A Novel Method of Data Encryption and Hiding Scheme using VPASS Technique

Anand L S[1], Prajwal S Sanket[2], Sharath R V[3], Varun R[4]

[1, 2, 3, 4] Department of Telecommunication Engineering, Dayananda Sagar College of Engineering
Bangalore, India

Abstract: ***Cryptography is an art of making the data unintelligible to third party other than the sender and receiver. The security for data can be implemented using public and private cryptography. The data is made secure using many data encryption techniques. We have proposed an advanced technique of encryption involving unique VPASS Algorithm. Original work related this includes the playfair technique and since then modification to this have been proposed. Our scheme involves the use of unique VPASS matrix to encrypt the messages. Security of the message can be enhanced by using a steganography technique. Steganography is the art of concealing the existence of information within seemingly harmless carriers. In this paper we have proposed a revised information hiding scheme using VPASS technique. Original work related to our scheme includes the Chang et al method of information hiding. The Chang et al method can be implemented for greyscale images but our method can be implemented for colour images.***

Keywords: Steganography, embedding, VPASS, reference matrix

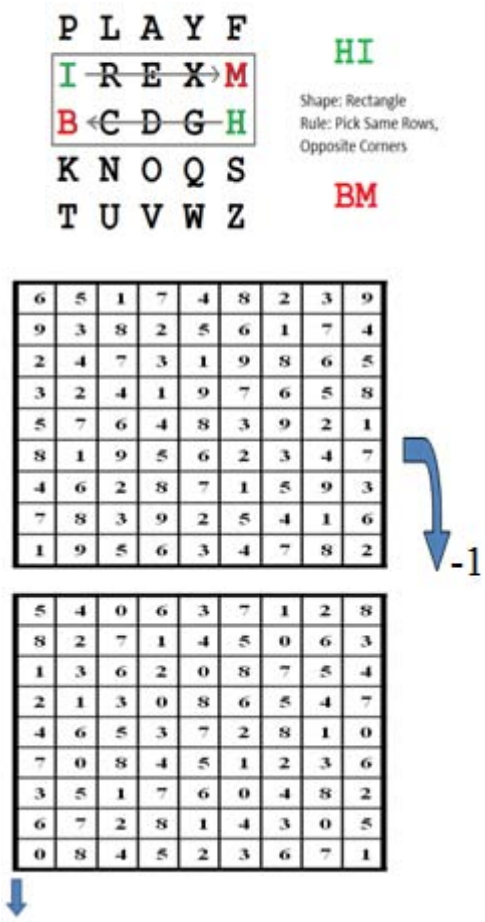
1. Introduction

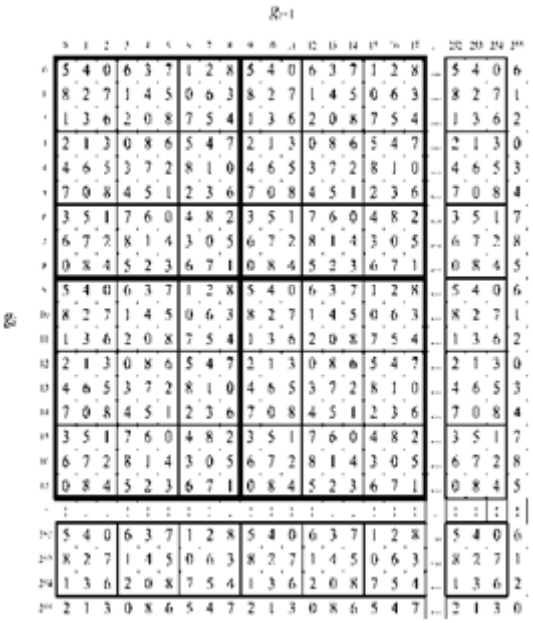
The technique of cryptography dates back to 3000 years. Various techniques have been evolved since then. The technique of cryptography can be divided into two categories-public and private. The conventional key system uses a single key for encryption and public key system 2 keys for encryption. Primary concern for an encryption technique is strength of the security algorithm and the time taken to decipher the message. The strength of encryption can be enhanced using the method of steganography. The image hiding scheme can be modified into three categories namely spatial domain, compressed domain and transformed domain. However information hiding using spatial domain is vulnerable to statistical Stegano analysis. An important factor one needs to consider when one designs a new embedding scheme is the embedding capacity and visual quality of the image. These two factors are inversely proportional hence tradeoffs must be made according to the application. Section 2 of this paper describes the literature survey and related work, section 3 with the proposed method of data encryption and hiding scheme followed by conclusion and other recommendations for the project. The main aim of this project is to propose a novel technique of encryption and data hiding using VPASS technique for colour images.

