A Hybrid Approach for Data Hiding using Cryptography Schemes

Gurtaptish Kaur[1], Sheenam Malhotra[2]
[1]Research Fellow, [2]Asst. Professor
[1,2]Sri Guru Granth Sahib World University,Fatehgarh Sahib,Punjab.

Abstract *—* ***The use of internet increases for communication and for other more aspects. There are number of Cryptography scheme that used to increase security where we discuss about the confidential information transfer. As unauthorized access & data loss increases so, in this work we proposed a hybrid approach to hide secret data in other file that it can't be lost or accessed by unauthorized user. This hybrid technique can be proposed by using advance hill cipher and DES to enhance the security which can be measured by calculating PSNR & MSE values. This technique is a new technique for hiding text data behind the image file and increase the security.***

***Keywords*— Cryptography, Data hiding, Encryption, Security.**

I. INTRODUCTION

Cryptography is the study of Secret (crypto-)-Writing (graphy).It is the science or art of encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original form. As the field of cryptography has advanced; cryptography today is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of information under difficult circumstances. Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives when we sign our name to some document and for instance and move to world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication.

Cryptographic mechanisms can be used to control access to shared disk drive, a high security installation, or a pay-per-view TV channel. The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication (Handbook of Applied Cryptography). Cryptography, the science of encryption plays a central role in mobile phone communication, e-commerce, Play-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily. In cryptographic systems, the term *key* refers to numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Secret key cryptography is also known as *symmetric key* cryptography. With this type of cryptography, both the sender and the receiver know the same secret code.

Encryption and Decryption

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an undecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other encryption algorithms can operate on much smaller keys relative to the message. Encryption and decryption are two mathematical functions that are inverses of each other. along with encryption as it's opposite. Decryption of encrypted data results in the original data. Encryption and decryption are two mathematical functions that are inverses of each other.

There are several ways of classifying cryptographic algorithms. For purposes of the paper will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use different types of algorithms.

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.

There are some specific security requirements, including:

a) Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)

b) Privacy/confidentiality*:* Ensuring that no one can read the message except the intended receiver.

c) Integrity*:* Assuring the receiver that the received message has not been altered in any way the original.

d) Non-repudiation*:* A mechanism to prove that the sender really sent this message.

Benefits of Cryptography

- It hides the message and privacy is secure.
- No one would be able to know what it says unless there's a key code.
- They can provide digital signatures that cannot be repudiated and the benefits of cryptography are well recognized. Encryption can protect communications and stored information from unauthorized access and disclosure.
- Other cryptographic techniques, including methods of authentication and digital signatures, can protect against spoofing and message forgeries. Practically everyone agrees that cryptography is an essential information security tool, and that it should be readily available to users.

II. Related Work

Devendra Kumar Malakar, Prof. Dineshchandra Jain [2] said that the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6) and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5". Cryptographic techniques to provide the problems what actually they have for which consider few example and listed corresponding errors that comes with these techniques and found the different errors that leads to different problem solving approach. One time pad technique is highly secure and suitable for small plain text but is clearly in practical for large messages.

Hill Cipher

The Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput. However, Hill cipher succumbs to a known plaintext attack and can be easily broken with such attacks. To overcome the weak security of the Hill algorithm, we present a method for adjusting the key matrix for achieving higher security and better image encryption. This method is easier to implement compared to other techniques like self invertible matrix etc. and if the block size and the modular index is suitably chosen it becomes extremely tuff to crack it by brute force as it is not very easy to find multiple inverses of a higher square matrix of higher order.

