Covenant Journal of Engineering Technology (CJET) Vol.1 No. 2, Dec. 2017

An Open Access Journal Available Online

Development of an Encrypting System for an Image Viewer based on Hill Cipher Algorithm

Okereke Chinonso, Osemwegie Omoruyi, Kennedy Okokpujie & Samuel John

Department of Electrical and Information Engineering,
Covenant University,
Ota, Ogun state, Nigeria
Corresponding Author: Kennedy.okokpujie@covenantuniversity.edu.ng

Abstract: Security breaches to personal computing devices, cloud storage accounts, portable media devices are rampant in today's world. Also, Increased intrusions into corporate servers and employee workstations often times lead to the unwarranted exposure of an individual or corporate secret and a breach to privacy. Information leaked through such intrusions and breaches especially images are often times in the public terrain without a user's or corporate consent. This breaches are due to a variety of reasons including internal saboteurs, theft, social engineering or a computer security attack. At times other crimes like fraud, blackmail, kidnapping and assassinations may follow. This study presents the development of an Encryption system in an Image Viewer Application. Encrypting Images before storage or transfer to any platform helps limit risk when images are stolen or leaked. The image viewer was designed in C#.NET using the Hill Cipher algorithm for Image Encryption and Decryption. The results for images are shown to be good for two image samples. However, low key image samples produce a better result after Encryption. In general, Encryption of user generated images is a vital security strategy and a good option to have to prevent against a growing number of threats.

Keywords: Images, Pictures, Cryptography, Encryption, Information Security, Cipher, Viewer.

1.0 Introduction

Pictures speak louder than words, so says a popular English proverb. Images have the ability to communicate non-verbally to people of all races or colour excepting the visually impaired or

challenged. The surge in social media's popularity is in no small way down to amongst many factors the use of diverse media especially images in varying formats used in communicating individual opinions and views [1]. Images are also vital to individuals, corporations and brands because they can communicate a variety of emotions including excitement, scorn, anger, embarrassment and humour. In 2013, Facebook, the world's largest social media base, noted on average that 350 million images are uploaded to its platform daily, an estimated 4000 images per second [2, 3].

There has also been a steady increase in Cloud storage i.e. Storage as a service platforms as an alternative to traditional user owned storage media (Flash drives, Compact Disc, External Hard drives, System Hard Drives). Computing and Mobile devices now carry software applications that make movement of images to such platforms seamless and easy. This has also encouraged a commensurate increase in user generated imagery and pictures. New platforms have also arisen from related to the Cloud storage trend, a good example user generated news platforms hosted by Electronic and Print Media for harvesting news contents. By using cloud storage such platforms support the upload of news stories using Images and Visuals. Although all of this can be judged as a positive trend, there are also the accompanying security risks and threats heralded by such developments. Breach to the security of private user generated images on web, social media, cloud storage and portable device platforms are on the increase. Such vulnerabilities on this respective platforms highlighted have become tools for nefarious actors to carry out non-technical attacks like social engineering and to perpetrate other crimes like fraud, blackmail, human trafficking, kidnapping and assassinations. Several of this platforms have responded by tightening privacy controls especially on web platforms, restricting users who can view particular information like images. However, they are not adequate to cover all risks posed by users on such platforms. A preventive strategy on the rise is that of encrypting information communicated between users but there are also legal and juridical challenges to this approach. Encryption of information employs specialised techniques of ciphering user content so that only legitimate or proper recipients are able to decipher such information with the aid of a special key. Adoption of encryption needs to be more prevalent on many platforms to limit and mitigate risks posed to users on a variety of platforms where image dissemination, transfer or storage is done.

This study details the development of an Encryption system in an Image Viewer Application for a variety of Image formats that uses the Hill Cipher cryptographic algorithm for encrypting viewed images on the go. Users also have the option of decrypting the Images for private viewing. The studies outline is as follows: Section 2 explains the Hill Cipher Algorithm. Section 3 covers the design phase of the developed encryption system. Section 4 outlines the results achieved for various Images. Section 5 concludes the study.

