A Comparative Performance Analysis of an Image Encryption Technique using Extended Hill Cipher

Yashpalsingh Rajput
Research Scholar,
Government College of Engineering, Aurangabad

A K. Gulve
Associate Professor,
Government College of Engineering, Aurangabad

ABSTRACT
The security of digital images is concentrating much attention nowadays, and many image encryption algorithms have been proposed by different authors and researchers. In [1], an improvement over an algorithm for image encryption was proposed. This paper explains the result and analysis of the proposed algorithm in [1]. The paper also discusses about the analysis based on some performance factors.

The paper is organized into different sections as follows. Section 1 contains a basic introduction to the image cryptography and hill cipher. Section 2 contains description of the proposed system. Section 3 contains performance analysis of the proposed system. Section 4 contains the conclusion of the work.

General Terms
Image Security

Keywords
Cryptography, Cryptanalysis, Image, Key, Hill Cipher

1. INTRODUCTION
Nowadays when lots of important and confidential information is stored on servers and transmitted over the web. Digital image is also an important part of sensitive or private information.

The security and safety of online information should be guaranteed. To improve data security generally data encryption and decryption techniques called cryptography is used. The process of converting data from readable form to non-readable form is called as encryption. In decryption, reverse of encryption is done i.e. data is converted from non-readable form to readable form. If encryption is done using a key then decryption will also require some key. When same key is used for encryption and decryption process, it is called as symmetric key cryptography otherwise it is called as asymmetric key cryptography. Image security can be ensured by applying encryption to the digital images. Image encryption techniques convert original digital image to encrypted image that is difficult to understand and to keep the image confidential between users. It is important that without decryption key no one can access the content. Image encryption has applications in online communication, multimedia systems, medical field, military communication; etc. However, the traditional cryptosystems used for text encryption can also be used for image encryption, but it is not suitable for some reasons. There are so many algorithms available to protect image from unauthorized access. [1][3]

The general image encryption process flow is shown in figure 1. As shown in figure 1, a human readable image is converted to a form which is not readable to a human being, using an image encryption algorithm. To get original readable image, the image must be decrypted using some key.

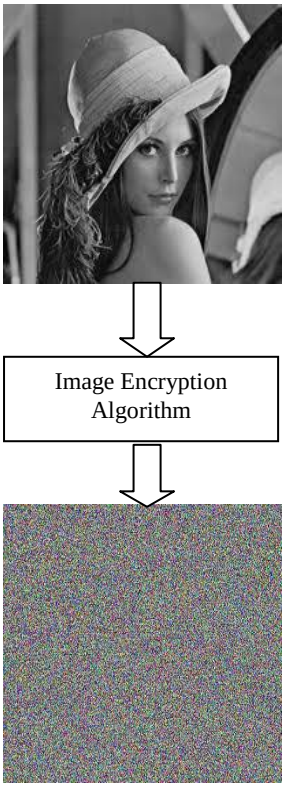

Fig. 1: Image Encryption

1.1 Hill Cipher
The Hill cipher algorithm is one of the known symmetric key algorithms in the field of cryptography proposed by Lester Hill in 1929. Hill cipher requires a matrix based polygraphic system. [6][7]
For example {abcdef…} = ab cd ef… or abc def… and so on.
For encryption, algorithm takes *m* successive plaintext characters and instead of that substitutes *m* cipher characters. In Hill cipher, each character is assigned a numerical value like $a = 0$, $b = 1$, …, $z = 25$. The substitution of ciphertext characters in the place of plaintext characters leads to *m* linear equation. The system can be described as follows:

$$C = KP$$

where C and P are column vectors of length n, representing the plaintext and ciphertext, respectively and K is a n x n matrix, which acts as key for encryption. All operations performed with modulus of 26.

In general the process of encryption using hill cipher can be written as follows:

Encryption Process:

$$C= E_k(P) = Kp$$

Decryption Process:

$$P = D_k(C) = K^{-1}C = K^{-1}Kp = P$$

In hill cipher, key is an invertible m x m matrix, where m is block length. Decryption process uses inverse of matrix K. If the block length considered as m, there are 26^m different m characters blocks are possible.