Hill ciphers provide a significant improvement in security over Viennese ciphers. They are very easily attacked if a few correct characters. The security of the Hill cipher depends on confidentiality of the key matrix K and its rank n. When *n* is unknown and the modulus *m* is not too large, the opponent could simply try successive values of *n* until the key is found. If the guessed value of n was incorrect, the obtained key matrix would be disagreed with further pairs of plaintext and cipher text. The most important security flaw of the Hill cipher is regarded to its vulnerability to the known plaintext attack since it can be broken by taking *n* distinct pairs of plaintext and cipher text. The total number of blocks depends on the length of input. The Hill cipher against the known-plaintext attacks includes some flaws and is vulnerable to the chosen cipher text attack. The security of the Hill cipher depends on confidentiality of the key matrix K and rank *n*. When *n* is unknown and the modulus *m* is not too large, the opponent could simply try successive values of *n* until he founds the key. If the guessed value of *n* was incorrect, the obtained key matrix would be disagreed with further plaintext-cipher text pairs. The most important security flaw of the Hill cipher is regarded to its vulnerability to the known-plaintext attack. It can be broken by taking just *n* distinct pairs of plaintext and cipher text of plaintext are already matched to a cipher text message, a so-called known plaintext attack.

Strengths of Hill Cipher

- It is resistant to the frequency letter analysis.
- It also very simple for uses matrix multiplication.

- It has high speed and high throughput.
- The key matrix is easy to calculate.

Limitation of Hill Cipher

- Non invertible key matrix over $z_{m.}$
- Security of Hill Cipher against known plaintext attack because all steps in Hill Cipher depend on linear algebra calculation.
- Hill Cipher is less variety of options for key matrix used public key to send the secret key.
- The key generation always difficult when key not invertible is solved.

Mohsen Toorani and Abolfazl Falahati [6] said that The Hill cipher is a classical symmetric encryption algorithm that succumbs to the know-plaintext attack. Although its vulnerability to cryptanalysis has rendered it unusable in practice, it still serves an important pedagogical role in cryptology and linear algebra. In the paper, a variant of the Hill cipher is introduced that makes the Hill cipher secure while it retains the efficiency. In this paper, a symmetric cryptosystem is introduced that is actually a secure variant of the Affine Hill cipher. It includes a ciphering core for which a one-pass cryptographic protocol is introduced. The outer structure of the ciphering core is similar to the Affine Hill cipher but its inner manipulations are different. Each block of data is encrypted using a different random number that is generated using a chained hash function. The proposed cryptosystem thwarts the known-plaintext, chosen cipher text, and chosen-plaintext attacks. Since the modulus is a prime number, the key space is greatly increased and the cipher text-only attack is also thwarted.

Affine Hill Cipher

The Affine Hill cipher is an extension to the Hill cipher that mixes it with a nonlinear affine transformation so the encryption expression. This concept in the encryption core of our proposed cryptosystem give more randomization to the introduced scheme and to strengthen it against the common attacks, each block of data is encrypted using a random number. For avoiding multiple random number generations, only one random number is generated at the beginning of encryption and the corresponding random numbers of following data blocks are recursively generated using HMAC. The time complexity of the conventional methods since it corresponds with the worst situation. The computational costs of the proposed scheme for encrypting and decrypting each block. The Affine Hill cipher extends the concept of Hill cipher by mixing it with a nonlinear affine transformation the encryption expression concept to introduce a secure variant of the Hill cipher. Since a shift cipher can produce only 25 different distinct transformations for the text, it is not a very secure encryption method. The affine cipher is a generalization of the shift cipher that provides a little bit more security. The affine cipher applies multiplication and addition to each character using the function.

Adi Narayana Reddy Ka, Vishnuvardhan B [9] said that the secure transmission of any form of data over a communication medium is prime important across the globe or in research arena. Cryptography is a branch of cryptology and it provides security for data transmission between any communicating parties. The Hill cipher is one of the symmetric key substitution algorithms. Hill Cipher is vulnerable to known plaintext attack. The paper presents an enhancement to the Hill cipher by utilizing the circulate matrices. The proposed technique shares a prime circulate matrix as a secret key and choose a non-singular matrix as a public key in such way that the determinant of the coefficient matrix is zero. Computational cost shows that the proposed technique is efficient and it thwarts all the security attacks.

