Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019)
IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8

Image Encryption Technique Using Huffman Coding and Spatial Transformation

Archana Singh
Dept. Of Computer Science & Engg
Anand Engineering College,
Keetham, Agra
archisingh.15@gmail.com

Vinay Kumar Singh
Dept. Of Computer Science & Engg
Anand Engineering College
Keetham, Agra
vks.vinaykumarsingh@gmail.com

Shashank Yadav
Dept. Of Computer Science & Engg
Anand Engineering College
Keetham, Agra
shashankyadav48@gmail.com

Abstract: Security of data or image is one of the important steps in the enormous domain of multimedia. Encryption of images is well known technique to protect the information present in the image in order to maintain the confidentiality, authenticity and integrity of images. This paper proposed a method for image encryption based on the Huffman coding and homogeneous transformation of pixels. Huffman coding is used to protect the huge amount of data with good visibility and no loss of information. Encrypted image generated by the proposed work is quite different from the original image.

Keywords: image processing, image encryption, image decryption, Huffman coding.

I. INTRODUCTION (*HEADING 1*)

Encryption is playing a vital role in communication, as people are using interactive media like image, audio and video. Image encryption is used to preserve the secrecy of image. It is also playing an important role in several fields like- National security agencies, military etc [13]. Encryption provides security to the senders and receivers for sharing confidential data over an insecure medium. Due to these security properties, cryptography is commonly used for image encryption across the network.

The primary aim of keeping images protected is to maintain confidentiality, integrity and authenticity [16] as shown in Fig. 1. and Fig. 2.

Fig. 1. Panda

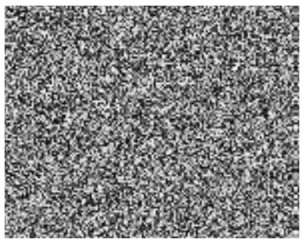


Fig. 2. Cipher

Encryption is an art which involves the conversion of plaintext into an encrypted data or cipher text that cannot be read by anyone without converting the cipher text in the plaintext [6]. Decryption is also an important process that is used to convert the cipher text or encrypted data into plaintext [13]. Fig. 3. shows the method for encryption and decryption. A secrete key is used to encrypt and decrypt the plain text. These keys are different with each other but mathematically they are related with each other.

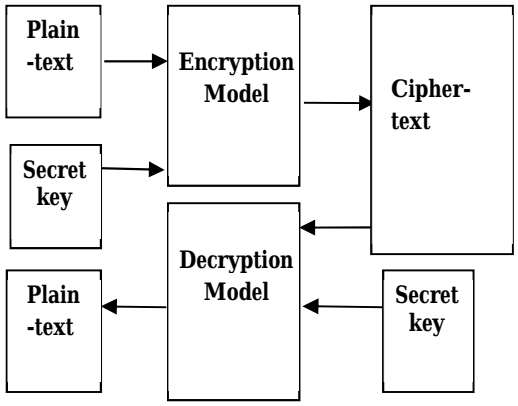


Fig. 3. Method for encryption and decryption

This paper focused on Huffman coding that is an important method for coding based on the frequencies of the symbols. Huffman coding is based on bottom up approach [7]. This method was introduced by David Huffman in 1952 [1]. In this scheme symbols are arranged accordingly to their frequencies or probability [8]. After that, the least frequent symbols are eliminated by adding the two lowest frequencies from the sorted list. Assign the sum of children's frequency to the parent node. Assign code **'0'** to the left child of the parent node and **'1'** to the right child of the parent node.

Example:

Input:	**A**	**C**	**B**	**D**	**E**	**F**
Frequency:	**6**	**4**	**5**	**1**	**2**	**3**

Arrange these symbols according to their probability are in ascending order.