2. Related Work

In this section we will briefly describe the conventional playfair technique used. The conventional play fair matrix consists of 5*5 matrix with alphabets used for the encryption. The message to be encoded is encrypted using the playfair matrix. The playfair matrix is shown in the figure 1.

The previous method related to VPASS technique can be referenced to Chang et al scheme of Steganography. The central idea of Chang et al.'s method is to modify the selected pixel pairs in the cover image based on a specially designed reference matrix M to insert secret digits. For an 8-bit grayscale cover image, the size of the reference matrix M is designed to be 256× 256. To construct a reference matrix M, a "tile" matrix T is constructed first by subtracting every digit in a Sudoku puzzle by one, so that the digits in matrix T ranged from 0 to 8, as shown in Figures 2. The reference matrix M is then consisting of an m×m tiling of copies of T, where m=|_256/9_| + 1.The reference matrix is replicated to a size of 256*256. The example of which is shown below.





Reference matrix M

3. Proposed method

3.1 Data encryption

Data encryption is done by taking the input data string and converting the characters into their corresponding ASCII values. We construct a unique matrix that consists of entire ASCII values. This matrix is a 16x16 matrix that consists of ASCII values in a unique manner. Then each character's ASCII value is searched from the matrix and the co-ordinate values are stored. Next the user is asked for an encryption key. The key is kept within the limits of the matrix size using mathematical functions. The ASCII value got after searching the matrix is circularly right shifted the number of times the key value. If the column value exceeds the limits of the matrix, it is shifted again from the starting column of the matrix. The new ASCII values obtained from the above procedure form an array of cipher text.

Cover image	*Size of image*	*Proposed method*	*Embedding capacity*
		PSNR	
LENA	256*256	39.78	8bpp
Baboon	256*256	37.97	8bpp
Tree	266*400	32.15	8bpp

3.2 Data Decryption

The original plain text is got back by circularly left shifting the cipher text value from the same matrix. After the left shift procedure, the value in the current co-ordinate position is the ASCII value of the original plain text character.

3.3 Data Embedding

Steganography using VPASS technique involves the use of cover image with along with the reference matrix. The reference matrix is of size 256*256 to accommodate 0 to 255 pixel values. The cover image can be of any size. The embedding capacity depends on the size of the image. The secret message to be embedded is taken from the encryption. The ASCII values are divided into 3 parts-0-3LSB bits, 3-6LSB bits and last 2LSB bits. The first 3 LSB bits are taken for embedding. For data embedding two entities are defined namely horizontal box and vertical box. A pixel from the cover image is chosen and plotted on to the reference matrix. This point is central point for horizontal box and the vertical box.

The horizontal box contains 8 elements numbered 0-8. The vertical box also contains 8 elements numbered from 0-8. The first 3LSB bits are compared to elements in the horizontal box and the distance between them is calculated using Manhattan distance formula. Similarly distance between 3lsb bits and element in the vertical box is compared and distance between them is calculated using Manhattan distance formula. The minimum distance between them is taken and the position of the compared number is noted. This new position is plotted on the cover image and the pixel at this position is taken for embedding the data. The RGB values at this pixel are used to embed the secret data. Red pixel is used to embed last 3bits of secret message, middle 3bits of message is embedded in the green pixel and last 2 bits are embedded in the blue pixel.