Advance Hill cipher

The proposed algorithm is based on Affine Hill cipher, which is the combination of Hill cipher and affine cipher. Affine Hill cipher mixes the Hill cipher with a nonlinear affine transformation (Stindon, 2006). Differing from the Hill cipher, the plaintext is encrypted as C = PK + V (mod m). To produce a robust cryptosystem, extend this encryption core. This extension will solve the noninvertible key matrix problem and increase the randomization of the algorithm to enhance its resistance towards common attacks. With the proposed algorithm, the plaintext is encrypted as C = PK + RMK (mod m) with three parameters, α, β and γ. The non-invertible key matrix problem is solved by implementing an algorithm proposed by Bibhudendra (2006). The algorithm produces an involuntary key matrix which can be used for both encryption and decryption process. Obviously, it reduces the computational complexity in decryption. Besides, a random matrix key, RMK is needed for encryption apart from the involuntary key matrix. RMK is computed based on the previous cipher text blocks and a multiplying factor. It enhances the security of the proposed algorithm as it increased the resistance of the algorithms to known plaintext attack. The comparison done on previously had showed that Hill++ is better compared to the existing Hill algorithms. But, depending on this comparison only is not enough in judging the encryption quality of the proposed algorithm. Thus, two measuring techniques have been used to evaluate the encryption quality of the proposed algorithm. These techniques are the maximum deviation measures Ziedan *et al*. (2003) and the correlation coefficient measures.

Strengths of Advance Hill Cipher

- Solve the Non-invertible key matrix problem.
- It is time-consuming as the decryption process involved the computation of an inverse key matrix.
- Save the computational time for encryption and decryption.
- Increase the randomization of the key.

Limitation

- Encryption process is totally failed.
- Correlation Coefficient is not correlated for quality of encryption.
- Two variables are not correlated.

III. Proposed Hybrid Approach

Data hiding using hybrid approach deals with hiding the data in some other content or data. This proposed hybrid approach is an enhanced approach that uses Advance Hill-cipher & DES techniques.

3.1 Proposed Model

The proposed modal focuses on following objectives which are helpful in increasing security to prevent data from malicious users and are implemented using MATLAB.

a. To propose a new hybrid data hiding technique using Cryptography & Encryption Algorithms.
b. Cryptography scheme uses advance hill cipher with DES encryption algorithm.
c. To implement security using password authentication.
c. Prevent confidential data from malicious users.

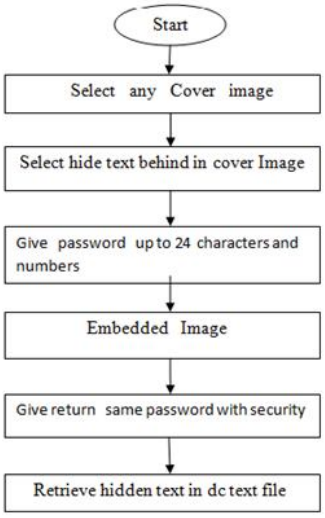

Fig 1: Proposed Model

In this proposed hybrid approach advance hill-cipher algorithm generate cipher and DES algorithm generates key. After Key generation, a secret data can be embedded to original image. One additional feature is also added that is to add password authentication up to 24 characters & it forms a crypt-image which hides our secret data.

3.2 Proposed Hybrid Algorithm

Encryption Algorithm:

1. Randomly select the cover image and hide text data in dem = Size, p = (RGB) mod N.

2. .Randomly select the characters or numbers for password authentication max = (size(x)).

3. Select the plaintext to be hidden P=R+B, P= (P+A) mod N.
P=Plaintext, R=Red, A=Advance Hill Cipher, N=length of matrix, M= Value of modulus , B=Blue .

4. Combine RGB colors for substitute (R, G, B) and permutate (R,B) [N M]=size(P) and inverse key of Advance hill Cipher for encryption.