Input:	**A**	**B**	**C**	**F**	**E**	**D**
Frequency:	**6**	**5**	**4**	**3**	**2**	**1**

With the help of Huffman tree as shown in Fig. 3. following codes are obtained:

Input:	A	B	C	D	E	F
Code:	0	101	100	1100	1101	111

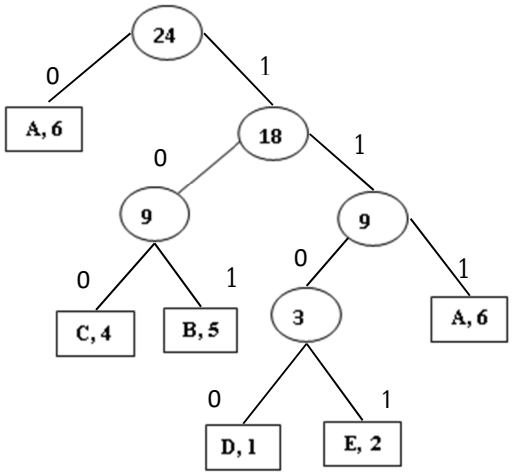


Fig. 3 Encoding method by Huffman Tree

II. LITERATURE SURVEY

Guosheng Gen et. al [5] proposed an image encryption algorithm based on substitution & permutation methods. This method improves the quality of the pseudorandom characteristics of chaotic sequence using cross sampling disposal and optimized treatment.

Amitava Nag et. al [2] proposed a method in which encryption is performed using 64 bits key. In this technique 4 subkeys each consisting of eight bits are used in Affin transformation to disperse the pixels. Then the entire image is broken down into 2 x 2 sub-images and an XOR operation is applied on each sub-image having subkeys (each of eight bits) to get the new pixel value.

Long Bao et. al [9] introduced a technique to compose 3 different dimensional well-defined chaotic maps. This proposed technique puts the logistic map as a controller to find the text map or a sine map to generate random sequence [9]. The diffusion and confusion property are then found, by using substitution and permutation network (SPN) structure [1,14]. As the key space is quite large, 240 bits are used to represent it.

Qiudong sun et.al [15] proposed a technique that uses uni-dimensional random scrambling. Initially the encryption algorithm transforms the whole image from two-dimensional image to one dimensional vector and performs random shifting on one dimensional vector [15]. After that, anti-transformation is applied on distributed vector for getting a cipher image. This method does not require iterative computation as the method obtains best result within one or two executions.

Mohmad Abbas et.at [10] has produced a novel technique that is based on the bit level permutation. This technique is based on the two steps: First XOR operation is applied then the pixel bits are rotated to perform confusion and diffusion properties. Then the algorithm performs a sequential XOR operation by applying circular right rotation on the bits of pixels present in the images. These two operations are performed multiple times to get the better result. In this method a common secrete key is used to perform encryption and decryption

Nidhi Sethi et.al [11] has imparted an encryption technique that compresses an image and also perform logistic mapping to encrypt an image. This technique compresses an image using Haar Wavelet transformation. Then break the entire image into 8 x 8 sizes of sub images and apply coding on these sub images. This encryption algorithm has two steps. In the first step of this algorithm, block-based scrambling is used to minimized correlation between the inter pixel. This shuffling technique uses genetic algorithm (GA) based crossover operation [11]. In the next step, the technique encodes pixel codes of the disseminated facsimile by performing two dimensional logistic maps. The method followed by logistic mapping fulfills the properties of diffusion and confusion in the encrypted image. Receiver receives a key by watermarking process that is generated by the logistic map.

Chang Mok Shin et.al [3] has propounded a method based on multilevel image encryption and image dividing system followed by binary XOR operation. In the method a binary image is obtained by splitting these multilevel images that have same gray values. Then the binary pictures are reproduced by phase encoding. In order to encrypt these images binary random phase images are used to perform binary phase XOR operation.

Rasul Enayatifar et.al [4] introduced a technique for image encryption using hybrid model followed by chaotic function and genetic algorithm. In this technique chaotic function is used to produce a number of encoded images. These encoded images are used as the initial population in the first generation of genetic algorithm. The genetic algorithm is used to find optimized solution. At the end, the best encoded-image is selected as the final encrypted image.

III. PROPOSED WORK

This paper introduced a method for image encryption based on Huffman coding and spatial transformation of homogeneous pixels using two random variables no. [U, V]. The intensity of pixels in the source image are reduced to encrypt the information available in it by using Huffman coding. Spatial transformation is used to redistribute the homogeneous pixels of output image.

A. Algorithm for encryption

- Read the gray scale image an as source image.
- Find out the frequency or probability of each pixel existing in the source image.
- Arrange all the pixels according to their frequency or probability in descending order to maintain a dictionary.

- Generate the binary code corresponding to each pixel present in the dictionary with the help of Huffman coding.
- Convert these binary codes generated by Huffman code into gray value.
- Assign these gray values to each corresponding pixel present in the dictionary.
- Generate output image with help of new pixel values from the dictionary. To generate output image, do the following steps:

  repeat steps

  if gray value ≤ 255

  then

  update original pixel value with new pixel value

  otherwise

  original pixel value

- Apply spatial transformation using two pixels of output image. Following mapping function is used to find out the co-ordinates of the pixels for cipher image.

$$X = A[I, J] \times U + A[I, J-1] \times V \quad (1)$$

$$Y = A[I-1, J] \times U + A[I, J] \times V \quad (2)$$

- Here ***'A'*** is the output image with the co-ordinates ***'I'*** & ***'J'***. ***'U'*** & ***'V'*** are the two random no. ***'x'*** & ***'y'*** are the co-ordinates value in cipher image,
- Generate the cipher image.
- Encrypt the dictionary by performing XOR operation using the global mean of pixels value present in the dictionary and each entry existing in the dictionary.
- Reshape the new dictionary.
- Exit

B. Algorithm for decryption

- Reshape the dictionary.
- Decrypt the dictionary by performing XOR operation using the global mean of pixels value of the original dictionary and each entry existing in the new dictionary.
- Find out the co-ordinates ***'I'*** & ***'J'*** of the output image with the help of the co-ordinates of cipher image using following mapping:

$$X = A[I, J] \times U + A[I, J-1] \times V \quad (3)$$

$$Y = A[I-1, J] \times U + A[I, J] \times V \quad (4)$$

- Arrange all the pixels of output image according to their frequency or probability in descending.
- Compare each entry of the original dictionary with the pixels of output image arranged according to their frequency or probability in descending.
- Generate original image.
- Exit.

IV. Experimental Result Analysis

This paper proposed a method to reduce the intensity of gray values present in the source image in order to encrypt it with the help of Huffman coding and spatial transformation. This method is categorized into two steps: (a) calculate the Huffman code value corresponds to each pixel present in the image. (b) Spatial transformation is used to redistribute the pixel values to encrypt the image. This algorithm has been applied on gray scale images. The range of the pixel values in gray scale images is 0 to 255 [12]. Fig. 4 shows the original images, images modified after applying Huffman code and cipher images after performing spatial transformation.

Histogram analysis of the original images and the cipher images is also included to ensure the secrecy of the images as it is possible to predict the information present in the histogram.

Correlation operation is used extract the similar information from images. High correlation shows high possibility to extract more information. In this paper we have calculated correlation coefficient between an image and the same image processed by median filter.

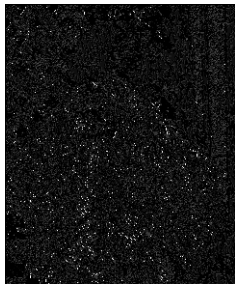
TABLE I. CORRELATION COEFFICIENT BETWEEN ORIGINAL AND CIPHER IMAGE

Image	Correlation	
	Original	Cipher
Pout	0.9959	0.2809
Tire	0.9969	0.2984
Rice	0.9902	0.3184

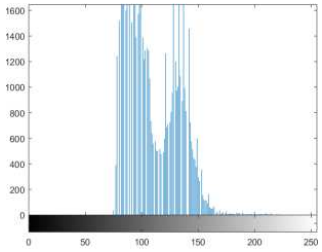
It has been observed that TABLE I shows the result in our favor as the correlation coefficient of cipher images is low as compare to original images.

