Advance Cryptography Scheme for Data Hiding using Advance Hill cipher & DES

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

Abstract **—** ***Cryptography is a scheme that used to increase security in most of the fields. Security is mandatory where we discuss about the confidential information. As with know, the use of internet rises, most of organizations transfer their confidential information through internet which is not fully secure and there is a chance of data loss or unauthorized access. In this work, we proposed an advance technique to hide secret text data in image file that it can't be lost or accessed by malicious user. In this proposed technique, we use advance hill cipher and DES to enhance the security level which can be measured by some measuring factors. The result of this work shows that this advance hybrid scheme gives better results than previous techniques.***

Keywords**— Security, Data hiding, Cryptography, Hill-cipher++, DES.**

I. INTRODUCTION

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Cryptography can be strong or weak, as explained above. Cryptographic strength is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. One would think, then, that strong cryptography would hold up rather well against even an extremely determined cryptanalyst No one has proven that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by PGP is the best available today. Vigilance and conservatism will protect you better, however, than claims of impenetrability.

Computer security people often ask for non-mathematical definitions of cryptographic terms. The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the cipher text. Thereafter, things get somewhat more complicated. There are a number of cryptographic primitives— basic building blocks, such as block ciphers, stream ciphers, and hash functions. Block ciphers may either have one key for both encryption and decryption, in which case they're called shared key (also secret key or symmetric), or have separate keys for encryption and decryption, in which case they're called public key or asymmetric. A digital signature scheme is a special type of asymmetric crypto primitive.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet. Within the context of any application-to-application communication, 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.

Cryptography then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

Advantages of Cryptography

1. Confidentiality (secrecy)
Only the sender and intended receiver should be able to understand the contents of the transmitted message.
2. **Authentication**
Both the sender and receiver need to confirm the identity of other party involved in the communication.
3. **Data integrity**
The content of their communication is not altered, either maliciously or by accident, in transmission.
4. **Access control**
An entity cannot access any entity that it is not authorized to.
5. **Anonymity**
The identity of an entity if protected from others

II. Security Using Cryptography

P. Elayaraja et al. said that Modern Cryptography abandons the assumption that the Adversary has available infinite computing resources, and assumes instead that the adversary's computation is resource bounded in some reasonable way [1]. In Particular, it may be assumed that the adversary is a probabilistic algorithm which runs in polynomial time. Similarly, the encryption and decryption algorithms designed are probabilistic and run in polynomial time. The running time of the encryption, decryption, and the adversary algorithms are all measured as a function of a security parameter k which is a parameter which is fixed at the time the cryptosystem is setup. In this paper a new concept combining cryptography and Rubik's cube has been introduced for information security and network security. Detailed steps with illustrations, of the concept have been described. Also the strength of the algorithm is discussed by explaining the complexities in encryption and decryption. This concept can be further enhanced by adding digital signatures to the cipher and the key transfer process. Also to avoid the evaluation complexity in the higher order cubes, the data can be fragmented and multiple lower order cubes can be processed in a distributed manner. This concept can be used for basic applications such as credit card transactions, pin transfers, bank account management, password management etc. Complex applications like defence data transfer which requires high level security rather than lower time complexity can be dealt using this method operated over higher degree cubes.

Neetu Settia said that Asymmetric cryptography uses a Key pair instead of a single key. The two keys are related to each other mathematically. It uses trap-door one-way function, which is a one-way function for which the inverse direction is easy given a certain piece of information (the trap door), but difficult otherwise [2**]**. The public key gives information about the particular instance of the function; the private key gives information about the trap door. Whoever knows the trap door can compute the function easily in both directions, but anyone lacking the trap door can only perform the function easily in the forward direction.

Anders Larsson said that choosing the correct algorithm for encryption can be crucial depending on the information the algorithm is suppose to protect. As described throughout the paper it is not only the algorithm that matters, but also the length and composition of the key used. When deciding on a length of the key one should consider for how long the information is needed to stay secure, and from whom one is protecting it [6]. In general a larger key length is always more secure. Choosing between asymmetric and symmetric algorithms should be based upon the intended use of the algorithm. If the key is needed to be sent over insecure pathways a asymmetric algorithm should always be used, on the other hand if the information is only to be stored in a safe environment and the key is never needed to be distributed among users a symmetric algorithm should be used. Symmetric algorithms are considerable faster than the asymmetric algorithms. Although the implementation was considerable helped by the Java programming languages support for arithmetic on arbitrary large integers. While implementing, it was easy to see that the asymmetric algorithm is based on a more mathematical foundation while the symmetric once is more straightforward. Since more and more information are stored and transferred using computers, encryption becomes more important to assure security to users, and will continue to develop.