Decryption

1. Select retrieve data and hidden data store in doc text file R= involute (k,d)

K=Key, D=Demensional

For I =1 to N

For j=1 to M

C= permute(R, B), C=Substitute(R, G,B)

2. For decryption image RMK=C-P(R, G)-C-S(R, G,B).
RMK=Random Matrix Key, C=Cipher text, P=Permutate, S=Substitute.

IV. Results and Discussion

Secret text hiding basically deals with hiding the text in the digital representation of the image. In the proposed work an enhanced approach using Advance Hill-cipher & DES techniques is discussed encryption add one more feature that is password authentication to enhance the security. Add the password up to 24 characters and it will be used for further query when are going to retrieve back our secret data. The requirements of a secret text hiding system when used for cryptographic purposes are of high hiding capacity and imperceptibility. Keeping in

view some conflicting features a reasonable amount of text data has been taken to be embedded in the cover medium. The strength of the algorithm is discussed by explaining the complexities in encryption and decryption. The concept can be further enhanced by adding digital signatures to the cipher and the key.

4.1 Select Cover Image

In Fig 2 Select any cover image for encryption process and choose any .jpg image and .jpeg image for embedding image and behind hide text in cover image for embedding image and randomly select any characters or numbers of password for security authentication. Compute time take to cover image and hide text behind the cover image process.

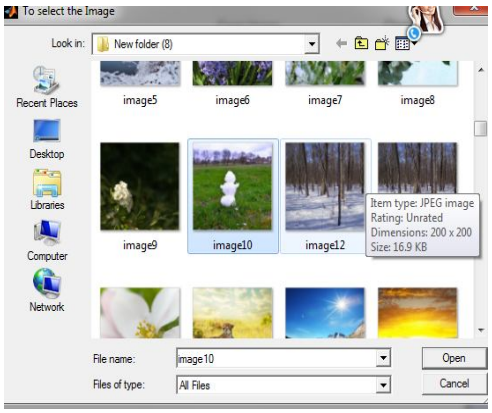

Fig 2: Select image for encryption process

4.2 Hide text

In Fig 3 Select a cover image and hide any text data behind the image by selecting the text file and set any password upto24 characters for securing. Add one feature that is password up to 24 characters and it will be used for further query when are going to retrieve back our secret data.

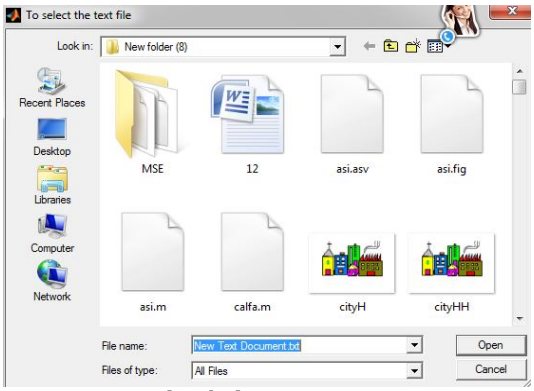

Fig 3: Select hide text in cover image

4.3 Retrieve Data

In Fig 4, For retrieving text back, enter the same password which was given first and secret data then stored in text file named dc text and calculate elapsed time for image process.

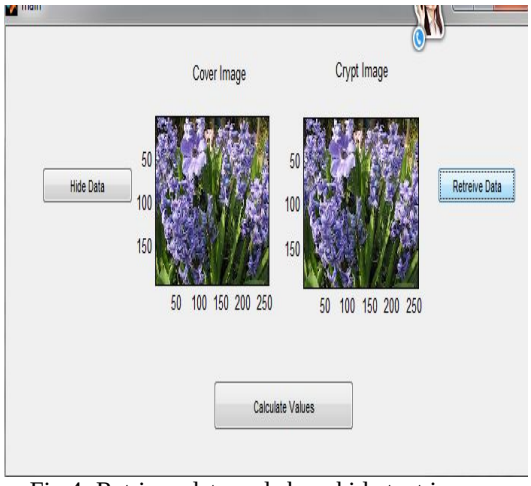

Fig 4: Retrieve data and show hide text in cover image

4.4 Some Cover Images

Fig 5 shows the original or cover images that can be used to hide the text during encryption process. All these cover images that are taken to hide text having resolution 255 x 255.

Fig 5: Collection of some cover Images

4.5 Some Embedded Images

Fig 6 Shows the embedded images , which are made from cover images during encryption process. Embedded images are those images which hides the text behind itself for security purpose .