2.0 Review of Hill Cipher Algorithm

Hill Cipher was developed in the late 1920s by Lester Hill [4, 5]. The Hill cipher is a polygraphic substitution cipher [6] were a block of at least two

numbers are replaced with another block of numbers or symbols with the same size. This mix is done using matrices and matrix manipulations. The Hill Cipher has several advantages including defending against attack by frequency analysis of cipher values [7, 8]. Hill Cipher also is very advantageous in data and plaintext encryption [4]. Implementation of the Hill Cipher requires linear algebra and modulo arithmetic. The ideal algorithm is a symmetric key algorithm where the same key (which could be a self-invertible key) for encryption is used also for decryption of a set of values. However, a regular invertible key would have to be inverted if it's to be used for decryption.

A matrix is said to be invertible if $M.M^{-1} = I$, where M^{-1} is the inverse of M and I is an identity matrix. In the case of the hill cipher key k, $K.K^{-1} = I$ is the requirement for an application generated or used encryption key. It is obvious that for a matrix to be invertible it must be a square matrix but it is also true that not all square matrices are invertible. A matrix is not invertible if its determinant equals zero. A simple example is a matrix $B = \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$, where the determinant is $2 \times 1 - 2 \times 1 = 0$ and the resultant inverse $\frac{1}{0}$ is undefined. This is said to be a singular matrix.

Digital Images can be modelled as a three band monochrome image data [9], i.e. Red-Green-Blue (RGB) components, each component been an 8 bit value ranging from 0 - 255 in decimal or 00- FF in hexadecimal. Discarding the Alpha component of our images, a three pixel bitmap block P contains $\begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix}, \begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix}$ *and* $\begin{pmatrix} G_1 \\ G_2 \\ G_3 \end{pmatrix}$ and requires a key

K= $\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$ for encryption to get the cypher image component:

$C = \begin{pmatrix} RC_1 \\ RC_2 \\ RC_3 \end{pmatrix}, \begin{pmatrix} BC_1 \\ BC_2 \\ BC_3 \end{pmatrix}$ *and* $\begin{pmatrix} GC_1 \\ GC_2 \\ GC_3 \end{pmatrix}$.

More clearly,

$$\begin{pmatrix} RC_1 \\ RC_2 \\ RC_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \\ R_3 \end{pmatrix} \bmod 256$$

$$\begin{pmatrix} BC_1 \\ BC_2 \\ BC_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \bmod 256$$

$$\begin{pmatrix} GC_1 \\ GC_2 \\ GC_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} G_1 \\ G_2 \\ G_3 \end{pmatrix} \bmod 256$$

$$RC_1 = (K_{11}R_1 + K_{12}R_2 + K_{13}R_3) \ mod \ 256$$
$$RC_2 = (K_{21}R_1 + K_{22}R_2 + K_{23}R_3) \ mod \ 256$$
$$RC_3 = (K_{31}R_1 + K_{32}R_2 + K_{33}R_3) \ mod \ 256$$

or $RC = KR$.

For decryption to retrieve the original decomposed RGB components, $R = K^{-1}.RC$. For the encryption key to be the same as the decryption key, Hill Cipher requires that the key k be a self-invertible matrix. In this case, $M = M^{-1}$. Panigrahy et al [4] expounds on solving and obtaining self-invertible matrices in detail. Using a self-invertible key may lengthen computation time because matrices would have to be generated and tested using the self-invertible condition.

3.0 Design of the Crypto Viewer

Based on the Hill Cipher algorithm, the Crypto viewer design flowchart shows the various sequence of steps and iterations in carrying out the encryption of an image divided into two stages. The first stage, involves the splitting of the image into Red-Green-Blue (RGB) components. The components are stored as separate arrays (R_{array}, G_{array} and B_{array}). The Alpha components although important is not used in this study. Alpha component contains details on image luminance.

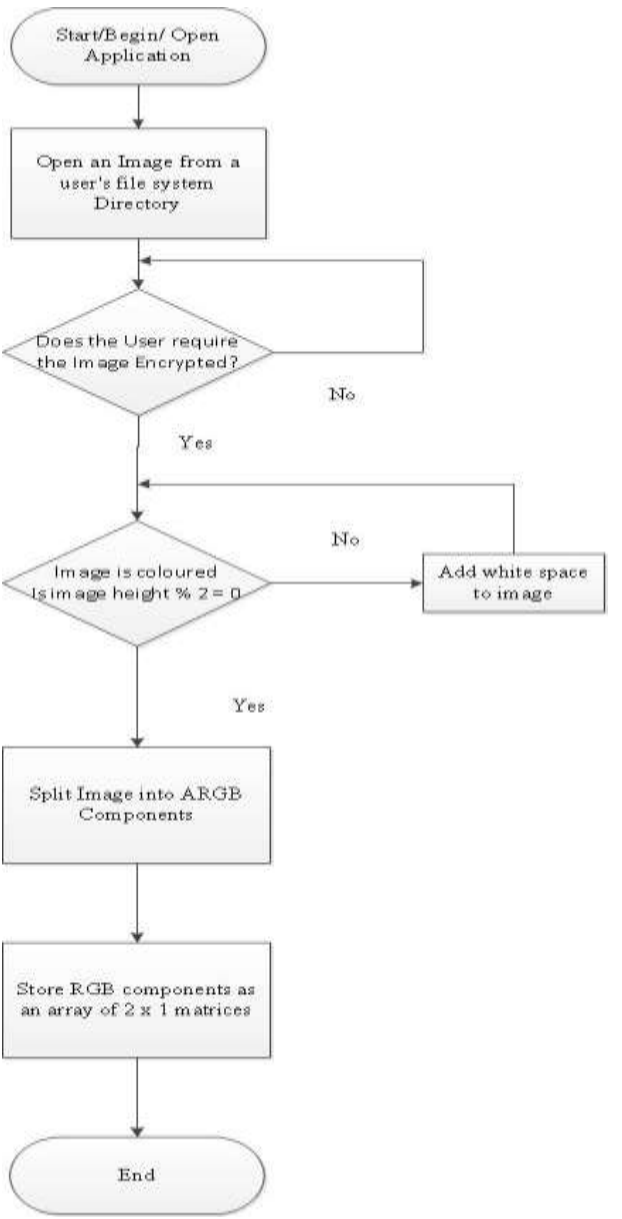

Figure 1. Decomposing of Image into RGB components

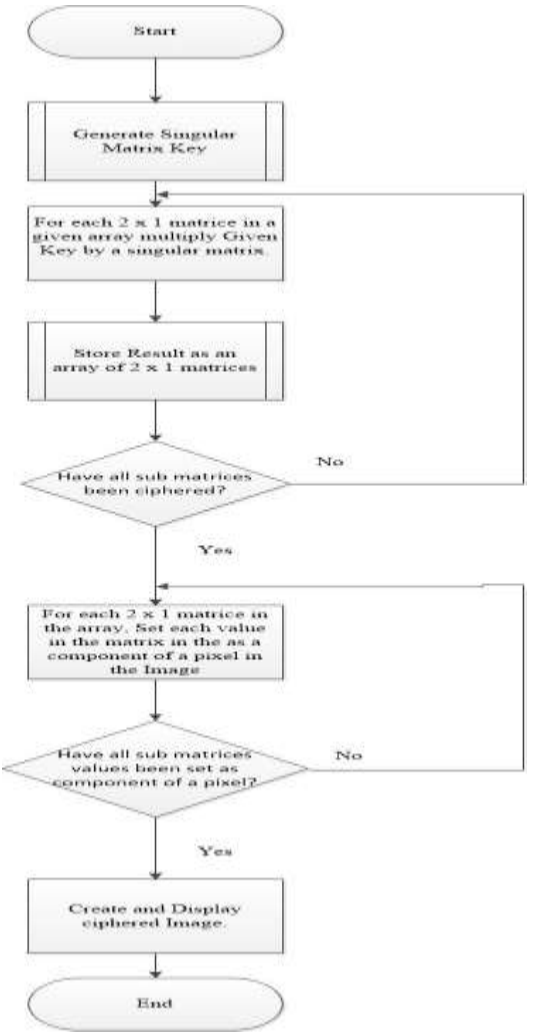

Figure 2. Generation of Encryption Key and the creation of an Encrypted Image.

4.0 Implementation

The results from two images are displayed as seen from Figures 3a, 3b, 3c, 4a, 4b and 4c. High value (key) images are a lot more recognizable after encryption. Low value (key) images i.e. images with more pixels closer to full amplitude produce better results on the whole. The processing speed of large images i.e. Images larger than 100KB takes > 15 seconds as seen in Table 1. Image formats can be .jpg .png, .jpg, .bmp or .gif.

Figure 3a.Original high key image

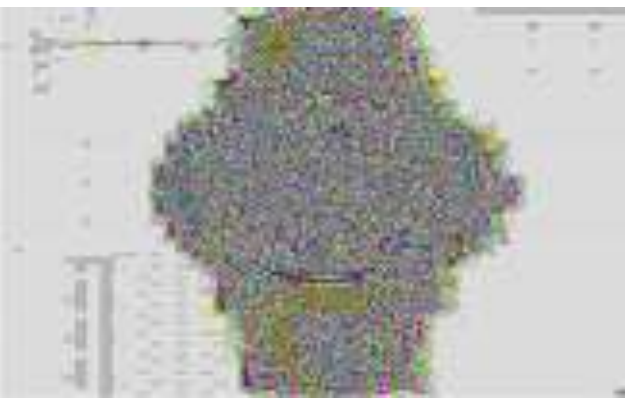

Figure 3b. Encrypted high key image

Figure 3c. Decrypted image result

Figure 4a Original low-key Image

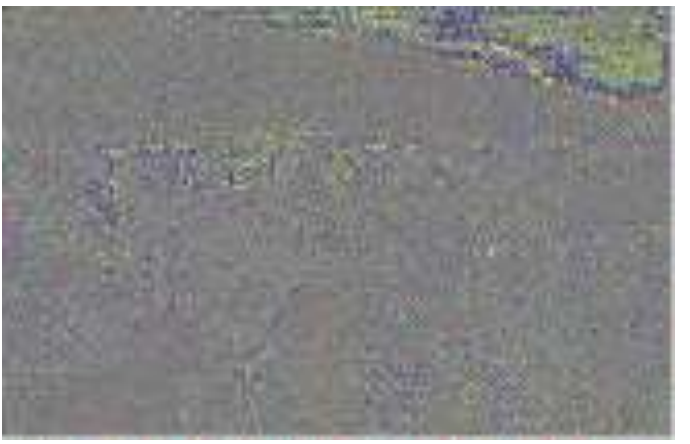

Figure 4b Encrypted low-key image

Figure 4c Decrypted image result

System Information	Intel Pentium B960 2.20 GHz 4GB memory		
Image name	**Encryption time(s)**	**Format**	**Size in KB(resolution)**
Watch	2..2657	.jpg	18.1(400 x 400
Old Custom Office	16.125	.jpg	143.0(1280 x 1116)

Table 1: System specification and Image Information

5.0 Conclusion

The unpredictability of an encryption scheme is always a desirable trait of any encryption tool. The above viewer makes the encryption of images fast for any user. However, more security could mean that tool can make use of a random key sizes whilst key size length and key could be stored as Meta data also in Encrypted format with the images. The encryption scheme can also be randomly chosen such that encrypted image results are more difficult to retrieve. Encrypted Images in this case are of a hybrid form. Image RGB components can also be randomly stored in key value stores and served on the fly for web based applications aside from a device based scenario.

Acknowledgements

We acknowledge the support of Covenant University in conducting this research and the cost of publication.

Further Study

This study hopes to further evaluate using a variety of encryption quality metrics the effectiveness of the hill cipher algorithm for image encryption.

Figure 5: Image Viewer Interface

References

[1] A. Lenhart, K. Purcell, A. Smith, and K. Zickuhr, "Social Media & Mobile Internet Use among Teens and Young Adults. Millennials.," Pew Internet Am. Life Proj., pp. 1–37, 2010.

[2] B. Thomee et al., "YFCC100M: The New Data in Multimedia Research," 2015.

[3] "Facebook by the Numbers (2017): Stats, Demographics & Fun Facts." [Online]. Available: https://www.omnicoreagency.com/facebook-statistics/. [Accessed: 14-Oct-2017].

[4] S. K. Panigrahy, B. Acharya, and D. Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm," Image (Rochester, N.Y.), no. February, pp. 21–22, 2008.

[5] K. Mani and M. Viswambari, "Generation of Key Matrix for Hill Cipher using Magic Rectangle," vol. 10, no. 5, pp. 1081–1090, 2017.

[6] B. Acharya, S. K. Patra, and G. Panda, "Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System," Int. J. Recent Trends Eng. Vol. 1, No. 4, May 2009, vol. 1, no. 4, pp. 106–108, 2009.

[7] M. Mokhtari, "Analysis and Design of Affine and Hill Cipher," vol. 4, no. 1, pp. 67–77, 2012.

[8] Chris Christensen, "Introduction to Hill cipher," Lecture note. [Online]. Available: https://www.nku.edu/~christensen/092mat483/hill/cipher.pdf. [Accessed: 30-Sep-2017].

[9] S. E. Umbaugh, Computer Imaging: digital image analysis and processing. CRC press, 2005.