iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4063

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Modified Hill Cipher Based Image Encryption Technique

Goutham L[1], Mahendra M S[2], Manasa A P[3], Mr. Prajwalasimha S N[4]
[1,2,3]Student, [4]Assistant Professor, Department of Electronics & Communication Engineering
ATME College of Engineering, Mysuru, Karnataka, India

Abstract: ***In the present advancing technology, data transmission of different multimedia like sensitive images, video, text is very important and security plays a dominant role in the fields of medical, commercial and military fields. During the transmission security of the information is required otherwise it can be accessed or hacked by the unauthorized person. Today as the ability of the network rapidly increasing, most of the data is transmitted in the form of images. Many methods like Cryptography and Steganography are developed to encrypt this kind of images which contained the data. In this paper a modified Hill cipher encryption technique has been proposed which uses an involutory key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background.***
Keywords: Multimedia, Security, Cryptography, Steganography and Hill cipher

I. INTRODUCTION

Nowadays, as the technology is advancing in the field of networking, it becomes very important to provide security for the data and tramission. Many application of multimedia technology and the increase in the ability of network leads us to obtain information directly through an image. Therefore protection of these images which contains data from the unauthorized access is important.

The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. For encrypting the plaintext, inverse of the key matrix is used which does not always exist. Then if this key matrix is not invertible, decryption is not possible. In the involutory matrix generation method the key matrix used for the encryption is itself invertible. So, at the time of decryption we need not to find the inverse of the key matrix. The objective of this paper is to encrypt an image using a technique different from the conventional Hill Cipher A comparative study of the proposed encryption scheme and the existing scheme is made. The output encrypted images reveal that the proposed technique is quite reliable and robust.

Encryption is one of the effective method of protecting and securing all he data such as images, videos and other kinds of transferable data. In encryption the data which is need to be secured is converted into another form, so that it remain unrecognized and prevents unauthorized access.

There are many methods of image encryption. Images can be encrypted using symmetric and asymmetric algorithm methods. In symmetric method of encryption, a single key is used to encrypt and decrypt. The most widely used algorithm used in symmetric key is AES (Advanced Encryption Standard).

In asymmetric method two interdependent keys, one to encrypt the data, and the other to decrypt it and in the conventional encryption method alphabets are grouped and are assigned numerical equivalent value 0 to 26. Each group is multiplied with equivalent hill matrix with mod26. The resultant matrix is ones again converted into the alphabets. It is quite difficult to calculate inverse of the modulus matrix. In our approach the text is converted into image which is divided into smaller size matrix(2x2). The each 2x2 matrix is multiplied with hill matrix without modulus function. Since there is no modulus operation, it is very easy to calculate the inverse during decryption.

In present AEC Cipher technique, in each round there are 4 steps such as substitute bytes, shift rows, mix columns, add round key. In our proposal it is just multiplication of matrix. The current key size is 256Kbytes but in our system the key size is around 64Kbytes. We use the 2x2 matrix so that inversion of the matrix is easily calculated.

II. LITERATURE REVIEW

Cryptography is the art of science encompassing the principles and methods of transforming an intelligible message in to one that is unintelligible and then transforming that message back to its original form. In modern times cryptography is considered to be a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering.

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

In this paper we have proposed an advanced Hill cipher algorithm which uses an involutory key matrix for encryption. The objective of this is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption where we may not be able to decrypt the encrypted message. So we use involutory key matrix for encryption using this matrix we encrypt gray scale or colour image.

Kamali S H presented a modification to the advanced encryption standard (AES) in order to increase the level of security and image encryption .The result shown by them was higher than that of original AES encryption algorithm [1]. Mohammed ali introduced a new permutation and a well known algorithm called Rijndael. The original image was divided into 4X4 pixels blocks.Then they were rearranged using permutation process to form a permuted image and the generated image was encrypted using the Rijndael algorithm. The results showed that the correlation between the elements of an image was decreased significantly by use of combination technique and higher entropy was achieved[2]. Stefan Mangard proposed highly scalable and regular hardware architecture for AES which was suited for full-custom as well as for design flows of semicustom. This architecture was scalable in terms of throughput, used key sizes. Similarities of encryption and decryption were utilized for high level of performance by using only a relatively small area[3]. Hung-Yu Chien presented an efficient time bound hierarchical key assignment scheme. New time-bound key assignment scheme is proposed by them for a tamper-resistant device. Computational performance and reduction in the cost of implementation is improved efficiently[4]. Ho Won Kim designed a asymmetric key crypto processor and its application and implemented to a Securing a System. A special-purpose microprocessor was optimized for the execution of cryptography algorithms[5]. This crypto processor can be used for various security applications such as storage devices, embedded systems, routers, security gateways using IP Sec and SSL protocol, etc. Aloka Sinha and Kehar Singh proposed a technique in which the digital signature of the original image was added to the encoded version of the original image. Then a suitable error code is followed to do encoding of the image, ex: Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature is used to verify the authenticity of the image [6].