Fig 6: Collection of some Embedded Images

Table 1: Calculate some images of MF1 and MF2

IMAGES	MF1(PSNR)	MF2(MSE)
palacio.png	105.42	-0.5321
city.png	104.83	-0.4971
white and red.jpg	104.85	-0.4991
water and red.jpg	104.82	-0.4324
purple flower.jpg	104.64	-0.5063s
green grass.jpg	104.11	-0.5063
white.jpg	104.27	-0.5163
pick flower.jpg	104.54	-0.5163
roots.jpg	106.99	-0.3924
desert.jpg	104.55	-0.5160
.jpg	104.40	-5.1332
lily.jpg	104.96	-0.4860
Tiger.jpg	104.79	-0.4905
sunshine.jpg	104.35	-0.5284
yellow blend rose.jpg	103.66	-0.5065
sunrise.jpg	104.76	-0.5111
river.jpg	104.63	-0.4964
Image19.jpg	103.99	-0.5002
Image20.jpg	104.76	-0.5221
green.jpg	104.87	-0.4984
green flower .jpg	104.45	-0.5186
white lily.jpg	103.89	-0.5321
pink flowers .jpg	104.87	-0.4901
white roots.jpg	104.67	-0.5065

To check the quality or effectiveness of the system. Calculate measuring factors named as MF1 and MF2 .MF1 includes the PSNR values and MF2 includes MSE values. Table 1 presents details of cover image with corresponding measuring factors that are peak signal to noise ratio PSNR (MF1) & Mean Squared Error (MF2). The (MF1) PSNR & (MF2) MSE has been calculated as follows. It is an important image, objective, quality index. It is actually a measure of quality of image when external data is embedded in it. It gives an idea about how much deterioration has embedding caused to the image.

V. CONCLUSION & FUTURE SCOPE

Network security covers a variety of computer networks, both public and private that are used in everyday jobs conducting, transactions communications in businesses, government agencies and individuals. Network security is involved in organizations, enterprises and other types of institutions. The requirements of a secret text hiding system when used for cryptography purposes of high hiding capacity and imperceptibility. Keeping in view some conflicting features a reasonable amount of text data has been taken to be embedded in the cover medium .In proposed scheme any image is taken as input that calculate the elapsed time for text hide and image process which gives better results as compared to other techniques like Hill Cipher and advanced Hill Cipher. The proposed work is a secret text hiding approach, which is the combination of Advance Hill cipher & DES techniques for securing confidential data from unauthorized access. DES is used for data hiding processing in little time.

In future, a new algorithm can be designed to embed and extract a secret data using artificial intelligence technique will be used in embedding process. These techniques can be used for defense research department for data exchange even for ERP (Enterprises Resource Planning) systems. Advance Hill cipher and DES may be used for data mining. Advance Hill cipher and DES may be also used for protocol data exchange and IP hiding.

REFERENCES

[1] Elayaaraja and M.Sivakumar, "*Securing data using 4 variables linear block cipher Asymmetric key Algorithm*", International Journal of Computers and Distributed Systems www.ijcdsonline.com Vol.1, Issue 3, October 2011.

[2] Devendra Kumar Malakar, Prof. Dineshchandra Jain, "*The Problem Analysis on Encryption Techniques in Cryptography*", International Journal of Societal Applications of Computer Science, Vol.2 , Issue 5 ,May 2012.

[3] A. Bagherzandi, M. Salmasizadeh, and J. Mohajeri, "*A related key attack on the feistel type block ciphers,*" International Journal of Network Security, Vol. 4 No 4,issue 2,2010.

[4] L. Sreenivasulu Reddy "*A New Modal of Hill Cipher Using Non- quadratic Residues*", International Journal of Soft Computing and Engineering,, Vol.2, Issue-2, May 2012.

[5] V. Umakanta Sastry, N. Ravi Shankar, "*A Modified Hill Cipher Involving Interweaving and Iteration*", International Journal of Network Security , Vol. 4, pp .11-16, July 2010.