2. PROPOSED SYSTEM

As shown the diagram below, the proposed system [1] is divided into the following 3 main phases:

The flow for proposed system is shown in Figure 2.

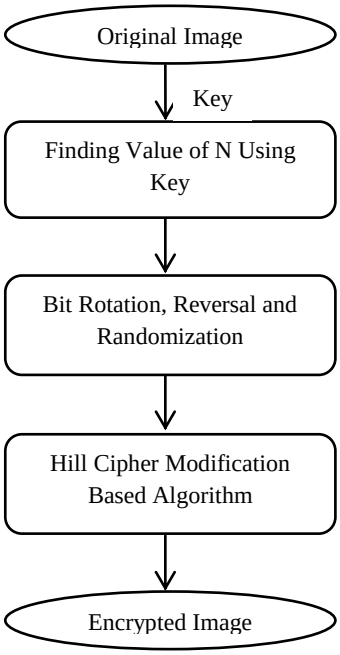

Fig. 2: Flow Diagram for Proposed System

2.1 PHASE-1: Image Blocks Generation

In this step, a plain image and a key is provided as input. The key provided may contains alphanumeric characters. In this phase, the image is divided into the n numbers of horizontal row-wise blocks and XOR is performed among these blocks.

After dividing the images into numbers of horizontal blocks, and keeping first horizontal block as it is, and all other horizontal blocks are replaced with the result of XOR of the corresponding horizontal block with first horizontal block. i.e. each horizontal block is XORed with first horizontal block. Here first horizontal block acts as a key block for XOR operation. Original image blocks can be recovered by XORing the result blocks again with first horizontal block i.e. key block.

2.2 PHASE-2: Bits Rotation, Reversal and Randomization

In this phase, value of each pixel of the image obtained as the result of PHASE-1 is converted into equivalent 8-bit binary number. Now length of key is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the length of key.

After bit rotation and reversal of bits, randomization of bits is done. For randomization purpose, here a sequence of bit rotation operations in anticlockwise direction is applied i.e. left rotation, down rotation, right rotation and up rotation operations on the image bits.

2.3 PHASE-3: The Extended Hill Cipher Technique for Image Encryption

Hill Cipher does not hide all features of the images containing large areas of single color. Recent research and development efforts have been done to enhance the security of Hill Cipher. To overcome the disadvantage of original hill cipher with respect to the images having large areas of single color, various improvements on original hill cipher are done.
The proposed work uses extended hill cipher technique for image encryption which is presented by Somdip Dey in [2].

3. PERFORMANCE ANALYSIS

The performance analysis of the proposed system is done with the help of some experimental testing. Some factors are considered for analyzing the performance of the proposed method. By comparing these factors with the other encryption schemes analysis is done.

3.1 PERFORMANCE FACTORS

To define a set of factors based on which evaluation can be done and the proposed method [1] can be compared with the other image encryption schemes. Some factors are listed below.

Tunability: It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications [4][5]. In this paper, tunability has one of the values ‘yes’ or ‘no.

Visual Degradation: This factor estimates the perceptual distortion of the digital image with respect to the plain digital image. In some applications, it could be desirable to achieve enough visual degradation, so that an attacker would still understand the content but prefer to pay to access the unencrypted content. However, for sensitive data, high visual degradation could be desirable to completely disguise the visual content [4][5]. High is the content distortion, it is very difficult to retrieve original content and hence less is the possibility of successful attack. Visual degradation has one of the values like high, medium, low.

Compression Friendliness: An encryption algorithm is considered compression friendly if it has zero or very little impact on data compression efficiency. Some encryption algorithms impact data compressibility by introducing additional data which is necessary for decryption [4][5]. An algorithm is said to be compression friendly, if the size of data after encryption is same as that of before encryption. Compression friendliness value can be ‘yes’ or ‘no’.