III. BLOCK DIAGRAM

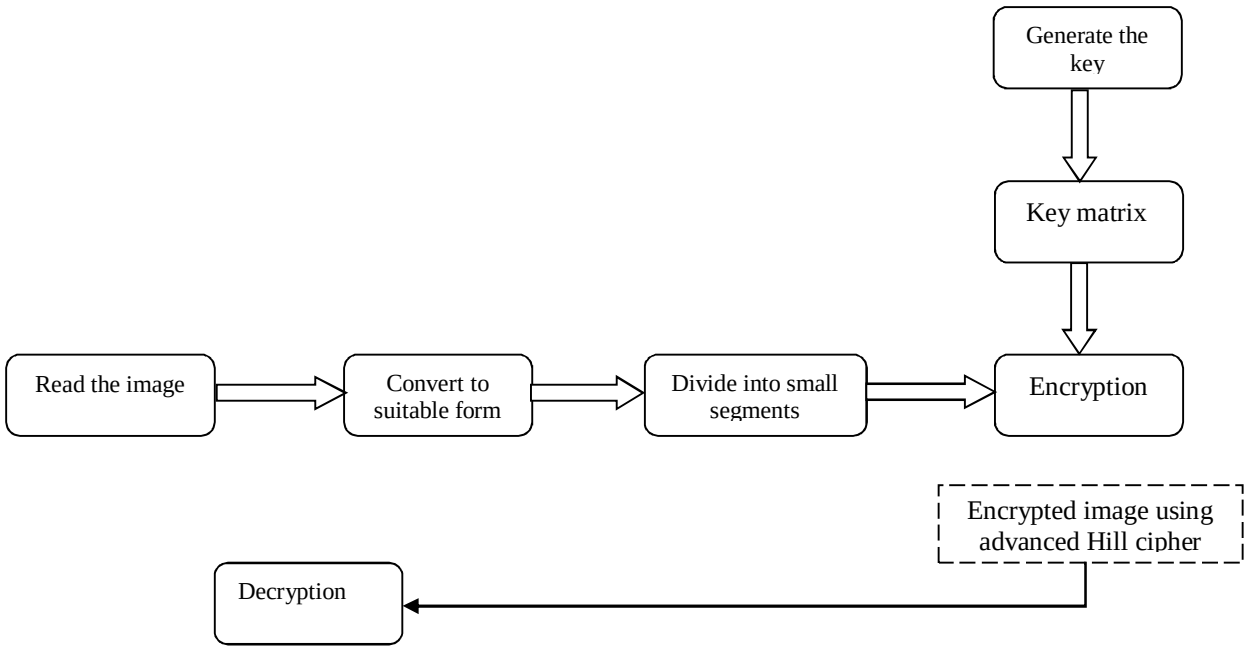


Fig. 1 Block Diagram of the proposed algorithm

IV. PROPOSED ALGORITHM

A. Original image is converted into suitable form. In this proposal we converted the original message image into 256x256 matrix
B. The 256x256 image is divided into 2x2 sub-matrices.
C. The 2x2 key matrix is generated.
D. Performing arithmetic operations using key matrix on the sub-matrix
E. Convert the resultant image into RGB format and encrypt using advance Hill cipher algorithm using the key matrix

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

F. By the side of receiver end, decrypt the image by using the same key matrix which is used in the encryption process

V. EXPERIMENTAL RESULTS

We have taken different images and encrypted using our proposed algorithm and the results are shown below.

Fig.2 Original Image 1 Fig.5 Original Image 2

Fig.3 Encrypted Image 1 Fig.6 Encrypted Image 2

Fig.4 Decrypted Image 1 Fig.7 Decrypted Image 2

VI. STATISTICAL ANALYSIS

Sl. No.	Name of the Image	Entropy of the encrypted Image	Correlation coefficient between original image and encrypted image
1	Camera man	5.3224	0.4736
2	Forest	6.1006	0.2876
3	Shadow	5.6827	0.3831
4	Circuit	4.7892	0.5180

VII. CONCLUSION

The proposed algorithm has better value for all analytical results. Here 128 bit key is used, hence it has 2^{128} combinations, so that it resists brute force attack. The method used is substitution, no transformation is applied. The original image matches with decrypted image with very minimum error margin. Further number of rounds can be extended in order to achieve more entropy and very less correlation coefficient between original and encrypted image.

REFERENCES

[1] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., "A new modified version of Advance Encryption Standard based algorithm for image encryption",Electronics and Information Engineering (ICEIE), 2010 International Conference .

