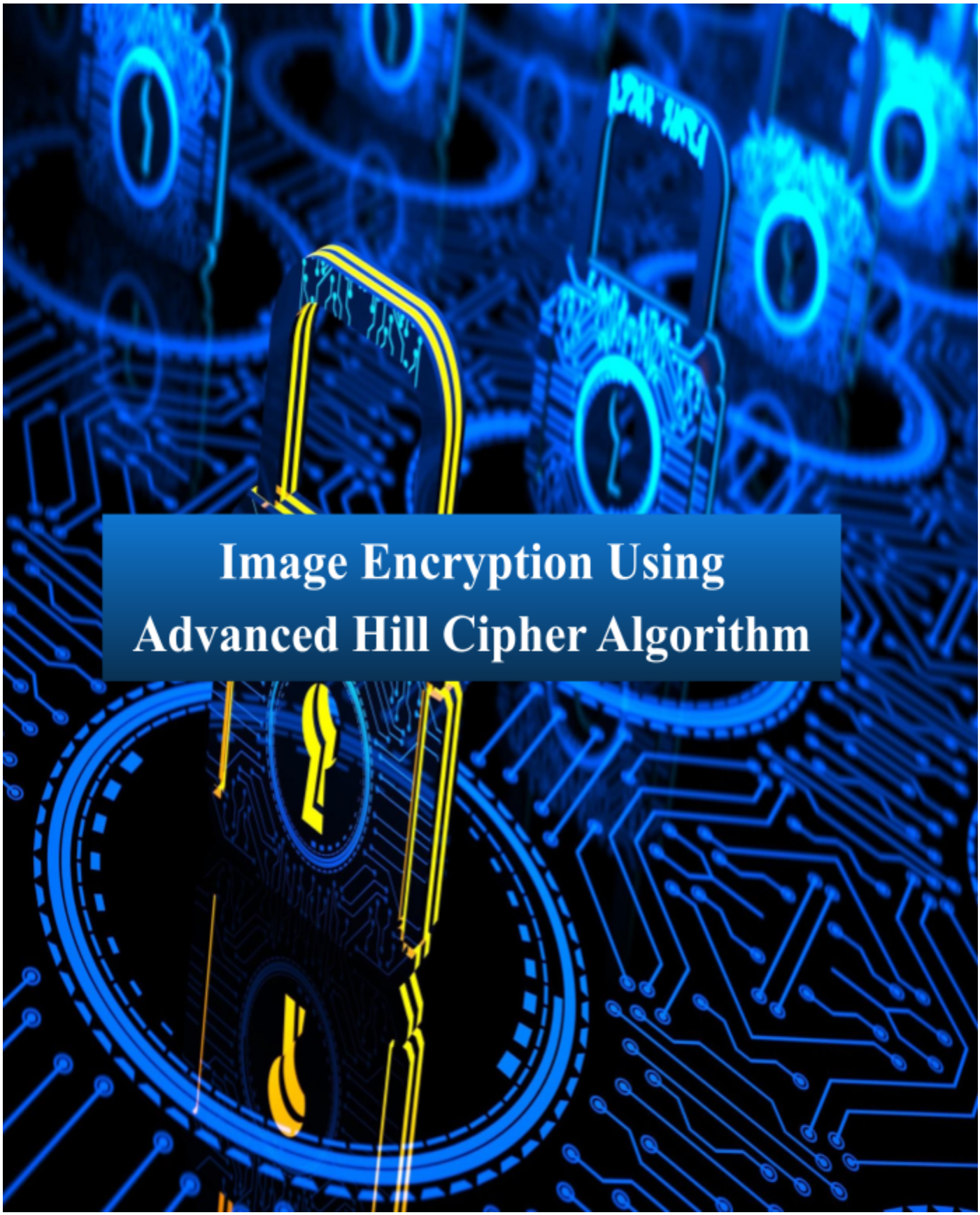
Image Encryption Using
Advanced Hill Cipher Algorithm

Image Encryption Using Advanced Hill Cipher Algorithm

Submitted to

Md. Iftekharul Amin

Associate Professor

Institute of Business Administration

University Of Dhaka

Submitted by

Muktadul Islam

BSSE 1215

Institute Of Information Technology (IIT)

University of Dhaka

Submission Date: March 15, 2023

Letter of Transmittal

15th March 2023,
Md. Iftekharul Amin,
Associate Professor,
Institute of Business Administration,
University of Dhaka.

Subject: Letter of transmittal for final report of BUS-503

Sir,
The report titled “Image Encryption Using Advanced Hill Cipher Algorithm” is attached herewith. The report presents the use of the Hill cipher algorithm, which is a widely used symmetric-key cryptographic technique, to secure digital images. The algorithm was modified to increase its security and efficiency for image encryption. The modified algorithm was tested on a set of sample images, and the results showed that it effectively encrypts images while maintaining their quality.

The report provides a detailed explanation of the encryption process and the modifications made to the Hill cipher algorithm. It also includes the implementation details and the results obtained from the experiments conducted

I will be obliged if you have a look at this report and approve its findings.

Sincerely,

Muktadul Islam
BSSE 1215

Acknowledgement

I would like to express my sincere gratitude and appreciation to our “Business Communication (BUS 503)” course teacher, Mr. Md. Iftekharul Amin, Associate Professor, Institute of Business Administration, University of Dhaka for giving me the opportunity to write this report on “Image Encryption Using Advanced Hill Cipher Algorithm”. I learned a lot about this field of study and it has been an eye-opener for me. This report has been prepared based on background studies from several websites and journals. I am thankful for all of the works cited. I am also thankful to my classmates who have discussed this report with me.

Table Of Contents

List of figures

Executive Summary

The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. Then if the key matrix is not invertible, then encrypted text cannot be decrypted. 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. In this paper a novel advanced Hill (AdvHill) 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 a homogeneous background. 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.

Chapter 1 : Introduction

1.1 Background Study

Image encryption using the advanced Hill cipher algorithm is a field of study in cryptography that focuses on securing digital images from unauthorized access. The Hill cipher is a classical encryption algorithm that was developed in 1929 by Lester S. Hill. It works by transforming the plaintext image into a ciphertext image through a series of matrix operations [4].

The advanced Hill cipher algorithm builds on the basic Hill cipher by adding an additional layer of security through the use of a secret key. The secret key is used to generate a random matrix that is used in the encryption process, making it more difficult for an attacker to decrypt the image without knowledge of the key. To encrypt an image using the Hill cipher, the image is first divided into blocks of equal size. Each block is then represented as a matrix of pixel values. The key matrix is then used to multiply each block matrix, and the result is taken modulo 256 to obtain the encrypted block matrix. The encrypted block matrices are then combined to form the encrypted image. The decryption process of the image is the same as encryption, except we use the inverse matrix of the key matrix as a key [5].

1.2 Origin of the report

The report was generated due to the increasing concern of image and video security. Though there are several encryption methods to protect those resources from third parties, still Advanced Hill Cipher will be one of the best of all which takes low runtime to encryption or decryption [5].

1.3 Objectives

Broad Objective: The broad objective of this report is to provide a method for image encryption which will take low rantime & will be more secure.

Specific Objectives: The specific objectives of Image Encryption Using Advanced Hill Cipher Algorithm could vary depending on the purpose and scope of the research or project. However, here are some possible objectives that could be pursued:

1. To develop a new or improved image encryption algorithm based on the advanced Hill cipher that provides stronger security and faster encryption and decryption times [2].
2. 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, if the key matrix is not invertible.
3. Reduce the computational complexity by avoiding the process of finding the inverse of the matrix at the time of decryption, as we use the Involutory key matrix for encryption.
4. To propose and implement improvements to the advanced Hill cipher algorithm to address any weaknesses or vulnerabilities identified during the testing and analysis.
5. To test the robustness of the advanced Hill cipher algorithm against various types of attacks, including brute-force attacks, statistical attacks, and chosen-plaintext attacks.

1.4 Scope of the report

The scope of a report on Image Encryption Using Advanced Hill Cipher Algorithm can vary depending on the purpose. However, here are some possible areas that the report could cover:

- Overview of image encryption techniques: The report could provide an introduction to the basic principles and techniques of image encryption
- Hill cipher algorithm: The report could describe the fundamentals of the Hill cipher algorithm, including matrix operations, modular arithmetic, and key management.
- Advanced Hill cipher algorithm: The report could explain the enhancements to the Hill cipher algorithm to make it more secure [3].
- Implementation details: The report could provide technical details on how to implement the advanced Hill cipher algorithm.
- Security analysis: The report could evaluate the security of the advanced Hill cipher algorithm against various attacks, including brute-force attacks, statistical attacks, and chosen-plaintext attacks.

1.5 Limitations

The primary limitations of this report are if the matrix size is increased then the computation will be also increased and if the matrix size is too small then the key can be identified by brute force attack. Moreover This algorithm works well for all types of gray scale as well as color images except for the images with background of the same gray level or same color [5].

1.6 Methodology

The study is conducted through secondary analysis based on personal experience. The data provided has been collected from research papers and websites.

1.7 Chapter Summary

This paper suggests an efficient method of encryption of images. Proposed AdvHill algorithm is more secure to brute force attacks as compared to the original Hill cipher algorithm. A Brute Force Attack requires $\mathbf{2}^{7+8*(n/2)*(n/2)}$ number of key generations; where n is the order of the key matrix. AdvHill is a fast encryption technique which can provide satisfactory results against the normal hill cipher technique. The proposed scheme is resistant against known plaintext attacks [5].

Chapter 2 : Hill Cipher & Modular Arithmetic

2.1 Hill Cipher Encryption & Decryption

It was developed by the mathematician Lester Hill. The core of Hill cipher is matrix manipulations. For encryption, the algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In the Hill cipher, each character is assigned a numerical value a=0, b=1, ... z=25 [2,3]. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equation. For m=3 , the system can be described as follows:

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \mod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \mod 26 \quad \text{.....(1)}$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \mod 26$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad \text{.....(2)}$$

or simply we can write as $C = KP$, where C and P are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3x3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires using the inverse of the matrix K . The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the ciphertext, and then the plaintext is recovered. In general term we can write as follows [4]:

For encryption:

$C = E_k(P) = K_p$ .....(3)

For decryption:

$$P = D_k(C) = K^{-1}C = K^{-1}K_P \quad \text{.....(4)}$$

If the block length is m, there are m^{26} different m letters blocks possible, each of them can be regarded as a letter in a m^{26} -letter alphabet. Hill's method amounts to a monoalphabetic substitution on this alphabet.

2.2 Modular Arithmetic Operation

The arithmetic operations presented here are addition, subtraction, unary operation, multiplication and division. Based on this, the Involutory matrix for Hill cipher algorithm is generated. The congruence modulo operator has the following properties [3]:

1. $a \equiv b \mod p$ if $n \mid (a-b)$
2. $(a \mod p) = (b \mod p) \Rightarrow a \equiv b \mod p$
3. $a \equiv b \mod p \Rightarrow b \equiv a \mod p$
4. $a \equiv b \mod p$ and $b \equiv a \mod p \Rightarrow a \equiv c \mod p$

Let $Z_p = [0,1,.....,p-a]$ the set of residues modulo p . If modular arithmetic is performed within this set Z_p ,the following equations present the arithmetic operations [3]:

Addition:

$(a+b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$

Negation:

$-a \bmod p = p - (a \bmod p)$

Subtraction:

$(a-b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$

Multiplication:

$(a*b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$

Division:

$(a+b) \bmod p = c$ when $a=(b*c) \bmod p$

The following exhibits the properties of modular arithmetic:

Commutative Law:

$$(\omega + x) \bmod p = (x + \omega) \bmod p$$

$$(\omega * x) \bmod p = (x * \omega) \bmod p$$

Associative law:

$$[(\omega + x) + y] \bmod p = [\omega + (x + y)] \bmod p$$

Distribution Law:

$$[\omega * (x + y)] \bmod p = [\{(\omega * x) \bmod p\} * \{(\omega * y) \bmod p\}] \bmod p$$

Identities:

$$(0 + a) \bmod p = a \bmod p$$

$$\text{and } (1 * a) \bmod p = a \bmod p$$

Inverses:

For each $x \in Z_p$, $\exists y$ such that

$$(x + y) \bmod p = 0 \text{ then } y = -x$$

For each $x \in Z_p$ $\exists y$ such that $(x * y) \bmod p = 1$

2.3 Generation of Involutory Key Matrix

The proposed Adv Hill algorithm uses an involutory key matrix for encryption technique. The various proposed methods can be found in literature [1]. One of
The methods are explained below.