[6] Mohsen Toorani, Abolfazl Falahati , "*A Secure Cryptosystem based on Affine Transformation,*" Journal of Security and Communication Networks, Vol. 4,Issue 2, pp. 207-215, Feb. 2011.

[7] O.Y. Chuan and M.R.K. Ariffin," *A Novel Enhancement Technique of the Hill Cipher for Effective Cryptographic Purposes*", Journal of Computer Science, Department Computer Science, Faculty of Informatics, University,Vol.7, Issue No.2,pp.785-789,2011.

[8] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrah, " *Novel Methods of Generating Self-Invertible Matrix for Hill ,Cipher Algorithm*", International Journal of Security (CSC Journals), Vol. 4, Issue 1, pp. 14-21, 2007.

[9] Adi Narayana Reddy Ka, Vishnuvardhan B," *Generalized Affine Transformation Based on circulate Matrices"* ,Department of CSE, Hyderabad Institute of Technology and Management, Hyderabad, Vol, 5,Issue 5,pp.332-335,2012.

[10] A. H. Rushdi and F. Mousa, "*Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher*", International Journal of Computer Science and Network Security, Vol.5, Issue 5, pp. 11-16, 2009.

[12] A. Bibhudendra, K. P. Saroj, K. P. Sarat and P. Ganapati, "*Image Encryption using Advanced Hill Cipher Algorithm*", International Journal of Recent Trends in Engineering, Vol. 1, Issue 1, pp. 663-667,2009.

[13] I. E. Ziedan, M. M. Fouad and D. H. Salem, "*Application of data encryption standard to bitmap and JPEG images*", in Proc. 12th National Radio Science conference, Cairo in Hyderabad, pp. 1-8, 2003.

[14] Sanagurunathan, V.Rajendran and Dr.T.Purusothaman ," *Classification of Substitution Ciphers using Neural Networks*", International Journal of Computer Science and Network Security, Vol.10,Issue.3, March 2010.

[15] G. Usha Devi , Ipsita Rana, Sutanu Nandi," *Multilevel Encryption System using Graceful Codes"* ,International journal of advanced research in Computer Science and Software Engineering, Vol. 2, Issue 3, pp-438-440,March 2012.

[16] Jeffrey Overbev, William Travels and Jerzy Wojdylo," *On the Key space of the Hill Cipher, Cryptology*", International journal of science computer ,Vol.2,pp 59–72, January 2005.

[17] Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu," *A generalized scheme for data encryption technique using a randomized matrix key"*, International Journal of Discrete Mathematical Sciences, Vol. 10,Issue 1, pp 73-81, Feb 2007.

[18] L.Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "*An efficient Protocol for Authenticated Key Agreement*," Journal of Designs, Codes and Cryptography, Department of Computer Security ,Vol.2, pp.119-134, 2003.

[19] M. Nordin A. Rahman, N. S. M. Usop" *Cryptography: A New Approach of Classical Hill Cipher*" ,International Journal of Security and Its Applications Vol. 7, March 2013.

[20] P. Lin, W. L. Wu, C. K. Wu, "*Security analysis of double length compression function based on block cipher*," International Journal of Network Security, Vol. 4, pp. 121-127, 2007.

[21] Ram Chandra S. Mangrulkar1, Pallavi V. Chavan2,"*Encrypting Informative Image by Key Image using Hill Cipher Technique"* International Journal of Recent Trends in Engineering, Vol. 1, Issue 1, May, 2009.S

[22] Ruisong *Ye Wei Zhou, "An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice*" **,**International Journal of Information and Communication Technology Research, Department of Mathematics, Shantou University Shantou Guangdong ,China ,Vol. 1, Issue 8, December, 2011.

[23] V. U. K. Sastary and V. Janaki, "*A modified hill cipher with multiple keys*," International Journal of Computational Science, Vol. 2,Issue 2, pp. 815-826, 2008.

[24] Y. 8. Kurniawan, A. S. A., M. S. Mardiyanto, I. S. S.,and S. Sutikno,,"*The new block cipher: BC2*," International Journal of Network Security, Vol. 8, Issue1, pp. 16-24, 2009.