[2] Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" , IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008

[3] S. Mangard, M. Aigner and S. Dominikus, "A Highly Regular and Scalable AES Hardware Architecture", *IEEE Transactions on Computers*, Vol. 52, No. 4, pp. 483- 491, 2003.

[4] H. Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme", IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, pp. 1301-1304, 2004.

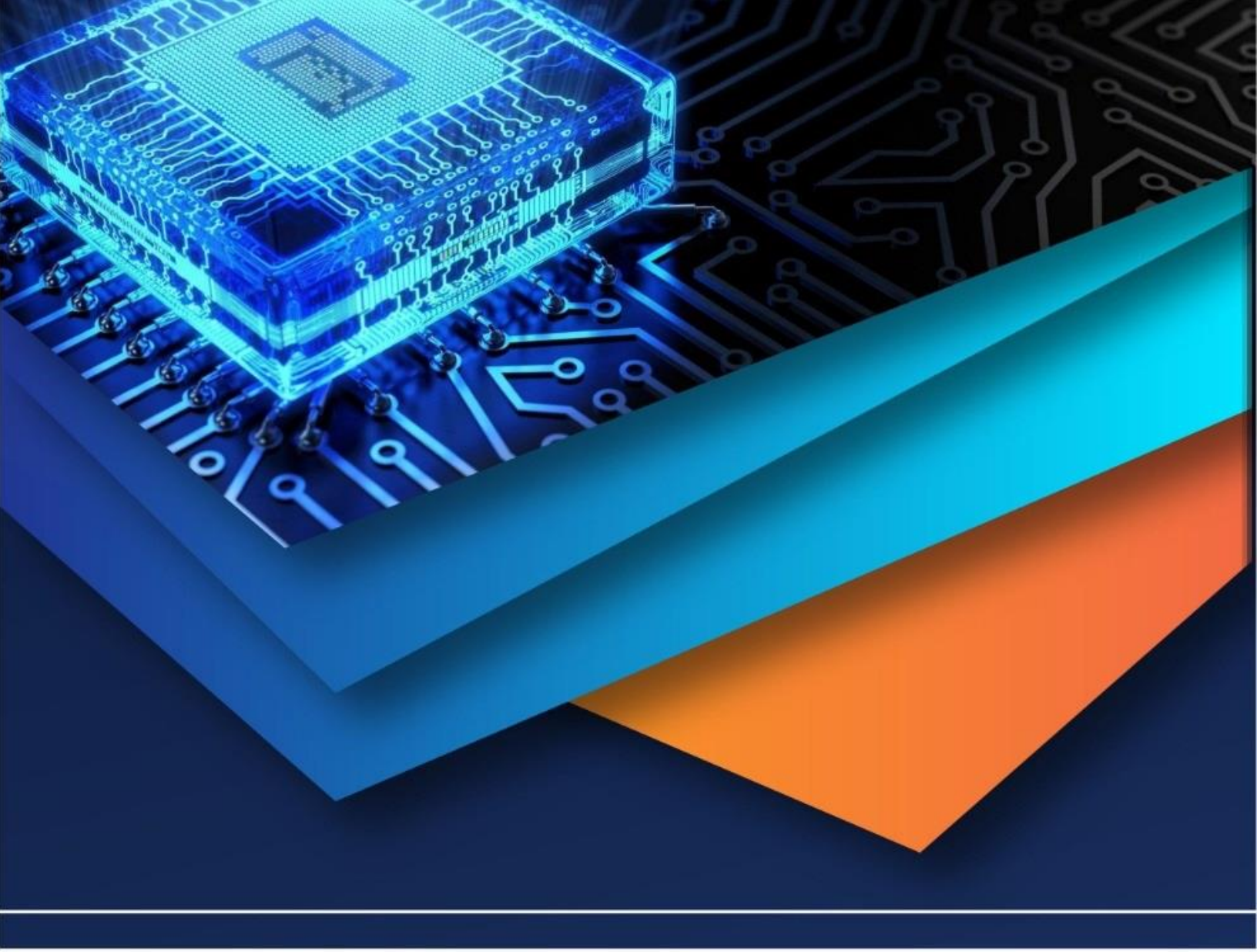
[5] H. W. Kim and S. Lee, "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System", IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 214224, 2004.

[6] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[7] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications, Vol. 9– No.7, pp,1923,November 2010.

[8] Bibhudendra Acharya et al. "Involutory, Permuted and Reiterative key Matrix generation Methods for Hill Cipher System". International Journal of Recent Trends in Engineering, Vol.1, No.4, May 2009, pp.106-108.

[9] Amanpreet Kaur, Renu Dhir, and Geeta Sikka , "A New Image Steganography Based On First Component Alteration Technique", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3,pp,53-56 ,2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY