Image Encryption Using Orthogonal Hill Cipher Algorithm

Soraj Singh Kandari
MIT2020066

Abstract

Hill Cipher is a practical algorithm that only requires a basic knowledge of arrays which makes it very useful. But, to decode the encoded information, the main matrix must have an inverse (the main matrix must be invertible) otherwise it is impossible to decode the presented information. The main goal of our research paper is to present an unconventional and improved version of Hill Cipher which will make encoding and deciphering the image easier. This paper diverged from the conventional method by using an orthogonal matrix (where the matrix transpose is equal to its inverse) as our master matrix. This method is faster and easier as finding the transposition of a matrix is much easier than finding the inverse of a given matrix, thus, facilitating the faster implementation process. To further break down the process into a simpler one, we have added some other restrictions.

Keywords: Orthogonal Matrix, Hill Cipher, Invertibility, Encryption.

1. Introduction

In this era, there have been many breakthroughs in digital communication and modern means of digital transfer of information is constantly replacing the conventional means thus increasing the emphasis on security and safe transfer of information, thus making cryptography crucial. Conventional Encryption can also be called as symmetric encryption or single key encryption. In fact, it was a type of encryption that was used before the development of public-key encryption. Conventional encryption can, in turn, be classified into the categories of classical and modern techniques. The security of the information has always been an important problem but its importance has been increasing with each passing day. Cryptographic algorithms can be divided into Symmetric and Asymmetric key algorithms. In symmetric algorithms, the receiver and the sender share a common key.

Asymmetric algorithms deal with a pair of keys (both public, private) which happen to be related mathematically. The primary polygraph cipher having specific advantages in data encryption is the Hill Cipher. These days, information security is beginning to play a major role in transmission of data as well as in its storage. Images are used in a wide range of processes which increases the importance of protection of image data from unauthorized access. The field of information concealment, image hiding or encrypting methods and algorithms employs image encryption to fulfil an important role in their processes.

Cryptography uses intricate mathematical calculations and logic for its process of encryption. Cryptography can also be thought of as an art, it restores people's faith in the electronic world by helping them to remain safe. People can carry on their online processes without the fear of their data being stolen or getting hacked and with the knowledge that their privacy is secure. The recent times have seen an upsurge of online transactions by people which calls for more encrypted and safer means and cryptography serves that purpose. The world today thrives on electronic transactions online by using online banking, payment sources like Paytm, PayPal, etc., This increase in using the online resources has resulted in increased dependence on cryptography and authentication. The transfer of information, while making sure that nobody understands it, is the purpose of cryptography. Here, the attempt is to make sure that when the enemy receives the message, it is in encrypted format so that he doesn't understand it. Confidentiality is the often considered as the main premise in the field of information shielding. Secure communication is one of the direct applications of cryptography. [1]

The central management problem keeps crippling the secure communication from becoming common and thus reducing their effectiveness. The production of public-key cryptography creates a large and an effective group of people who can communicate securely with one another even if they had never communicated before.

In visual cryptography, an attacker cannot judge or find relevant information but can alter it without knowing the repositories of data which can create problems in decryption. There may be some bit flipping or bit alterations during communication also. To overcome this problem people have proposed many ways to detect the tampering [2]. The hill cipher is a classical symmetric cipher based on matrix manipulation. It has several advantages including its resistance to frequency analysis and its simplicity due to the fact that it uses matrix multiplication and inversion for encryption and decryption. However, it succumbs to the branded plaintext attack [3-4]. Substitution Cipher is a technique that transforms a given text into random or stochastic data bits. There are many cryptographic substitution algorithms like Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Polyalphabetic Ciphers, One Time Pad, etc. [5-6]

In this paper, we have used an improved version Hill Cipher method which uses an orthogonal matrix as its key matrix. The

primary aim of this paper has overcome the problems that arise when using a random matrix as a key matrix because if the key matrix is not invertible, then the message cannot be decrypted. To further simplify the calculations that are involved in calculating the inverse of a key matrix, we have use an orthogonal matrix since finding a transpose is much simpler than finding the inverse. We have also added a few more constraints to make the computation simpler.