Yousuf Ibrahim Khan et al. said that some more technical improvements are possible in future also. Like it is common practice to divide a digital system into software and hardware components. The greatest functionality and performance occurs when functions

are placed in dedicated system hardware that is highly parallel and is optimized to perform the intended operations. More often than not it is far too expensive in time and money to create such dedicated hardware so the available hardware resources are used to implement a conventional processor which executes programmable instructions in a highly sequential manner. So a dedicated system could be possible to create to detect handwritings in different environments and also in Real-Time [3]. Some applications that could greatly benefit from this technology include Real time processing, Data encryption/decryption, RSA cryptography, Data Compression, Image and video processing. The experiment conducted in this study reveals that neural networks approaches to character recognition was simple and achieved better results. Although in the cryptography technique discussed above was simple. It was done to show that it is possible to create an efficient method using simple ideas. A more improved technique could be employed to get better result in future.

Ram Chandra et al. focus on implementation of Informative Image Encryption using cryptographic principles. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering [4]. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. Until modern times, cryptography referred almost exclusively to encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., cipher text). Decryption is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (ideally, known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes.

III. Proposed Technique For Secret Text Hiding

Secret text hiding basically deals with hiding the text in the digital representation of the image. So, this work proposed an enhanced approach using Advance Hill-cipher & DES techniques.

3.1Proposed Model

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

a. To propose Enhanced Text Hiding Scheme using Advance Hill-cipher & DES Encryption Algorithms.
b. To implement security using password authentication.
c. Prevent from unauthorized access on confidential data.

In this proposed work, Advance Hill-cipher algorithm is firstly used to generate cipher and key generation can be done by using DES algorithm. After Key generation, a secret text can be embedded to original image. One additional feature is also added in it is that we add password authentication that is a password of up to 24 characters & it forms a crypt-image which hides our secret text message.

3.2 Basic Design

Security is the major need to prevent our secret text data from unauthorized access while using internet to transfer the information. This proposed enhanced scheme use Advance Hill-cipher & DES Encryption schemes & generate a crypt-image where secret text can be hide. We can divide our design into different modules.

- Crypt Module
- Security Module
- Decrypt Module

3.2.1 Crypt Module:

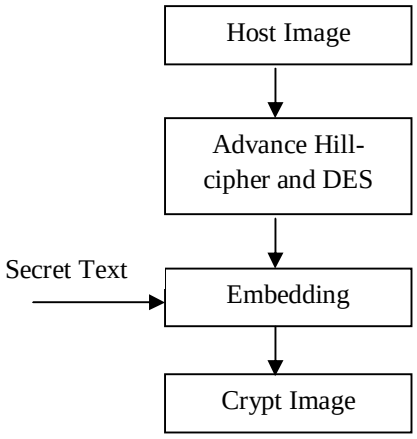

Fig 1: Basic Design of Crypt Module

In this crypt module as shown in Fig 1 encryption is done. Here we first select the original image and apply advance hill cipher to generate a cipher & add one more algorithm that is DES to generate key. Then secret text can be embedded with the original

image and it gives crypt image where our secret data is being hidden in encrypted form.

3.2.2 Security Module:

With encryption we add one more feature that is password authentication to enhance the security. We add this password up to 24 characters and it will be used for further query when we are going to retrieve back our secret data.

3.2.3 Decrypt Module:

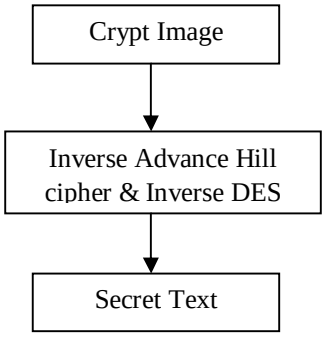

Fig 2: Basic Design of Decrypt Module

In this decrypt module as shown in Fig 2 decryption is done. Here we select our encrypted image and apply inverse advance hill cipher & DES to retrieve the secret data.

3.3 Algorithm

Encryption Algorithm:

Step 1: Select Cover Image (host image).

Step2: Select Secret Data.

Step3: Encrypt using Advance Hill cipher and key generation using DES.

Step 4: Enter password of character length up to 24.

Step5: Secret data hide behind the Embedded Image.

Decryption Algorithm:

Step1: Select the Embedded Image.

Step2: Enter the same password.

Step3: Apply Inverse Advance HILL Cipher and DES to decrypt the data.

Step4: Secret data saved in dctext.txt

IV. RESULTS AND ANALYSIS

The requirements of a secret text hiding system when used for cryptography 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 so as to keep degradation in the image quality minimum. For the testing the efficiency of the proposed scheme we used a test image. Fig 3shows the host images with their corresponding crypt-image.