3.4 Data extraction

The position at which the secret message is embedded is noted. Using simple AND- XOR operation the bits can be extracted.

4. Results

Data encryption

enter the data="An Innovative Method of Data Encryption and Hiding Scheme
Using VPASS Technique"
enter the key=500
>> char(cipher_text)
Ans=
MjEjjkzemziIilkhkbPeeAjovudmkjejhDmhmjc
_oliaiYwmjcRLM__Xioljm}qi

Steganography

Figure 1: Original image

Figure 2: Stego image

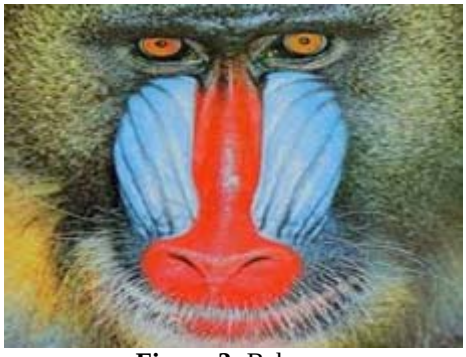


Figure 3: Baboon

Figure 4: Lena

Data Decrypted

Original data is= "An Innovative Method of Data Encryption and Hiding Scheme Using VPASS Technique".

5. Conclusion

Steganography over cryptography provides better security than cryptography taken alone. Cryptography makes the message unintelligible and Steganography provides enhancement for this security. In this paper we have introduced a novel technique of encryption using the analogy of play fair cipher. The cipher text from the encryption stage is embedded into the cover image. The unique reference matrix makes the VPASS technique secure. The number of possible solutions would be 6.71x10^21. The quality of steganography technique depends on embedding capacity and good visual capacity. Our technique provides good embedding capacity according to the image size. If the image size is big the embedding capacity will be more. This technique can be applied to various fields such as satellite communication, military communication etc.

6. Acknowledgement

We would like to acknowledge Mrs.Smitha Sasi, Assistant professor, Telecommunication Engineering, Dayananda Sagar College of engineering for her constant support without which this project would be unsuccessful.

References

[1] New Data Hiding Algorithm in MATLAB using Encrypted secret message Agniswar Dutta, Sankar Das, Asoke Nath, Abhirup Kumar Sen, Shalabh Agarwal. 2011 International Conference on Communication Systems and Network Technologies

[2] Steganography using Sudoku Puzzle Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade 2009 International Conference on Advances in Recent Technologies in Communication and Computing 978-0-7695-3845-7/09 $25.00 © 2009 IEEE

[3] 978-0-7695-3845-7/09 $25.00 © 2009 IEEE, ©gopalax -International Journal of Technology And Engineering System(IJTES): B. Premamayudu, Dr. Koduganti Venkata Rao, M. Krishna Teja, M. Haneesh Krishna, K. Mukesh

[4] C.-C. Chang, T. D. Kieu, and Y.-C. Chou. High capacity data hiding for grayscale images. In Proceedings of the First International Conference on Ubiquitous Information Management and Communication, pages 139–148. Seoul, Korea, February 2007.

[5] C.-C. Chang and C.-Y. Lin. Reversible steganography for vq compressed images using side matching and relocation. IEEE

[6] Transactions on Information Forensics and Security, 1(4):493–501, December 2006.

[7] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating

[8] Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21.

[9] Cryptography and Network Security by William Stallings , Fourth Edition

Authors Profile

Anand L S is pursuing B.E. degree in Telecommunication Engineering from Dayananda Sagar College of Engineering under Visvesvaraya Technological University.

Prajwal S Sanket is pursuing B.E. degree in Telecommunication Engineering from Dayananda Sagar College of Engineering under Visvesvaraya Technological University.

Sharath R V is pursuing B.E. degree in Telecommunication Engineering from Dayananda Sagar College of Engineering under Visvesvaraya Technological University.

Varun R is pursuing B.E. degree in Telecommunication Engineering from Dayananda Sagar College of Engineering under Visvesvaraya Technological University.