2. Generation of Orthogonal Key Matrix

For the encryption technique, the Orthogonal Hill (OTH) Cipher algorithm that has proposed uses orthogonal matrix as the key matrix. The procedure that has adopted to generate the orthogonal matrix is elaborated below

The matrix A is said to be orthogonal matrix if $A A^T = I$ or transpose of A is equal to its inverse. The structure that has been followed for the generation of orthogonal key matrix is valid for matrix whose elements are real number. The algorithm that we have proposed can be used for square matrices with order "n" provided that "n" is even. We have illustrated it by taking the example of a 4x4 matrix.

$$\text{Let } A = \begin{bmatrix} a & b & c & d \\ E & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \quad (1)$$

$$a_{11} = \begin{bmatrix} a & b \\ e & f \end{bmatrix}, a_{12} = \begin{bmatrix} c & d \\ g & h \end{bmatrix}, \quad (2)$$

$$a_{21} = \begin{bmatrix} i & j \\ m & n \end{bmatrix}, a_{22} = \begin{bmatrix} k & l \\ o & p \end{bmatrix} \quad (3)$$

$$\text{Therefore, } A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad (4)$$

$$\text{Which implies } A^{-1} = \begin{bmatrix} a_{11}^T & a_{21}^T \\ a_{12} & a_{22} \end{bmatrix} \quad (5)$$

A is an orthogonal matrix which implies $A A^{-1} = I$
Or $A^{-1} = A^{-1}$

Consequently,

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} * \begin{bmatrix} a_{11}^T & a_{21}^T \\ a_{12}^T & a_{22}^T \end{bmatrix} = I_{4x4}$$

Therefore,

$$a_{11} a_{11}^T + a_{12} a_{12}^T = I$$

$$a_{11} a_{21}^T + a_{12} a_{22}^T = 0$$

$$a_{21} a_{11}^T + a_{22} a_{12}^T = 0$$

$$a_{21} a_{21}^T + a_{21} a_{22}^T = I$$

These are the conditions which are arrived at using the property of the orthogonal matrices but this isn't simple enough to carry out analysis. That is why some more constraints have been added to simplify the process.

Constraint: $a_{11} = a_{12}$

Which results in $a_{22} = -a_{21}$

$$\text{Now } A = \begin{bmatrix} a_{11} & a_{11} \\ -\alpha_{22} & a_{22} \end{bmatrix} \quad (11)$$

$$\text{And, } A A^T = I \quad (12)$$

$$\begin{bmatrix} 2 * a_{11} * a_{11}^T & 0 \\ 0 & 2 * a_{22} * a_{22}^T \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (13)$$

Equating it,

$2\, a_{11}\, a_{11}^T = I = 2\, a_{22}\, a_{22}^T$

$$a_{11} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{(say)}$$

Simplifying it, we get the expressions for a, b, c and d

$$a = \frac{2 * b * c * d}{2 * d^2 - 1} \quad (14)$$

$$b = \frac{2 * a * d * c}{2 * c^2 - 1} \quad (15)$$

$$c = \frac{2 * a * d * b}{2 * b^2 - 1} \quad (16)$$

$$d = \frac{2 * a * b * c}{2 * a^2 - 1} \quad (17)$$

By substituting values for a, b, c, d which satisfy the above equation we are able to generate a_{11} and similarly a_{22}.

Hence by following this procedure, the key matrix can be generated, thus eliminating the complexity involved in the regular Hill Cipher method.

Algorithm:

1. Select any arbitrary 2x2 matrix a_{11}(It will be one of the blocks of the main matrix)
2. Generate the second block which is the same as that of the first block($a_{11} = a_{12}$)
3. Select another arbitrary matrix (this will be the third block), a_{21}
4. Find the final block by using $a_{22} = -a_{21}$
5. By combining all the blocks, the required key matrix is obtained.