(a) Pout

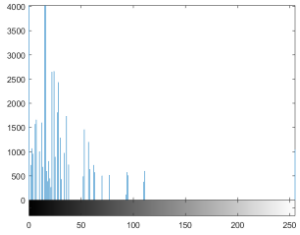
(b) by Huffman code



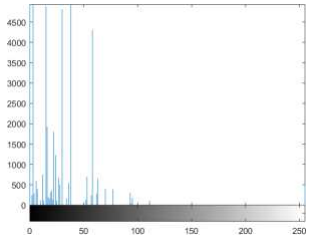
(c) Cipher image



(i) Histogram of original image

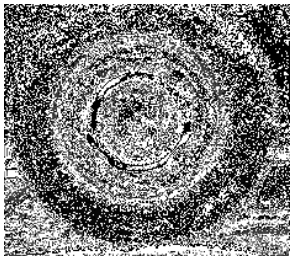


(ii) Histogram of an image generated by Huffman code

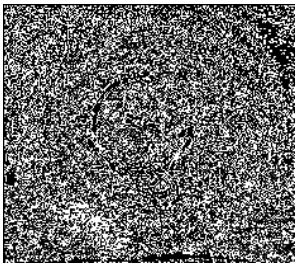


(iii) Histogram of Cipher image

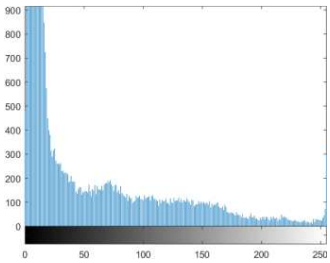
(a) Tire



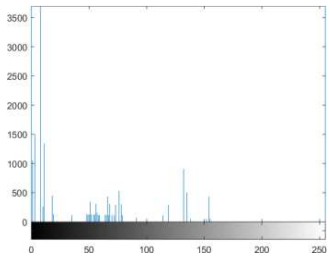
(b) by Huffman code



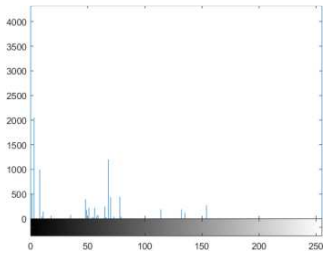
(c) Cipher image



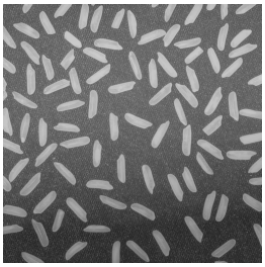
(i) Histogram of original image



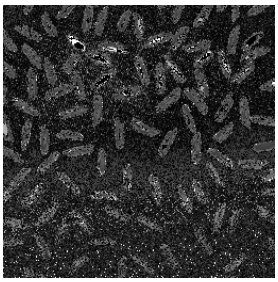
(ii) Histogram of an image generated by Huffman code