Format Compliance: The encrypted bit stream should be compliant with the compressor. Standard decoder should be able to decode the encrypted bit stream without decryption. [4][5]

Computational Speed: Sometimes it is important that the encryption and decryption methods are efficient in terms of time i.e. fast enough to meet real-time requirements. [4][5]

Security: It defines, to what extent the encryption algorithm is secure against different cryptographic attacks such as brute force attack, statistical attacks and other plaintext-cipher text attacks. For multimedia application, it is important that the encryption algorithm should provide enough cryptographic security. [4][5] Cryptographic security can be measured in three levels: low, medium and high.

Key Length Value: In cryptographic techniques, key is the most important factor. The security of the algorithm is mostly depends on the key value. According to Kerckhoffs's principle, "A cryptographic system should be secure even if everything about the system is public knowledge, except the key."[14]

3.2 Comparison of Various Image Encryption Schemes

This section presents performance analysis and comparison among various image encryption schemes. The figure 3 shows a png image, which is provided as input for the proposed technique. Its histogram is also shown before it undergone the process. The string 'cameraman!@#' is provided as key, which gives us number 3 after PHASE 1 of the algorithm. The proposed method is applied. The figure 4 shows same image with its histogram but after decryption. Notice that the histogram difference in both the images shown in figure 3 and figure 4 is zero. It means there is not any kind of loss of data i.e. no visual degradation, etc.

On the basis of factors like tunability, visual degradation, cryptographic security, compression friendliness, etc. the proposed system is compared with the other image encryption techniques. The performance analysis and comparison among various image encryption methods with respect to above factors is shown in Table 1. [4]
The symbol used is: "?" for unspecified criteria.

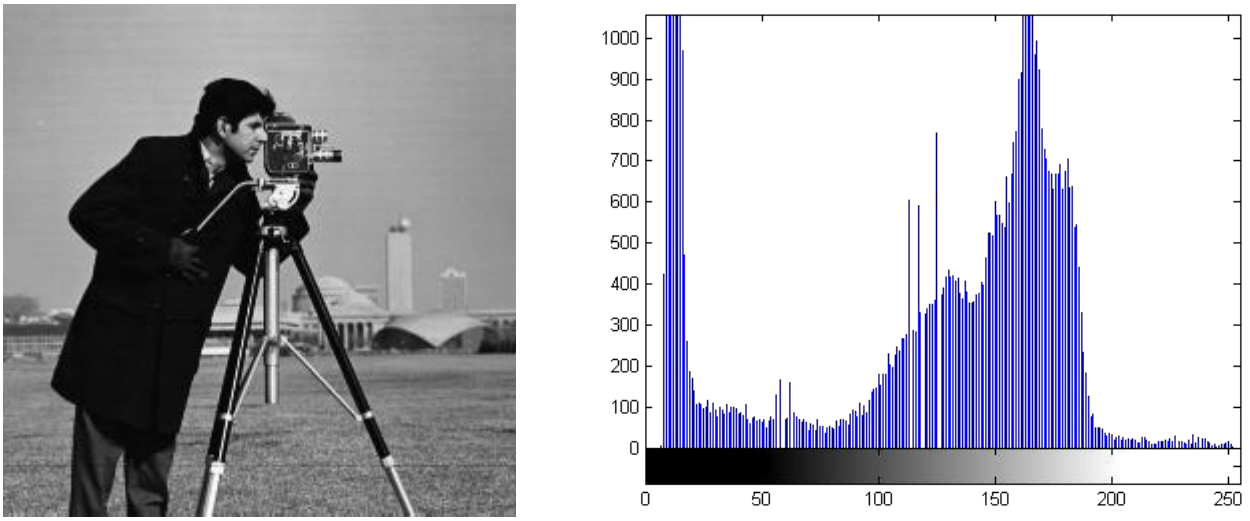

Fig. 3: Image and its histogram before encryption (Cameraman.png)