3. Image Encryption Using OTH Cipher

We know that the original Hill Cipher method can be used for encrypting both grey scale and color images, the procedure that we have proposed can also be adopted for grey scale and color images and we have also verified the results using python. For the color images, we can convert the whole image into a three dimensional matrix by splitting the image into three different colors namely red, blue and green. We use the key matrix that we have generated earlier and we encrypt the given matrix. The Encryption Algorithm:

1. Import the image onto python

2. Assign a variable to it (say b)
3. b is a Three Dimensional Array, whose constituents hold the RGB (Red Green Blue) value of the Pixels of the image.
4. Split b into its 3 different matrices say b1, b2 and b3,using:
   b1=b(:,:,1);
   b2=b(:,:,2);
   b3=b(:,:,3);

5. It is noteworthy to remember that the values inside these matrices are in "uint8" format. That is, they range from 0-255 only and are not subject to any matrix operation.
6. Convert them to "double" format matrices: bb1=double(b1); bb2=double(b2); bb3=double(b3);

7. Now apply the OTH cipher key to these matrices. The K obtained here is orthogonal and obtained from the above mentioned algorithmbbe1=K*bb1; bbe2=K*bb2; bbe3=K*bb3;

8. The new matrices obtained are encrypted and can now be inserted back into the Pixel format, after converting them back to uint8 format.
   To convert them back to
   uint8: bbeu1= uint8 (bbe1);
   bbeu2= uint8 (bbe2); bbeu3=
   uint8 (bbe3);

9. These are the new RGB values of the encrypted image.
10. To view the image, insert them back into the Array form:
    A=bbeu1 (say)
    A(:,:,2)=bbeu2;
    A(:,:,3)=bbeu3;

11. To view the encrypted
    image: Image(A)

12. Thus the encrypted image is obtained.
    In order to get back the original image, the same procedure is to be followed, only change being that K is replaced by KI = inv(K) = K^{-1}

4. Simulation

Generation of the key matrix using Gram-Schmidt orthogonalisa-tion:
We use the projection formula as:

$$proj_{u}(v) = \frac{\langle v, u \rangle}{\langle u, u \rangle} u \qquad (18)$$

Where $\langle v, u \rangle$ is the inner product of vectors v and u. Now, we take set of basis elements n, n being the dimension of pixels we want to encrypt as nxn matrix. Let this set of basis elements be $\{v_1, \vec{v_2}, \vec{v_3}, \vec{v_4}, \ldots\ldots, \vec{v_n}\}$. Then the set of orthonormal basis is calculated as $\{\vec{e_1}, \vec{e_2}, \vec{e_3}, e_4, \ldots\ldots, e_n\}$ as:

$$\vec{u_1} = \vec{v_1} \; ; \vec{e_1} = \frac{\vec{u_1}}{\left\| \vec{u_1} \right\|} \qquad (19)$$

$$\vec{u_2} = \vec{v_2} - proj_{u_1}(\vec{v_2}) \; ; \vec{e_2} = \frac{\vec{u_2}}{\left\| u_2 \right\|} \qquad (20)$$

$$\vec{u_3} = \vec{v_3} - proj_{u_1}(\vec{v_3}) - proj_{u_2}(\vec{v_3}) \; \vec{e_3} = \frac{\vec{u_3}}{\left\| u_3 \right\|} \qquad (21)$$

So on till,

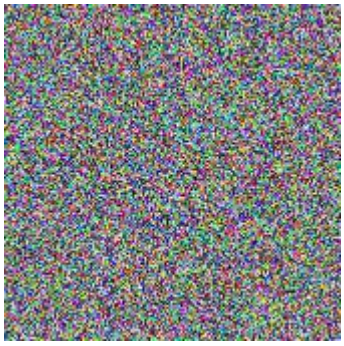
$$\vec{u_n} = \vec{v} - \sum_{j=1}^{n-1} proj_{u_j}(\vec{v_j}) \; ; \vec{e_n} = \frac{\vec{u_n}}{\left\| \vec{u_n} \right\|} \qquad (22)$$

Now these orthonormal basis vectors $\{\vec{e_1}, \vec{e_2}, \vec{e_3}, e_4, \ldots\ldots, e_n\}$ are then placed in an n × n matrix and this matrix is then used as encryption matrix for encrypting the image information by distorting its pixels by multiplying the pixel matrix with this matrix. While coding in C programming language we are working with two matrices, "matA" and "matQ1". First the code asks for dimension of the matrix and then matA matrix takes the input values from the user as basis elements $\{\vec{v_1}, \vec{v_2}, \vec{v_3}, v_4, \ldots\ldots, \vec{v_n}\}$ using „inputMatrix" function and then proj and normalize functions calculate the projection and normalized values respectively and finally these normalized values are put in n × n matrix to get the orthogonal matrix "matQ1".

