

# Encryption of Decomposed Image by using ASCII Code based Carrier Signal

Reema Dhiman<sup>1</sup>, Butta Singh<sup>2</sup>

<sup>1</sup> Student Mtech, Department of Electronics and Communication Engineering, GNDU RC, Jalandhar, India.

<sup>2</sup> Assistant Professor, Department of Electronics and Communication Engineering, GNDU RC, Jalandhar, India.

\*\*\*

**Abstract** - Encryption is one of the best method to secure picture data. An ASCII code based carrier signal and image decomposition has been outlined in this paper. Image decomposition is an efficient technique which is used for image encryption and this decomposed image is further proceeding for encryption process. The Carrier image is used for encryption process which is to be generated by using ASCII Codes. A sturdy password is used to encrypt the image with the help of carrier. This method is applied on various images for the calculation of image parameters. After evaluating all these aspects, parameters like correlation, entropy is calculated for both the encrypted as well as decrypted image.

**Key Words:** Carrier Image, ASCII Code, Entropy, Correlation

## 1. INTRODUCTION

Security issues [1] have turned out to be increasingly genuine with the fast improvement of the web and the approach of advanced cell phones that use a lot of private data, particularly pictures, which are presented to the system. However, because of data size and the high excess among the crude pixels of a computerized picture, conventional encryption algorithms such as data encryption standard (DES), international data encryption algorithm (IDEA) and advanced encryption standard (AES) might not be appropriate for image encryption. To forestall image data spillage, many new image encryption algorithms have been proposed by using different techniques, including chaos theory [2], DNA coding [3], and compressed sensing [4]. Information security is one of the significant issues in the current information age, as there is a continuous development in the pace at which the information is being distributed [5]. There are few techniques for image encryption which manages their own thoughts or ideas. In couple of algorithms, encryption process depends just on the catch phrases; however in some different algorithms they utilize some carrier image for encryption. Because of this, we have a thought to combine the current algorithms to get another way for encryption by taking the benefits of individual techniques. Consequently we concoct the idea of decompose the original image and create carrier for Image encryption to get profoundly contorted Image. Panduranga et al proposed [6] a secure method by hybridizing the SCAN

pattern and the carrier image for image encryption to get extremely distorted image. They developed the perception of generating the carrier image with the help of distinctive code called as 4 out of 8-code. The proposed hybrid approach for image encryption gives very superior results but the password used in this algorithm is not secure. So, in our proposed approach, ASCII codes are used for generating the carrier image and this carrier is used further for encryption process.

## 2. PROPOSED METHODOLOGY

Encryption of an image should be possible at various stages and in numerous ways. If the encryption process is only in single stage then security is less as contrast with multistage encryption [6]. In our proposed mechanism, the decomposition of image is carried out over various levels and this decomposed image is used for encryption process. Now, the following steps are used for both the encryption and decryption process.

### 2.1 Encryption Process

The encryption process is implemented in MATLAB and it involves the following steps:

**Step 1:** Load an image for encryption.

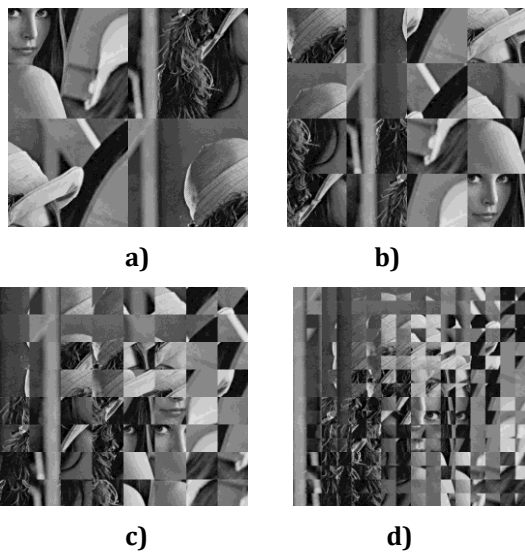
**Step 2:** Decompose the image into various levels in vertical and horizontal direction. This decomposition is carried out at 4 levels.

**Step 3:** Enter the prototype for arranging the decomposed blocks at level 1, level 2, level 3 and level 4 as shown in Fig-1.

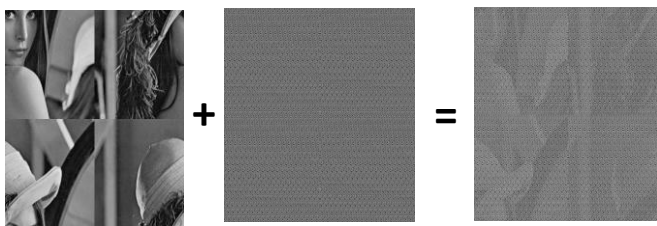
**Step 4:** Enter the password for encryption and generate the carrier image by using ASCII code. The password used in the encryption process is '!~"z#y\$x \$w%v &u\*t+s,r-q.p/o 1n 2m 3l4k 5j 6i 7h8g 9f:e;d <c=b>a?'@\_A^B\CZDYEXFWGVHUITJS KRLQMP NO'. With the help of this password, a carrier image is generated.

**Step 5:** Add the carrier image with the decomposed image as shown in Fig-2.

**Step 6:** Finally, we get an encrypted image.



**Fig-1:** Decomposed Images at a) Level 1 b) Level 2  
c) Level 3 d) Level 4



**Fig-2:** Addition of Carrier with decomposed Image

In this way, encrypted image is generated at the transmitter side. Now, this image is passing through the channel and received at the receiver end.

## 2.2 Generation of Carrier Signal by using ASCII Codes

Here we are characterizing another code called ASCII code. This code is of 8 bit length and it gives an encoding of 128 characters.

$$\log_2 128 = 7$$

A set of 94 conceivable combinations of the ASCII code words and each code is allotted to an alphanumeric character and additionally special characters. Depending upon the keyword, carrier image is generated and utilized as a part of the addition process to create an encrypted image. In this we choose the ASCII codes that is used for the generation of strong password that comprises of special characters which is having binary values as well as DEC values. For Ampersand, the ASCII value is 38, for single quote, the ASCII value is 39, for left and right parenthesis, the ASCII values is 40 and 41. For Asterisk, the ASCII value is 42, for Plus, the value is 43, for comma=44, minus=45, period=46, slash=47, zero=48, One=49, Two=50, Three=51, Four=52, Five=53, Six=54, Seven=55, Eight=56, Nine=57, Colon=58, Semicolon=59, less than=60, equality sign=61,

greater than=62, question mark=63, at sign=64, capital letters= 65 to 90, left square bracket=91, Backslash=92, right square bracket=93, caret / circumflex=94, Underscore=95, grave / accent=96, small letters=97 to 122, left curly bracket= 123- C3, vertical bar= 124-C4, right curly bracket= 125- C5, Tilde=126-C6, Delete=127- C7.

Following are the steps which are used to generate the carrier image.

**Step 1:** Enter the password for encryption.

**Step 2:** Search the alphanumeric characters and symbols in the ASCII code words.

**Step 3:** The binary values of ASCII code words is converted into the decimal values.

**Step 4:** With the help of these decimal values, the carrier image is generated with different patterns.

Hence, in this way, carrier image is generated for the encryption process.

## 2.3 Decryption Process

The decryption process is implemented in MATLAB and it involves the following steps:

**Step 1:** At receiver end, the encrypted image is received.

**Step 2:** Enter the password for decryption and generate the carrier image by using ASCII code words.

**Step 3:** When the password match then it will subtract the encrypted image from carrier image and we get an original decomposed image.

**Step 4:** Enter the prototype for re-arranging the decomposed blocks and then we get a decrypted image.

The above steps show the encryption as well as decryption process.


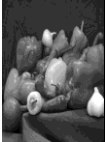



## 3. RESULTS AND DISCUSSION

This section describes the implementation of proposed methodology for different images. Here, the methodology is used on different images and its results will be calculated. The essential requirement to implement our approach are MATLAB of version R2013a or higher. The parameters used are correlation analysis and entropy analysis as discussed below:

### 3.1 Entropy Analysis

The mathematical determination of randomness in an image and that can be utilized to describe the texture of the input image quantity [7]. The Table-1 shows the results of different images at different level of decomposition.

**Table -1:** Entropy Analysis of encrypted and decrypted image

Image	Entropy of original image	Image Decomposition Level	Entropy of encrypted image	Entropy of decrypted image
	7.4571	Level 1	7.5193	7.4571
		Level 2	7.5202	7.4571
		Level 3	7.5197	7.4571
		Level 4	7.5192	7.4571
	6.9924	Level 1	7.5115	6.9925
		Level 2	7.5109	6.9925
		Level 3	7.5117	6.9925
		Level 4	7.5115	6.9925
	7.1225	Level 1	7.5307	7.1227
		Level 2	7.5306	7.1227
		Level 3	7.5247	7.1227
		Level 4	7.5305	7.1227
	7.2154	Level 1	7.5245	7.2154
		Level 2	7.5249	7.2154
		Level 3	7.5247	7.2154
		Level 4	7.5250	7.2154
	7.3738	Level 1	7.5136	7.3738
		Level 2	7.5142	7.3738
		Level 3	7.5310	7.3738
		Level 4	7.5142	7.3738

The above table shows the entropy of original, encrypted and decrypted images for different images at all the decomposition levels. As observed the entropy of encrypted image is increases as compared to the original image which shows that the encrypted image has superior randomness. Also, there is a slight difference between the original and decrypted image which shows our algorithm gives improved results.

### 3.2 Correlation Analysis

The effect of the image decomposition is related to the correlation of adjacent pixels. In order to calculate the correlation between the plain image and the original image then different levels of decomposition are analyzed for both the original and the plain image. Following are the formulae

which are used to calculate the correlation coefficients in the horizontal, vertical and diagonal directions.

$$\gamma = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$


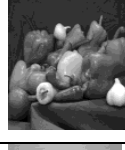



$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))$$

Where E(x) and D(x) are the mean and standard deviation of the corresponding gray scale values of two-adjacent pixels in the image and N is the number of duplets (x,y) obtained from the image. The Table-2 shows the various value for correlation.

**Table -2:** Correlation Analysis of encrypted and decrypted image

Image	Name of Image	Image Decomposition Level	Correlation for encrypted with original image	Correlation for decrypted with original image
	Lena	Level 1	0.0072	1
		Level 2	0.0086	1
		Level 3	0.0063	1
		Level 4	0.0273	1
	Peppers	Level 1	-0.0110	1
		Level 2	-0.0167	1
		Level 3	0.0175	1
		Level 4	0.0278	1
	Camera-man	Level 1	-0.0268	1
		Level 2	0.0087	1
		Level 3	0.0287	1
		Level 4	0.0710	1
	Boats	Level 1	-0.0372	1
		Level 2	0.0152	1
		Level 3	0.0287	1
		Level 4	0.0383	1
	Baboon	Level 1	0.0102	1
		Level 2	0.0089	1
		Level 3	0.0275	1
		Level 4	0.0192	1

As observed the correlation of encrypted image is highly correlated as compared to the original image. For effective encryption, the correlation coefficient should be close to zero which can be observed in the above table. Also, the correlation analysis between the original and decrypted image is nearly one which means the the original and decrypted image is same.

#### 4. CONCLUSIONS

An alternative approach is proposed for image encryption in which carrier image is generated by using ASCII code words. Here, the image is decomposed into 4 levels and after that the decomposed image is used as an input image for encryption process. A sturdy password is generated by using ASCII code words and then we get a highly encrypted image. Calculation of entropy and correlation analysis between encrypted and decrypted images is done for all the 4 levels. This chapter concludes that the proposed algorithm for image encryption gives better results as compared to other encryption process. For the sake of complexity, we use ASCII code words in which we can generate the carrier image by using alpha-numeric as well as special characters. We applied this approach on various images at different levels of decomposition. i.e. level 1, level 2, level 3 and level 4 for the complexity of algorithm. From all the experimental results, we conclude that our algorithm is best suited for encryption process.

#### ACKNOWLEDGEMENT

I would like to express my sincerest thanks to Dr. Butta Singh, Department of Electronics and Communication Engineering, who gave me support and encouragement and also provided me valuable and countless resources.

#### REFERENCES

- [1] Shujun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, Kwok-Tung Lo, "On the design of perceptual MPEG- video encryption algorithms," IEEE Trans Circuits Syst Video Technol, vol. 17, no. 2, pp. 214-223, February 2007.
- [2] Xing-YuanWang, Sheng-Xian Gu, Ying-Qian Zhang, "Novel image encryption algorithm based on cycle shift and chaotic systems," Opt Lasers Eng. vol. 68, pp. 126-134, May 2015.
- [3] RasulEnayatifar, Hossein JavedaniSadaei, Abdul HananAbdullah, MalreyLee Ismail FauziIsnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata." Opt Lasers Eng, vol. 71, pp. 33-41, August 2015.
- [4] NanrunZhou, AidiZhang, FenZheng, LihuaGong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing." Opt Laser Technol, vol. 62, pp. 152-160, October 2014.
- [5] Vinod patidar, N.K. Pareek, K.K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps." Common Nonlinear Sci Number Simulat, vol. 14, pp. 3056-3075, July 2009.
- [6] Panduranga H.T., Naveen kumar S.K., "Hybrid approach for image encryption using SCAN patterns and carrier images." International Journal on Computer Science and Engineering vol. 2, no. 2, 297-300, 2010.
- [7] Quist. A. Kester. "Image encryption based on the RGB pixel transposition and shuffling." International Journal Computer Network and Information Security vol. 7, pp. 43-50, June 2013.