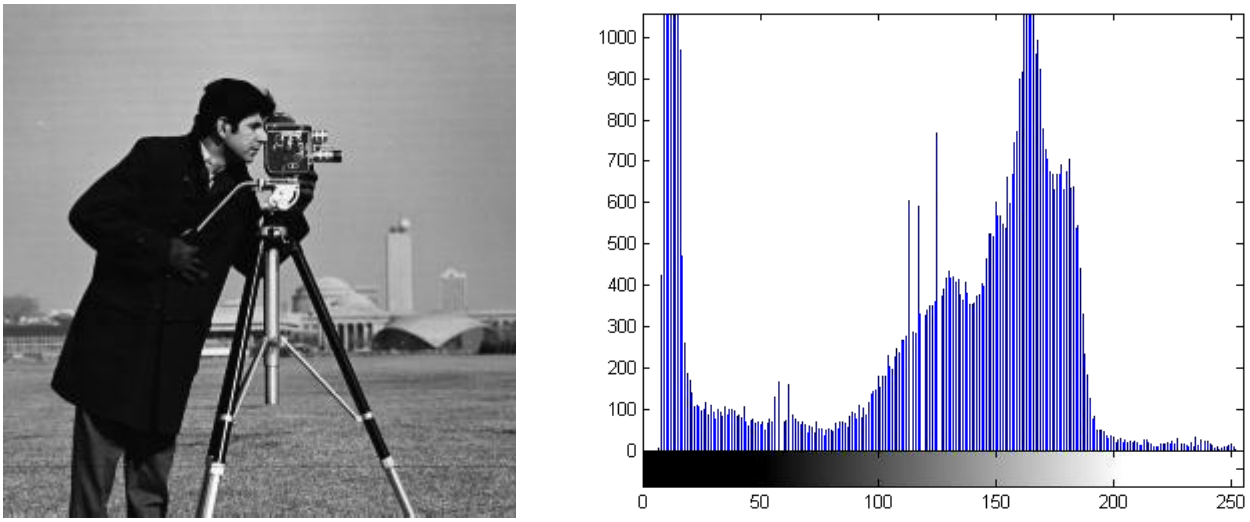

Fig. 4: Image and its histogram after decryption (Cameraman.png)

Table1 1: Performance Comparison of Image Encryption Schemes

Encryption Technique	Tunable	Visual Degradation	Compression Friendliness	Format Compliant	Speed	Cryptographic Security
Partial Encryption of Compressed Images and Videos (2002) [8]	No	High	Yes	Not Applicable	Fast	Low
Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments (2002) [9]	No	High	No	Yes	Fast	Medium
Techniques for a selective encryption of uncompressed and compressed images (2002) [10]	Yes	High	Yes	Not applicable	Fast	Low
A Partial Image Encryption Method with Pseudo Random Sequences (2004) [11]	Yes	High	No	?	Fast	?
A Robust Image Encryption Technique based on Random Vector (2008) [12]	?	High	Yes	?	Fast	Moderate
Securing Image Transmission using In-compression Encryption Techniques (2010) [13]	?	High	Yes	?	?	High
An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher [1]	Yes	High	Yes	No	Variable	Moderate

From table 1, it is observed that the performance of the proposed system is somewhat improved over other existing image encryption techniques.

As shown in table 1, value of the factor visual degradation is high for proposed technique, which means after encryption the plain image becomes so distorted that it can't be able for attackers to recognize that what the content of the image is?

The value of the compression friendliness factor is yes for the proposed algorithm which means after encryption the size of the image remains same as that of original plain image. The size of the image also remains same after decryption also.

The encryption speed of the algorithm is shown as variable which means the algorithm executes fast for small images and the execution time goes on increasing as the size of the image is increases. Also as it is a symmetric key algorithm, its speed is comparatively better than other asymmetric algorithms.

The cryptographic security of the proposed algorithm is completely depending on the key provided for the encryption. Decryption of the encrypted image is possible only when proper key is provided.

The result analysis can also be done with the help of some parameter calculations. Parameters like Entropy, Coefficient Correlation, Peak Signal-to-Noise Ratio (PSNR) can be used to compute the performance of an encryption algorithm.

Peak Signal-to-Noise Ratio (PSNR): The term peak signal to noise ratio is an expression for the ratio between the maximum possible value of a signal and the value of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of decibel.

If an algorithm can enhance a known degraded image or decrypt an encrypted image to more closely match to the original, then it can be concluded that it is a better algorithm. [15]

To test performance of proposed algorithm, Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are calculated using standard image processing tools like MATLAB.