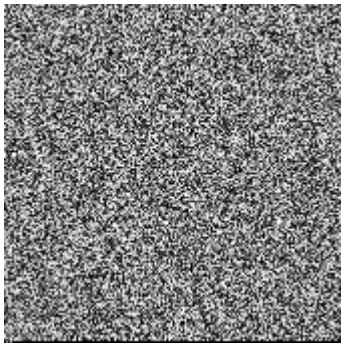
5. Results

Before encryption, the original images: Figures:

fig(a):original image



fig(b):encrypted image



fig(c):key value

fig(d):final image

Clearly, the encryption algorithm has encrypted the images be-yond recognition or beyond any resemblance to the original image. Concretely, the matrix obtained by the above mentioned method of generation orthogonal matrix has been used in the OTH cipher to encrypt the images.

Fig.6(a) and Fig.6(b) illustrates how the algorithm has changed the pixel values of the images resulting in them appearing altered and making them unable to represent any visual meaning.

An important observation here is that the encryption algorithm is only as effective as more abstract or more random the orthogonal matrix may appear.

6. Conclusion

This paper has delineated on how to properly encrypt images by using OTH Cipher technique. The proposed encryption mecha-nism considerably reduces the problems faced while encrypting images using original Hill Cipher Technique. In this paper, a unique algorithm has been developed for generation of key matrix and it also elaborates on generation of key matrix using Gram-Schmidt orthogonalization by means of the software code that has been written. Further, the images that have been encrypted sub-stantiate the algorithms that have been mentioned earlier.

References

[1] Acharya, Bibhudendra, et al. "Image encryption using advanced hill cipher algorithm." International Journal of Recent Trends in Engi-neering 1.1 (2009).

[2] Sastry, V. U. K., and N. Ravi Shankar. "Modified Hill Cipher with Interlacing and Iteration 1." (2007).

[3] Acharya, B., Jena, D., Patra, S. K., & Panda, G. (2009, January). Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System. In Advanced Computer Control, 2009. ICACC'09. International Conference on (pp. 410-414). IEEE.

[4] Hill, Lester S. "Concerning certain linear transformation apparatus of cryptography." The American Mathematical Monthly 38.3 (1931): 135-154.

[5] Hill, Lester S. "Cryptography in an algebraic alphabet." The Amer-ican Mathematical Monthly 36.6 (1929): 306-312.

[6] Ganesan, K., and R. Anandan. "Version Control using Crypto-graphic Access Control." In Information Technology, 2006. ICIT'06. 9th International Conference on, pp. 192-196. IEEE, 2006.

[7] Sastry, V. Umakanta, N. Ravi Shankar, and S. Durga Bhavani. "A Modified Hill Cipher Involving Interweaving and Iteration." IJ Network Security 10, no. 3 (2010): 210-215.

[8] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[9] Hori, G. (2011, May). Natural gradient approach in orthogonal ma-trix optimization using cayley transform. In Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on (pp. 2116-2119). IEEE.

[10] Sastry, V. U. K., Murthy, D. S. R., & Bhavani, S. D. (2010). A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side. International Journal of Computer Theory and Engineering, 2(5), 805.

[11] Ismail, I. A., Mohammed Amin, and Hossam Diab. "How to repair the Hill cipher." Journal of Zhejiang University-Science A 7.12 (2006): 2022-2030.

[12] Khalaf, A. A., El-karim, M. S. A., & Hamed, H. F. (2015, July). Proposed triple hill cipher algorithm for increasing the security lev-el of encrypted binary data and its implementation using FPGA. In Advanced Communication Technology (ICACT), 2015 17th In-ternational Conference on (pp. 454-459). IEEE.

[13] Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2007.

[14] Stallings, William, and Mohit P. Tahiliani. Cryptography and net-work security: principles and practice. Vol. 6. London: Pearson, 2014.

[15] Feistel, Horst. "Cryptography and computer privacy." Scientific american 228.5 (1973): 15-23.