Modern Image Security Mechanism using Hill and Vernam Cipher

Mrs. Madhavi Verma
Student M. Tech Information Security
DIMAT Raipur

***Abstract*— Image is most important multimedia digital content transfers over internet in today's modern communication network. It contains the confidential information, which protection is achieved by encryption. In this methodology, authors achieved image security by applying Hill Cipher and Vernam Cipher together on image. In this paper, I have done the literature review on existing work for image encryption with detail study of SD-AIES and proposed my work to enhance existing method.**

I. Introduction

In today's modern communication network, digital images and documents travel widely and rapidly, in multiple manifestations, through email and across internet. With increase use of internet in 21st century digital images are exchanged over various types of networks. These digital images contain confidential information. Controlling and protecting sensitive and confidential information in images has become an important aspect of today information security system. So image security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security.

IJERT

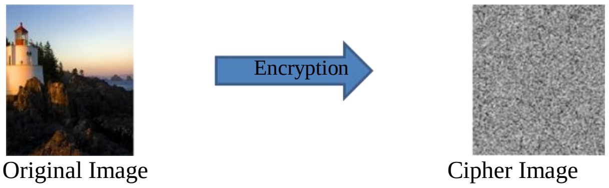

Figure 1. Image Encryption

Image encryption techniques try to convert original image to another image that is hard to understand; to keep image confidential between users. It means whenever we want to send image to someone that should be encrypted in such a way that no one can decrypt without knowing the key of the decryption process.

II. Difference between Text and Image Encryption

To better understand the image encryption there is need to first analyze the differences between implementations for image data and text data encryption. Basically, there are some differences between image and text data encryption.

- When Cipher text in produced, it must be decrypted to the original plaintext in a full lossless manner. However, the cipher image can be decrypted to the original plain image in some lossy manner.
- Text data are sequence of words. They can be encrypted directly by using block and stream ciphers. However, digital image are usually represented as two-dimensional (2D) arrays. For protecting the stored 2D arrays of data with text- processing algorithms, they must be converted to 1D arrays before using various traditional encryption techniques.
- Because the storage space of a picture is very large, it is sometimes inefficient to encrypt or decrypt images directly. One of the best method is to encrypt/decrypt information that is used by image compression only for reducing both its storage space and transmission time.

III. Basic Cryptography Techniques

Encryption is the process of encoding message/images such that it's meaning becomes not obvious; decryption is the reverse process: transforming an encrypted text/sound/data/image back into its normal form. A system of encryption and decryption is called a cryptosystem.

The art and science of keeping a message/image secure is cryptography, and it is practiced by cryptographers. Cryptography deals with the design and analysis of systems that provide secure communications or resist cryptanalysis.

Cryptanalysts are practitioners of cryptanalysis; the art and science of breaking Cipher text/image; that is, seeing through disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a restricted algorithm.

The security of the modern cryptography is based on the key. The range of the possible values of the key is called the key space.

Cipher systems can be classified according to key into two types: secret key systems and public key systems.

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

A. *Symmetric Key cryptography*

These algorithms encrypt and decrypt messages with a key in such a way that it is difficult to decrypt without the key. Because the encryption and decryption keys in a secret-key cryptosystem are the same, such systems are often called symmetric in the literature.

Most secret-key cryptosystems operate on messages one block at a time; a block may be 64 bits long, and the keys are usually short, say, 56 bits long. Ideally, an attacker's only approach is trial and error. Secret-key cryptosystems provide confidentiality and key management to parties who have previously agreed on a secret key.

B. *Asymmetric key Cryptography*

These algorithms encrypt and decrypt messages with two different keys in such a way that it is difficult to decrypt without the decryption key. The encryption key can be published without compromising security. And is called the public key for this reason; the decryption key is called the private key. Because the encryption and decryption keys in a public-key cryptosystem differ, such systems are often called asymmetric in the literature. The idea comes from Diffie and Hellman.

Public-key cryptosystems provide confidentiality and key management. They can be as secure as or more secure than secret-key cryptosystems, but they are generally slower. Their main advantage is that, since the encryption key can be published, parties need not first agree on a secret key. They are often combined with secret-key cryptosystems to gain the benefits of both: speed without prior secrets.

IV. Related Works

In order to protect digital images from unauthorized users doing illegal reproduction and modifications, a variety of image encryption schemes have been proposed. Most of the algorithms specifically designed to encrypt digital images were proposed in the mid-1990s.

One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a Visual Secret Sharing Scheme where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

Table 1. Comparison Table

Work	Methodology	Advantage	Disadvantage
A modified AES based algorithm for image encrypttion	* A5/1 key stream generator * W7 key stream generator	* W7 key stream generator improves the security of the AES algorithm * Better performance * The use of key stream generator for all types of images improves the encryption security * Overcome the problem of textured zones existing in other known encryption algorithms	* Time taking * Risky
Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm	Matrix Based and Encrypt Gray Scale * For gray scale image encryption use modulus of 256 * For Color image first decompose the color into R-G-B component, then encrypt, then concatenate encrypted component	* Computational complexity can be reduced matrix * Encrypt gray scale as well as color images * High Speed * High Throughput	Overcome the drawback of using a random key matrix * Not applicable in image with background of same gray level or same color * Suffered from known plain text attack
A New Image Encryption Approach using Combinational Permutation Techniques	* Combination of different permutation techniques * Higher Entropy and Correlation between image elements decreased	* Reduces the correlation between the pixel, bit or block of image * Higher entropy decreased	* Permutation process is too complex * Time taking * Chance of mistake is high
Symmetric key cryptosystem using combined cryptographic algorithms - Generalized	Clubbed both bit level and byte level generalized modified vernam cipher method with feedback * Bit level encryption * Byte level encryption	* Resistant to differential attack or known plain text attack * Effective for encrypting short message, password, confidential key * Brute force attack is not applicable	* Decryption procedure need exact initial random matrix * Time taking for large text

IJERT

modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm	* Exit		message
SD-EI: A Cryptographic Technique To Encrypt Images	Algorithm * Rotation and reversal * Extended Hill Cipher using Involutory Matrix	* Encrypt any image * Also able to encrypt stenographic image	* Time taking * Bit and byte manipulation need further enhancement
SD-AEI: An Advanced Encryption Technique For Images	Algorithm * Bit Rotation and reversal * Extended Hill Cipher using Involutory Matrix * Modified MSA randomization	* Upgraded version on SD-EI * Randomization process make it more secure * Take optimal amount of time to encrypt	* Small range of rotation of bit
An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES	Algorithm * Modified Bit Rotation and reversal technique using N_r * Extended Hill Cipher using Involutory Matrix * Generalized modified Vernam Cipher iv. Modified MSA randomization	* Upgraded version of SD-AEI * Inclusion of Vernam cipher make it more strong * Byte level encryption * Using effective number in Bit rotation and reversal process make more effective rotation	* Bit rotation still has 0-6 ranges * Need more secure randomization process * Time taking

V. Existing Methodology

SD-AIES method is devised by Somdip Dey and it is itself a successor and upgraded version of SD-AEI and SD-EI image encryption technique. The four different encryption modules, which make up SD-AIES Cryptographic methods, are as follows:

1) Modified Bits Rotation and Reversal Technique for Image Encryption
2) Extended Hill Cipher Technique for Image Encryption
3) Generalized Modified Vernam Cipher for File Encryption
4) Modified MSA Randomization for File Encryption

VI. Problem Identification in Existing Methodology

I analyze the all algorithm of the existing methodology and find some problem that are-

1. In the first stage of the problem a 'code' is generated from the given password which is of two digits. Therefore whatever password entered by the user will generate only two digit code which range from 10 to 99.

2. In bit rotation and randomization technique effective number generated by password is operated by modulus 7 i.e.

$N_R = N \bmod 7$

Where, '7' is the number of iterations required to reverse entire input byte and N = [n1 + n2 + n3 + n4 +……nj]. So there is only 7 type of randomization pattern in existing method.

3. In hill cipher we have to choose only self involutory matrix.

While reading other image encryption technique came to know that most of image encryption algorithm is suffered from some of common problem e.g., time taking encryption process, pixel correlation not reduced much more, risky etc.

VII. Proposed Methodology

My objective in this project is –

* Enhancing its Bit rotation and reversal method by applying different key generation method

* In previous work password randomization ranges only 1 to 7 i.e. only 7 type of randomization format possible so there is chance to two different password shows same type of randomization process. To overcome this problem I will apply/include some more parameters in randomization process e.g. change process of random generation

* I will try to extend Hill cipher by apply hill cipher twice on same input image.

IJERT

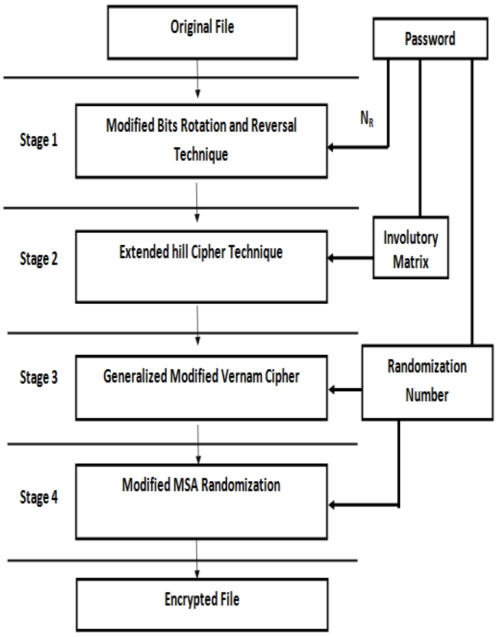
Original File
Password
Stage 1
Modified Bits Rotation and Reversal Technique
N_R
Stage 2
Extended hill Cipher Technique
Involutory Matrix
Stage 3
Generalized Modified Vernam Cipher
Randomization Number
Stage 4
Modified MSA Randomization
Encrypted File

Figure 2. Block Diagram of Methodology

VIII. Discussion and Future Scope

In this paper, the author proposes a standard method of image encryption, which first tampers the image and then disrupts the file structure of the image file. This encryption method is very successful to encrypt the image perfectly to maintain its security and authentication. The inclusion of modified bits rotation and reversal technique, and modified Vernam Cipher along with feedback mechanism, made the system even stronger than it used to be before. In future, the security of method can be further enhanced by adding more secure bit and byte manipulation techniques to the system. Cryptanalysis attack can also perform on the this image encryption scheme. Addition of another security strategies makes it more secure than others techniques.

Acknowledgement

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on image encryption. I sincerely express my gratitude to Mr. Akash Wanjari of Dept. of MCA, DIMAT for giving constant inspiration to complete this work. I am also thankful to Mrs. Preeti Tuli, Prof. Somesh Dewangan, Dept. of CSE, DIMAT for helping me directly and indirectly during this work. I am really thankful to my all friends for their blessing and support.

References

[1] M. Zeghid, M. Machhout, L. khriji, A. Baganne, and R.Tourki, “A modified AES based algorithm for image encryption”, *World Academy of Science, Engineering and Technology 27*, 2007, pp. 206-211.

[2] S.K. Panigrahy, B. Acharya, D. Jena, “Image Encryption using self-invertible key matrix of Hill cipher algorithm”, *1st International Conference on Advances in Computing,* Chikhli, India, 21-22 Febururary 2008, pp. 1-4.

[3] A. Mitra, Y.V. Subba Rao and S.R.M. Prasanna, “A New Image Encryption Approach using Combinational Permutation Technique”, *World Academy of Science, Engineering and Technology*, vol-14, 27-02-2008, pp. 842-846.

[4] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, “Image Encryption Using Advanced Hill Cipher Algorithm”, *ACEEE International Journal on Signal and Image Processing*, Vol 1, No. 1, Jan 2010, pp. 37-41.

[5] D. Chatterjee, J. Nath, S. Dasgupta and A. Nath, “ a new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm”, *2011 International Conference on Communication Systems and Neteorks Technologies”,* IEEE Computer Society, 2011, pp. 89-94.

[6] Somdip Dey, "SD-EI: A Cryptographic Technique To Encrypt Images", *Proceedings of The International Conference on Cyber Security*, CyberWarfare and Digital Forensic (CyberSec 2012), held at Kuala Lumpur, Malaysia, 2012, pp. 28-32.

[7] Somdip Dey, "SD-AEI: An advanced encryption technique for images", *IEEE Second International Conference on Digital Information Processing and Communications (lCDIPC)*, 2012, pp. 69-74.

[8] Somdip Dey, "An Image Encryption Method: SD-Advanced Image Encryption Standard: SDAIES*", International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 1(2), 2012, pp. 82-88.

[9] Prabal Banerjee and Ashok Nath, “Bit and Byte Level Generalized Modified Vernam Cipher Method with Feedback”, *International Journal of Computer Application (0975-8887),* Vol 64-No. 2, February 2013, pp. 9-15.

[10] Ankita P. Baheli, Lokesh Singh and Ashif Ullah Khan, “A Comparative Literature Survey On Various Image Encryption Standards”, *International Journal of Engineering Research & Technology (IJERT),* Vol. 2 Issue 4, April 2013, pp. 1444-1450.

[11] Behrouz A. Forouzan, *Cryptography and Network Security,* Tata McGraw Hill Companies, India, 2007.

[12] A. Uhl and A. Pommer, *Image and vedio Encryption,* Springer, 2005.

[13] Fathi E. Abd El-Samie, Hossam Eldin H. Ahmed, Ibrahim F. Elashry, Mai H. Shahieen, Osama S. Faragallah, El-Sayed M. El-Rabaie and Saleh A. Alshebeili, *Image Encryption: A communication Perspective,* CRS Press, 2013.

IJERT