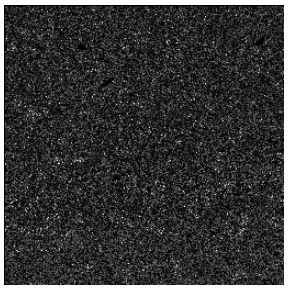
(iii) Histogram of Cipher image



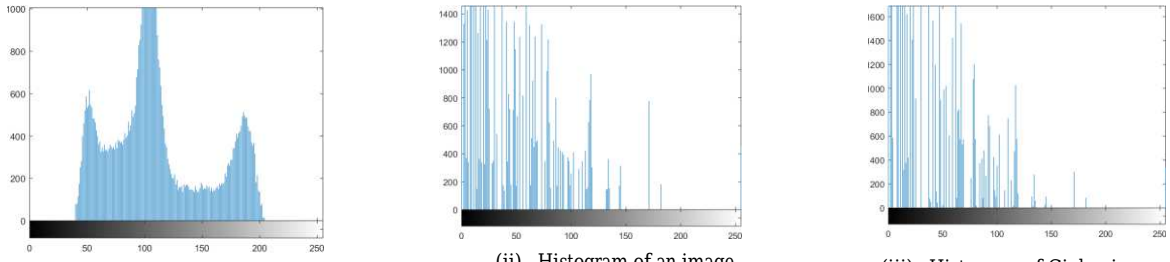
(a) Rice



(b) by Huffman code



(C) Cipher image



(i) Histogram of original image

(ii) Histogram of an image generated by Huffman code

(iii) Histogram of Cipher image

Fig. 4. (a) Original Image (b) Image generated by Huffman code (c) Cipher image and (i) Histogram of original image (ii) Histogram of an image generated by Huffman code (iii) Histogram of Cipher image

V. Conclusion and Future Work

Nowadays, communication of digital products is more challenging task over the open network. For this purpose, several image encryption algorithms have been reviewed. This paper proposed a method to encrypt an image using Huffman coding. This method is useful for real time encryption. Decryption of the image is also not easy as it requires the same dictionary that was used in encryption as a secret key spatial transformation is also applied that relocates the homogeneous pixel coordinates in the cipher images. From Fig. 4. and TABLE I it has been observed that the proposed algorithm provides better result to maintain the confidentiality of an image. This technique can be improved using adaptive Huffman coding technique. It is an extension to Huffman coding.

REFERENCES

[1] A. A. Shaikh, P. P. Gadekar, "Huffman Coding Technique for Image Compression", 2015, COMPUSOFT, An international journal of advanced computer technology, Volume-4, Issue-4, ISSN:2320-0790.

[2] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation" 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 21-22 July 2011, pages: 309-312.

[3] Chang-Mok Shin, Dong-HoanSeo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, "Multilevel Image Encryption by Binary Phase XOR Operations", IEEE Proceeding in the year 2003.

[4] Enayatifar Rasul, Abdullah Abdul Hanan, "Image Security via Genetic Algorithm", 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.

[5] Gen Guosheng, Han Guoqiang, "An Enhanced Chaos Based Image Encryption Algorithm", IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

[6] John Justin M, Manimurugan S, "A Surve on Various encryption Techniques", International Journal of Soft Computing and Engineering.

[7] Khalid Sayood. "Introduction to data compression. Morgan Kaufmann Publishers", San Francisco, California, 1996.

[8] Lavisha Sharma, Anuj Gupta, "Image Encryption Using Huffman Coding for Steganography, Elliptic Curve Cryptography and DWT for Compression", 2016, International Journal of Advance research, Ideas and Innovations in Technology, Volume2, Issue5, ISSN: 2454-132X.

[9] Long Bao, Zhou Yicong, Chen, C. L. Philip, Liu Hongli, "A New Chaotic System for Image Encryption" 2012 International Conference on System Science and Engineering, June 30-July 2, 2012, pages: 69-73.

[10] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", 2012, International Journal of Security and Its Applications, vol.6, no.1, pages: 1-8.

[11] Nidhi Sethi, Deepika Sharma, "A New Cryptographic Approach for Image Encryption", 2012, Parallel, Distributed and Grid Computing (PDGC), IEEE 2nd International Conference on 6-8 Dec. 2012, pages: 905-908.

[12] R. C. Gonzalez, Woods R. E. and Eddins S. L., 2009, "Digital Image processing Using MATLAB". Gatesmark PublishingA Division of Gatesmark, LLC.

[13] Shuqin Zhu, Congxu Zhu and Wenhong Wang, "A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256", 2018, MDPI-Entropy 2018, 20, 716; doi:10.3390/e20090716.

[14] Stinson D. R., Cryptography, Theory and Practice. Third edition: Chapman & Hall/CRC, 2006.

[15] Sun Qiudong, Guan Ping, Qiu Yongping, Xue Yunfeng "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling" 2012 9th International Conference on Fuzzy Systems and Knowledge

[16] William Stallings, "Cryptography and Network Security", Principles and Practice. Fifth edition.