A is called an involutory matrix if $A = A^{-1}$ [6]. The analysis presented here for generation of involutory key matrix is valid for matrices of +ve integers that are the residues of modulo arithmetic of a number. This algorithm can generate involutory matrices of order n×n where n is even [3].

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{bmatrix}$ be an nxn involutory matrix

partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ where n is even and A_{11} , A_{12} , A_{21} & A_{22} are matrix order n/2 X n/2.

So, $A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$

Algorithm:

1. Select any arbitrary (n/2 * n/2) matrix A_{22}.
2. Obtain $A_{11} = - A_{22}$
3. Take $A_{12} = k(I - A_{11})$ or $k(I+A_{11})$ where k is a scalar constant.
4. Then $A_{21} = (I - A_{11})/k$ or $(I+A_{11})/k$
5. Form the matrix completely.

Chapter 3 : Image Encryption Using AdvHill Technique

As we note that Hill cipher can be adopted to encrypt grayscale and color images, proposed AdvHill algorithm can also be used for grayscale and color images. For grayscale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted color image.The algorithm is given below and the block diagram for the encryption process is shown in Figure 1.

3.1 Algorithm of AdvHill

Step-1: An involutory key matrix of dimensions m×m is constructed.

Step-2:The plain image is divided into m×m symmetric blocks.

Step-3: The ith pixels of each block are brought together to form a temporary block.

a. Hill cipher technique is applied onto the temporary block.

b. The resultant matrix is transposed and the Hill cipher is again applied to this matrix.

Step-4:The final matrix obtained is placed in the ith block of the encrypted image.

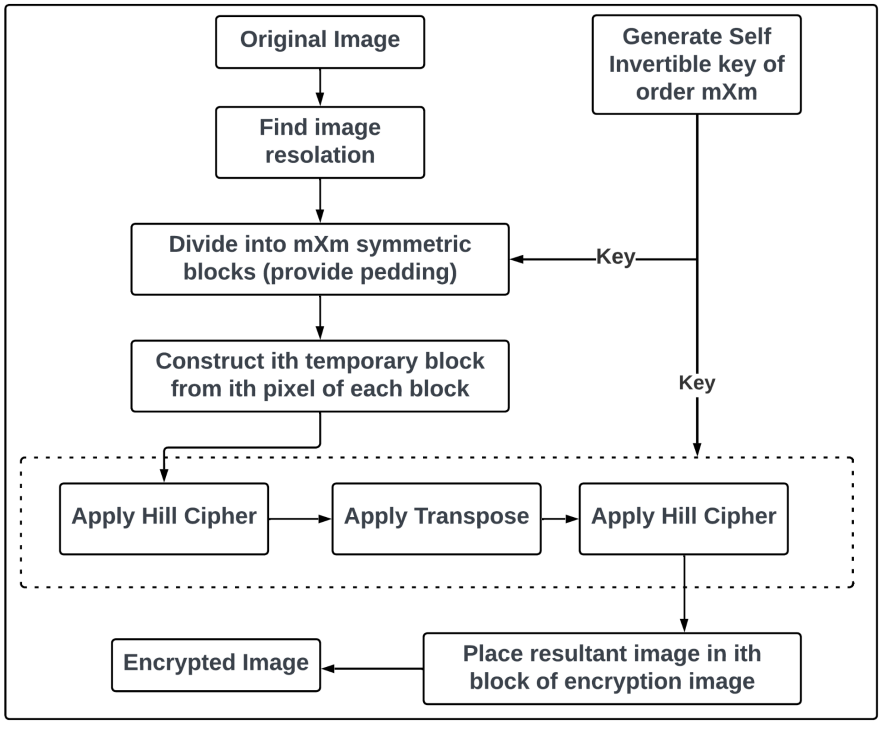

Figure. 1. The block diagram for proposed AdvHill algorithm.

