversible Data Hiding on Compressed Image", International Journal of Computer Applications, Volume 69– No.25, ISSN: 0975 – 8887, (pp. 1-5).

[6]. Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin(2016) , " An Improved Method for LSB Based Color Image steganography Combined with Cryptography ",(pp. 1-4).

[7]. M Nandish, Rudra Kailash (2015), "Combination of DNA Sequence in Scan Patterns and Dyadic Permutation in Securing the Image Contents", European Journal of Advances in Engineering and Technology, Vol. 2, Issue 4, ISSN: 2394 - 658X (pp 23-30).

[8]. Thenmozhi M.J., T. Menakadevi (2016), "A New Secure Image Steganography Using Lsb and Spiht Based Compression Method", International Journal of Engineering Research & Science, vol 2, ISSN: 2395-6992, (pp. 80-85).

[9]. Somaraj Shrija, Hussain Mohammad Ali (2017),"An Image Encryption Technique Using Scan Based Approach and Image as Key", (eds.), Proceedings of the First International Conference on Computational Intelligence and Informatics, Advances in Intelligent Systems and Computing, (pp. 645-653).

[10]. HT Panduranga, SK Naveen Kumar (2010), "Hybrid Approach for Image Encryption Using SCAN Patterns and Carrier Images ", International Journal on Computer Science and Engineering, (pp. 297-300).

[11]. M Nandish, Kumar Jalesh, H G Mohan(2018) ,"An Image Encryption Process Based on Multiple Chaotic Maps", Journal of Research in Image and Signal Processing, Volume 3 Issue 2, (pp.1-12).

[12]. SS Maniccam and NG Bourbakis (1999), Scan Based Lossless Image Compression and Encryption, Proceedings of International Conference on Information Intelligence and Systems, (pp. 490-499).