Fig 3: Original Image & Crypt Image

Table 1 presents details of cover image with corresponding measuring factors that are peak signal to noise ratio PSNR (MF1) & Mean Squared Error (MF2). Further a comparison of the proposed secret text hiding scheme with the previous which uses only advance hill cipher and it can be shown in table 1. Fig 4 graphical comparisons between the proposed technique and that of previous one. The (MF1) PSNR & (MF2) MSE has been calculated as follows.

Peak Signal to Noise Ratio (PSNR):

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. It is represented as

$$PSNR = 10 \log_{10} \frac{255^2}{mse} \text{ db}$$

Where 'mse' is mean square error and is given by

$$mse = \left[\frac{1}{N * M}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})$$

Where N and M are image dimensions, and represent original and stego images respectively.

Table 1: MF1 & MF2 of Proposed scheme & Previous

Techniques	MF1	MF2
Previous	103.0	0.00081

Proposed	105.14	-0.4033

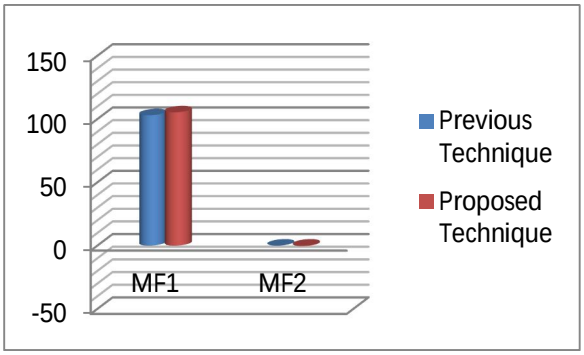

Fig 4: Previous Approach & Enhanced Approach

V. CONCLUSION

In this paper, we proposed a secret text hiding approach, which is Enhanced Approach using Advance Hill cipher & DES techniques, for securing confidential data from unauthorized access. One extra authentication is added and that is password authentication. Embedding is done using this technique helps to least deterioration in the original image. This enhanced approach can achieve better results than the previous approach which used only advance hill cipher for text hiding.

REFERENCES

[1] P. Elayaraja and M. Sivakumar , "*New Approach and Additional Security to Existing Cryptography Using Cubical Combinatorics*".

[2] Neetu Settia ,"*Cryptanalysis of Modern Cryptographic Algorithms*" Vol. 1, Issue 2, December, 2010

[3] Anders Larsson, "*Cryptography*", A personal project in the course TDDD55 By Anders 760903-7192.

[4] Yousuf Ibrahim Khan, Saad Mahmud Sonyy, S.M. Musfequr *Rahman ,"Image based Cryptography from a distance"*

[5] Ramchandra S. Mangrulkar1, Pallavi V. Chavan2,"*Encrypting Informative Image by Key Image using Hill Cipher Technique"* International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May, 2009.

[6] 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 ,Volume 1, No. 8, December, 2011.

[7] Xiaoyi Zhou*1,2, Jixin Ma2, , Yongzhe Zhao, *Ergodic Matrix and Hybrid-key Based Image Cryptosystem"* Computer Science and Technology School, Jilin University, Changchun, Jilin, China, June, 2011.

[8] Mao, Y. B., Chen, G., Lian, S. G.,*" A novel fast image encryption scheme based on the 3D chaotic Baker map.* International Journal of Bifurcation and Chaos ,14, 613--3624 ,2004.

[9] Y. Rangel-Romero, G. Vega-García, A. Menchaca-Méndez, D. Acoltzi-Cervantes, L. Martínez-Ramos, M. Mecate-Zambrano, F. Montalvo-Lezama, J. Barrón-Vidales, N. Cortez-Duarte and F. Rodríguez-Henríquez, "Comments on How to repair the Hill cipher", Journal of Zhejiang University Science A, vol. 9, no. 2, **(2006)**, pp. 211-214.

[10] A. H. Rushdi and F. Mousa, "Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher", Int'l Journal of Computer Science and Network Security, vol. 9, no. 5, **(2009)**, pp. 11-16.

[11] D. R. Stinson, "Cryptography Theory and Practice", 3rd edition. Chapman & Hall/CRC, **(2006)**, pp. 13-37.

[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, no. 1, **(2009)**, pp. 663-667.

[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, **(2003)**, pp. 1-8.

[14] M. Toorani and A. Falahati, "A Secure Variant of the Hill Cipher", in Proc. 14th IEEE Symposium on Computers and Communications, Sousse, **(2009)**, pp. 313-316.

[15] Mohsen Toorani, Abolfazl Falahati , "A Secure Cryptosystem based on Affine Transformation,"
Journal of Security and Communication Networks, Vol. 4, No. 2, pp. 207-215, Feb. 2011.