3.2 Some Encryption Examples:

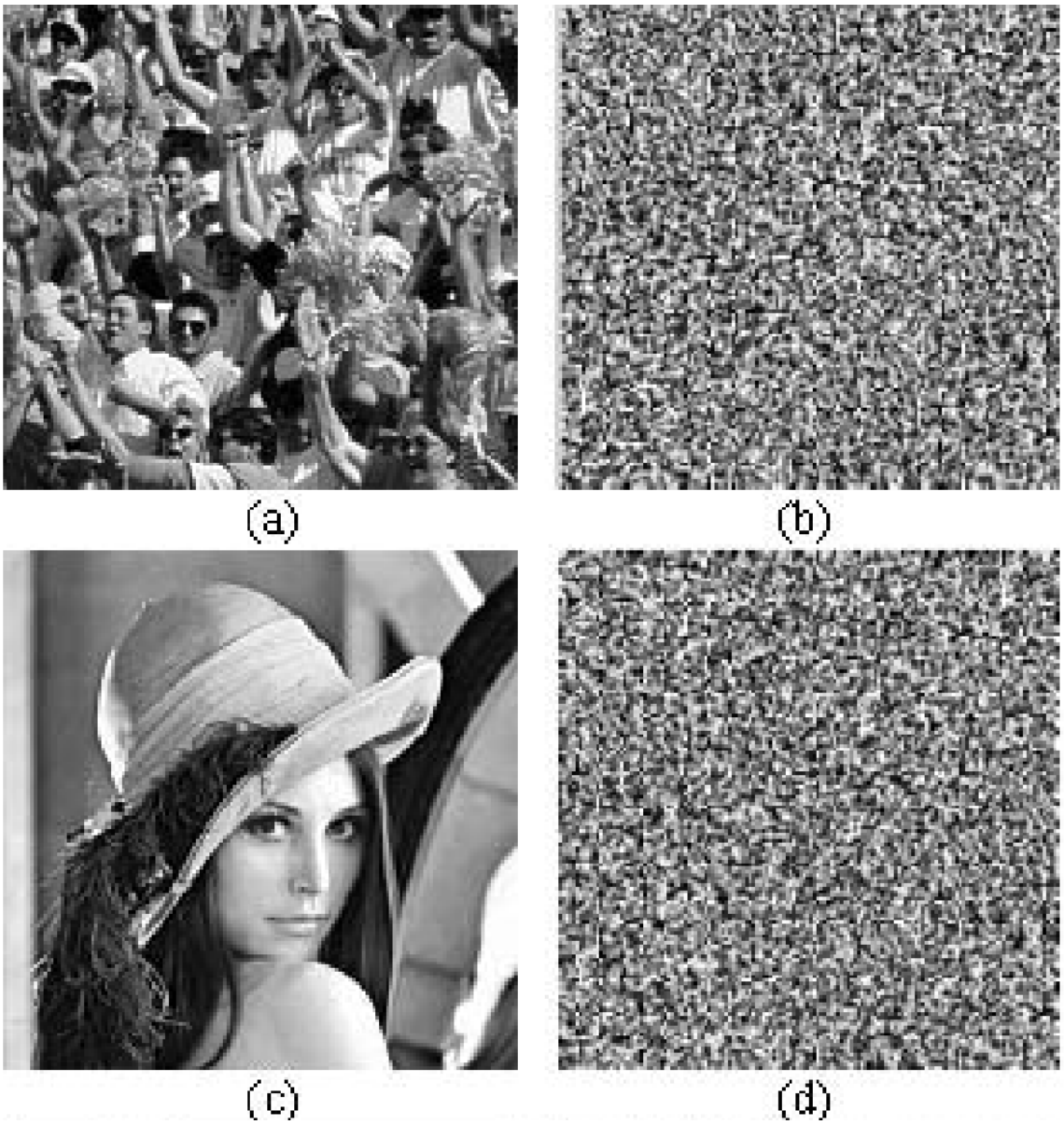

Figure. 2. Original images (a, c) and corresponding encrypted images (b, d) by original Hill Cipher Algorithm

Chapter 3 : Ending Summary

In this paper,I have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption [1]. The objective of this paper 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, if the key matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use the Involutory key matrix for encryption.

References

1. Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S. K. (2007). Novel methods of generating self-invertible matrix for hill cipher algorithm.
2. Menezes, A. J., P.C. Van Oorschot, S.A. Van Stone. 1996. Handbook of Applied Cryptography. CRC press.
3. Stallings, W. Cryptography and Network Security.2005. 4th edition, Prentice Hall.
4. https://en.wikipedia.org/wiki/Hill_cipher (12-03-2023).
5. Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. (2009). Image encryption using advanced hill cipher algorithm. *International Journal of Recent Trends in Engineering*, *1*(1), 663-667.
6. https://en.wikipedia.org/wiki/Involutory_matrix (12-03-23)