MSE is calculated by using the formula,

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{i,j} - Y_{i,j}\right)^2$$

Where $X_{i,j}$ is the value of the original input image pixel and $Y_{i,j}$ is the value of the decrypted image pixel.

PSNR is calculated by using the formula

$$PSNR = 10 \log_{10} \left(\frac{{I_{max}}^2}{MSE} \right)$$

Where I_{max} is the maximum intensity value.

It means higher is the value of the PSNR; the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm.

When the MSE between two images is calculated and the MSE obtained is zero then the two images are identical to each other. The MSE value for any image used for encryption using proposed method is calculated as zero. And as MSE calculated as zero, automatically PSNR calculated as infinity. When MSE is zero and PSNR is infinity, then there is zero data loss in the decrypted image. i.e. decrypted image is identical to original image.

4. CONCLUSION

The proposed method is implemented on .net platform using C#. This method of encryption can be applied for all the formats of images. The proposed system is an improvement over existing image encryption methods using a combination of block based image transformation and encryption techniques. Correlation among pixels was decreased when the proposed method was applied to the blocks. As the number of blocks is not fixed therefore it can't easily be guessed by any attacker.

For better transformation the block size should be small, because fewer pixels keep their neighbors. In this case, the correlation among the pixels will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighborhood pixels.

The proposed system uses maximum 8 blocks for dividing an image. The future work for this method is using more blocks. Also security of key can also be improved.

5. ACKNOWLEDGMENT

Yashpalsingh Rajput thanks to Prof. A. K. Gulve, Associate Professor, Computer Science & Engineering Department, Government College of Engineering, [Autonomous], Aurangabad, for his constant support and helping out with the preparation of this paper.

6. REFERENCES

[1] Yashpalsingh Rajput and A K Gulve, "An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher", International Journal of Computer Applications 83(13):4-8, December 2013. Published by Foundation of Computer Science, New York, USA

[2] Somdip Dey, "SD-AI: A Cryptographic Technique to Encrypt Images", International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 26-28 June 2012, pp. 28 - 32.

[3] Garry C. Kessler, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html#intro

[4] Jolly Shah and Dr. Vikas Saxena, "Performance study on Image Encryption Schemes", International Journal Of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011, pp. 349 – 355.

[5] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp. 3033 – 9622.

[6] "Practical Cryptography - HILL CIPHER", http://practicalcryptography.com/ciphers/hill-cipher/

[7] Vidit Kumar Singh, "Hill Cipher–Essays-Vidschauhan", http://www.studymode.com/essays/Hill-Cipher-1592453.html

[8] Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos," IEEE Transaction on Signal Processing, Vol. 48, No. 8, August 2000, pp. 2439- 2451.

[9] M. Podesser, H. P. Schmidt, and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments," in Proceedings of the 5th Nordic Signal Processing Symposium, Tromso, Norway, October 2002.

[10] M. Van Droogenbroeck and R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images", in Proceedings of Advanced Concepts for Intelligent Vision Systems, Ghent, Belgium, September 9-11, 2002, pp. 90-97.

[11] Y.V. Subba Rao, Abhijit Mitra and S.R. Mahadeva Prasanna, "A Partial Image Encryption Method with Pseudo Random Sequences", In Proceedings of International Conference on Information System Security, Kolkata, India, December 19-21, 2006, Springer LNCS 4332, pp. 315-325.

[12] Nidhi s. Kulkarni, Indra Gupta and Shailendra N. Kulkarni, "A Robust Image Encryption Technique based on Random Vector", in International Conference on Emerging Trend in Engineering and Technology, July 16-18, 2008, pp. 15-19.

[13] Shaimaa A. El-Said, Khalid F. A. Hussein and Mohammed M. Fouad, "Securing Image Transmission using In-compression Encryption Techniques", International Journal of Computer Science and Security, Vol. 4, No. 5, 2010, pp. 466-481.

[14] Kerckhoffs principle - http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Kerckhoffs__principle.html

[15] PSNR - http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio