IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Image Encryption and Decryption Algorithm using XOR Operator

Jampani Ravi, R. Bhavana, P. Ratna Rohith, P. Sai Kiran, P. Santhi Priyanka
Department of Electronics and Communication Engineering
S. R. K. R. Engineering College, Bhimavaram, A.P, India

Abstract: *As the result of the rapid development of technology, information science has become much easier, and therefore the problem of information security is growing. This paper deals with the secretiveness of images, so image encryption is that the latest trend in information caching. The novelty of the work lies in generating crucial images for encryption. The crucial image is then created with the assistance of a secret alphanumeric key. Each alphanumeric key will have an 8bit value generated by the binary key table. The challenge is to return up with an image encryption algorithm that is simple yet safe, with featherweight computer processing. This encryption algorithm which mixes Playfair cipher and therefore the Vigenere cipher gives better results. An experiment showed a correlation between the precipitation of the image after encryption and its decline. Supported the standard of quality of encryption, the speed of change of image pixels was high enough for the cipher image to be difficult to spot. The image is meant to be more distorted in this fashion. The deciphered image is obtained by applying the backward process.XOR technique is used in the present paper, for security analysis using XOR technique is an effective method of scrambling, in visual component which may be used as an important visual cryptography. For secure transmission of an image XOR cipher is a best technique.*

Keywords: Encryption, Decryption and Cryptography

I. INTRODUCTION

Computer-based image processing methods help manipulate digital images. In the form of imaging dataSatellite platform detectors contain scarcities. Experiencing colorful phases of processing prompts us to look beyond similar excrescences and encourages originality. Pre-processing, improvement and display, and information birth are the three general phases all types of data have to pass through when using digital fashion. A new fashion is needed for preventing information leakage as a result of the advancement of the data age. For digital data fashion had been developed that is cracking it[8]. This is converting data of readable form into non readable form, in order that if a hacker hack the information he cannot understand it until he know the decryption fashion and decryption word. Now a daysDigital revolution has changed the lifestyle of a common man. We are moving towards complete digitalization. Most importantly, transactions done using the digital system have saved our time and efforts. We use different forms of data such as audio voice and images to communicate from one end to another end. These data may carry plenty of important information especially for defense or any other ministry. Thus secure data transmission is a major area of concern for many researchers. Visual encryption is one of the techniques to hide the original message for unwanted persons. There are many techniques reported for visual encryption such as sub-image encryption method [2], Multilevel encoding [3], R prime shuffle technique [4], Block-based Scrambling [5], Random Grid technique [6], Arnold Cat map [7], etc. Our article deals with one of the methods to do the same. We have developed a new algorithm to scramble the image to provide security while sending the information to an individual. We performed various testing on the scrambled image to judge its capability to handle different types of attack.

1.1 Encryption

There are massive amounts of sensitive information managed and stored online in the cloud or on connected servers. Encryption uses cyber security to defend against brute-force and cyber-attacks, including malware and ransom ware [2]. Data encryption works by securing transmitted digital data on the cloud and computer systems. There are two kinds of digital data, transmitted data or in-flight data and stored digital data or data at rest.Modern encryption algorithms have

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

replaced the outdated Data Encryption Standard to protect data [9]. These algorithms guard information and fuel security initiatives including integrity, authentication, and non-repudiation. The algorithms first authenticate a message to verify the origin. Next they check the integrity to verify that contents have remained unchanged. Finally, the non-repudiation initiative stops sends from denying legitimate activity.

There are several different encryption methods, each developed with different security and security needs in mind. The two main types of data encryption are asymmetric encryption and symmetric encryption [4].

With more and more organizations moving to hybrid and multicloud environments, concerns are growing about public cloud security and protecting data across complex environments. Enterprise-wide data encryption and encryption key management can help protect data on-premises and in the cloud [4].

Cloud service providers (CSPs) may be responsible for the security of the cloud, but customers are responsible for security in the cloud, especially the security of any data. An organization's sensitive data must be protected, while allowing authorized users to perform their job functions. This protection should not only encrypt data, but also provide robust encryption key management, access control and audit logging capabilities.

Robust data encryption and key management solutions should offer:

- A centralized management console for data encryption and encryption key policies and configurations
- Encryption at the file, database and application levels for on-premise and cloud data
- Role and group-based access controls and audit logging to help address compliance
- Automated key lifecycle processes for on-premise and cloud encryption keys.

1.2 Decryption

Decryption is a Cyber Security technique that makes it more difficult for hackers to intercept and read the information they're not allowed to do [1]. It is transforming encrypted or encoded data or text back to its original plain format that people can easily read and understand from computer applications [8]. This is the reverse of encryption, which requires coding data to make it unreadable for all, but only those with matching Decryption keys can read it. Although encryption protects the data, recipients must have the right Decryption or decoding tools to access the original details. What Decryption does is unencrypt the data, which can be done manually, automatically, using the best Decryption software, unique keys, passwords, or codes [4]. This translates unreadable or indecipherable data into original text files, e-mail messages, images, user data, and directories that users and computer systems can read and interpret.

The reason for the use of Decryption is different, but adequate protection is one of the advantages. In particular, this technique gives the organization smooth management. The method helps Cyber Security professionals as it prevents the use of encryption to confuse ex fill iteration with confidential information [9].

The transformation of encrypted data to its original form is known as Data Decryption. It's basically a reverse encryption method. It decrypts encrypted information such that the authorized user can access the message only because Decryption requires a secret key or password [5].

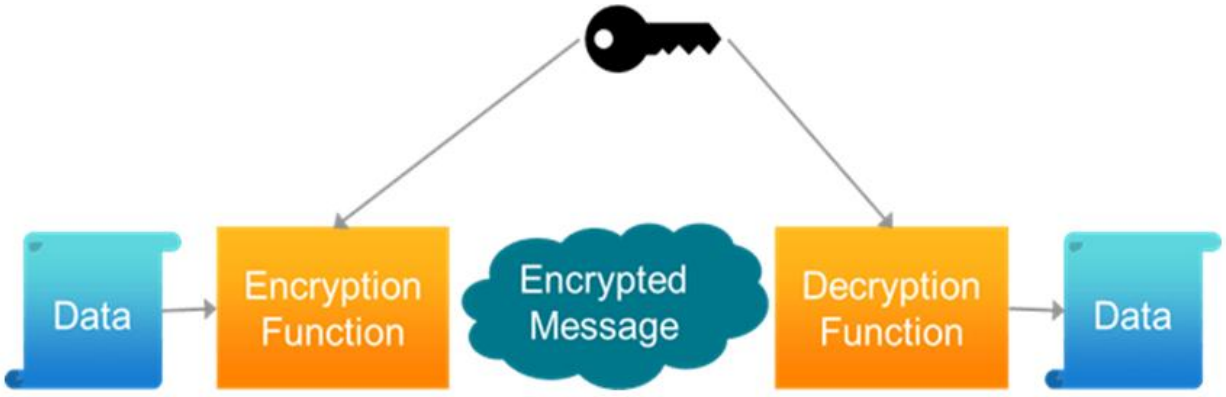
1.3 Cryptography

A general definition is constructing and analyzing protocols to overcome the influence of adversaries, which are combined with colorful aspects of information security such as data confidentiality, authentication, and non-repudiation [2]. Ultramodern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering [13]. Cryptography is used inATM cards, computer passwords, and electronic commerce [11].

In the pre-ultramodern era, encryption—the transformation of data from a legible state to apparent gibberish—was practically synonymous with cryptography [6]. The creator of a translated communication participated in the decoding fashion required to recover the initial information only with intended donors, preventing unauthorized individuals from trying to the same harmonious with this, they will choose a cipher, which means a secret key with the backing of that cipher, they will cipher the Communication [19]. Each letter of the ABC is moved a certain number of times during a Caesar cipher; for example, during a Caesar cipher with a shift of three, A would come D, B would come E, and Y would likewise come B [16].The Vigenère cipher is made up of a series of Caesar ciphers with varying shift values [12]. Charles Wheatstone created the Playfair Cipher scheme in 1854 [9]. However, Lord Playfair eventually became the name of the plan [14]. The Playfair Cipher, also known as Playfair Square, is a cryptographic method that's

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

employed for in-house knowledge encryption [11]. Theoretical developments, like as improvements in integer factorization methods, and quickly computing technology allow these results to be continuously adjusted, which is why these schemes are designated as computationally secure [15].



1.4 Need for Security

On mobile devices, data encryption eliminates the risks of loss or theft. Unauthorized users cannot utilise the data as a result of the process [4]. Typically, encryption software transforms data into "cipher text" by processing it through a mathematical calculation referred to as an algorithm. After this conversion, users must enter their own credentials in order to access the data [7]. They make it nearly impossible for anybody else to access the data if those credentials are kept confidential [5]. The majority of early computer programs had no security or, at best, very limited security [12]. This persisted for a while before the significance of data was finally understood [17]. Computer data was formerly seen to be useful but not something that needed to be protected [15]. The necessity for security became apparent in a way that had never been done before when computer applications were created to manage financial and personal data [16]. People were aware of how crucially significant computer data was to modern life. As a result, several aspects of security started to take centre stage [18].

The following are two common instances of such security measures: Give each user a user id and password, and then use those details to verify their identity [14]. Encrypt the data kept in the databases in some way to prevent users without the proper access from seeing it [13].

Technology advancements led to a highly developed communication infrastructure and the emergence of ever-more-novel apps to meet the expectations and needs of different user groups [19]. People quickly came to the conclusion that the fundamental security measures were insufficient [1].

In addition, the Internet grabbed the world by storm, and there were several instances of what might occur if applications made for the internet lacked adequate security. Therefore, techniques to safeguard information moving over the internet have been created [13].

Therefore, we are putting out a new technique called the enhanced encryption algorithm, which will make use of two carriers. Carrier1, also known as the Playfair cipher, and carrier 2, also known as the Vigenère cipher, are produced with the use of carrier1 and key stream generators. Dual security is provided through the use of two carriers, improving the encryption's quality. The primary phases of this method are two. Carrier1 and Carrier2 cipher generation and use with pictures[2].

II. METHODOLOGY

Although there are numerous ways out there, but here we tried to build the simplest and most secured way in order to perform Encryption and Decryption.

The proposed methodology to perform this process is using XOR operation. In here XOR operation is considered to be as one of the Symmetrical Encryption method.

In order to protect it from illegal access and keep it private and secure, we simply turn our data or information into secret code.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Firstly, let's understand the functionality of XOR operation:

The basic XOR cipher in cryptography is an example of an additive cipher, an encryption technique that functions in accordance with the principles

A^ 0 = A,
A ^ A = 0,
A ^B = B^A,
(A ^B)^ C = A ^(B^ C),
(B ^A)^ A = B^ 0 = B

This process is also known as modulus 2 addition (or subtraction, which is identical). According to this reasoning, a string of text may be encrypted by utilizing a specified key and the bitwise XOR operation on each character. Simply performing the XOR function again with the key will get rid of the encryption and allow you to decode the result.

Using the repeating key 11110011, the string "Wiki" (01010111 01101001 01101011 01101001 in 8-bit ASCII) may be encrypted as follows:

```
  01010111 01101001 01101011 01101001
^ 11110011 11110011 11110011 11110011
= 10100100 10011010 10011000 10011010
```

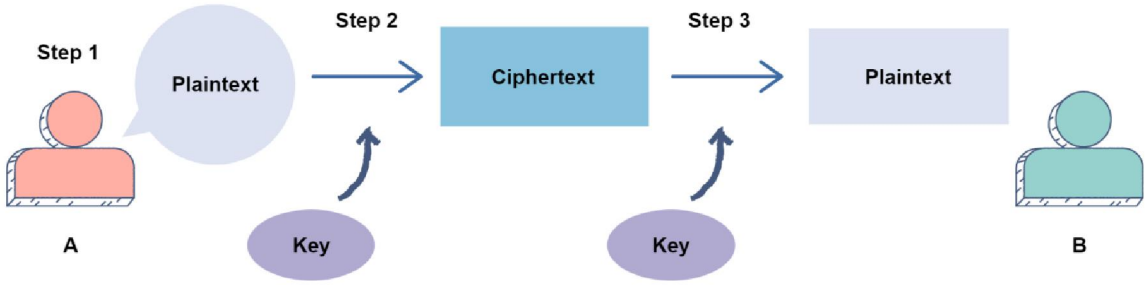
Likewise, for decryption:

```
  10100100 10011010 10011000 10011010
^ 11110011 11110011 11110011 11110011
= 01010111 01101001 01101011 01101001
```

Before delving into the operation of XOR encryption and decryption, it is crucial to establish the foundations of cryptography. Communication between two endpoints is protected by encryption. For instance, in order to encrypt and decode a message that A wants to transmit to B, both A and B need a key. These are the steps involved:

1) The original text message that A intends to convey to B is known as the plaintext.
2) The text that A has encrypted using the key is called the ciphertext.
3) B will use the key to convert the ciphertext back to the plaintext and read the message.

The steps above are shown in the figure below:



Now let's implement the above concept into .The software shown below illustrates the fundamental method of encryption using XOR operator:

```
# Assign values
data = 1281
key = 27

# Display values
print('Original Data:', data)
print('Key:', key)

# Encryption
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

```
data = data ^ key
print('After Encryption:', data)

# Decryption
data = data ^ key
print('After Decryption:', data)
```

As we can see, the program above uses two variables, data, and a key, and when we perform an XOR operation on them for the first time, we obtain encrypted data. After that, we obtain the same result as our input variable data when we again do the XOR operation between our data and key (decrypted data). When encrypting and decrypting a byte array of Images, the same reasoning will be used.

In the process of Encryption, we will first choose an image, after which we will convert it into a byte array, converting the entire image data into numeric form so that we can simply do the XOR operation on it. Now, the data will change anytime we apply the XOR function to each value in the byte array, making it impossible for us to access it. But we must always keep in mind that our encryption key is crucial because we cannot decrypt our image without it. It serves as a decryption password.

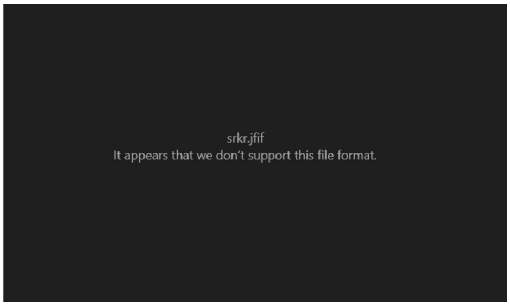
Now once when the Encryption is done and we have obtained an encrypted output to our image. And here the main thing is that only the sender and receiver will know the Key, which can be manually set by the sender while the process of Encryption. Through this we can obtain more security.

And when the topic comes to Decryption, It only involves transforming our encrypted data into readable form. Here, we'll use the same XOR procedure to decode a picture that has been encrypted. However, never forget that our encryption key and decryption key must match.

III. PROPOSED METHODOLOGY

Encryption key: 22

Input Image



Encrypted Image

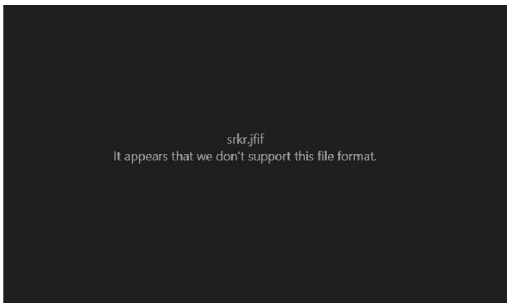
Decryption key: 22

Decrypted Image

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

Encryption key: 34

Input Image



Encrypted Image

Decryption key: 34

Decrypted image

Figure 1: Original and Encrypted image

In this methodology we do have the luxury of assigning Key of your choice. Basically the Key here is set-up by the Sender where as on the other hand the receiver can easily decrypt the file which has been already encrypted by simply using the Key setup by the sender at the time of Encryption.

3.1 Histogram Analysis

Histograms

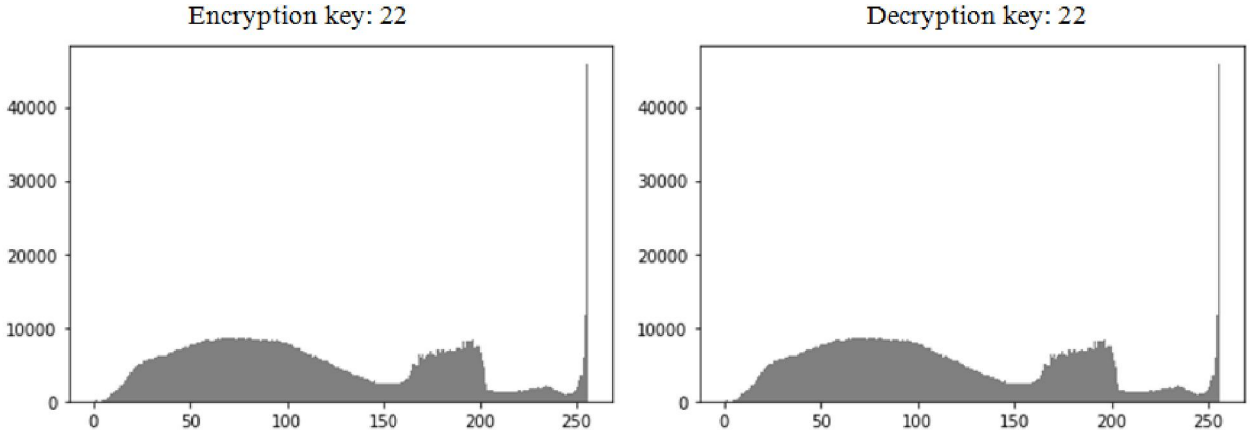


Figure 2: Histogram of Original and Encrypted images

- **Scrambling of Image:** Four images are used to analyzing their suitability of scrambling technique. Original images along with their scrambled images are shown in fig 1. Fig 1 is analyzed using XOR technique. we have done vertical correlation and horizontal correlation and histogram for supporting the above statement.
- **Histogram Analysis:** Generally histogram shows in an image distribution of pixel values. The four images of encrypted images and histogram images are as shown in fig 2. Every histogram of an picture shows the estimation of how the pixels are distributed. Based on results of histogram of fig 2 it is clear that XOR operation is very useful to secure the selected picture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

- **Adjacent Pixel Values**: The adjacent pixel values of a meaningful image always carry nearby values. So when we scramble an image we always expect those nearby pixel values to be scattered.
- **Information Entropy Analysis:** Entropy is a process of measure randomness of pixels in an image. If the random distribution of pixel is low then we can say that the image is meaningful. But if the random distribution of an image is high then we can say that the image is less meaningful. We have calculated randomness of different original images and their cipher images.

The visual values of picture pixel intensities are determined via histogram analysis. The histograms for the original image and the encrypted image are shown in Fig. 3, allowing us to observe how much the intensity values have been changed. To examine the compatibility of the color distribution between the plain picture and the cipher image, color histogram analysis is utilized. It may be argued that the cipher picture does not provide any hints to undertake a statistical attack on the encryption technique if the histogram value has a considerable distribution of diversity of the cipher image and also has a significant difference from the histogram of the plain image.

3.2 Results

Input imageEncrypted file

Decrypted file

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

3.3 Histogram Output for input Image

On execution, we have obtained the following results:

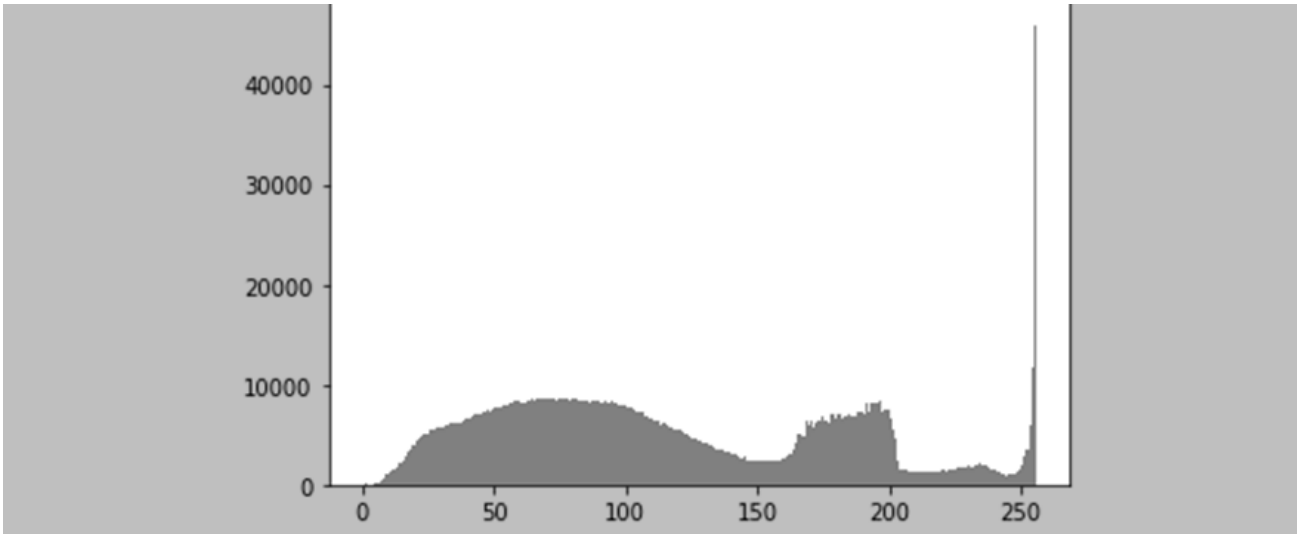


image mean: 118.06344217649648
image variance and std: 4464.0822151870725 66.81378761294013
histogram mean: 118.06344217649648
histogram variance and std: 4464.079084532487 66.81376418472834
histogram variance2 and std2: 4464.079084532486 66.81376418472833
normalized histogram mean: 0.4629938908882215
normalized histogram variance and std: 0.06865173524848116 0.2620147615087386
entropy: 5.325538336800033
normalized entropy: 0.96039096857068

3.4 Histogram Output for Output Image

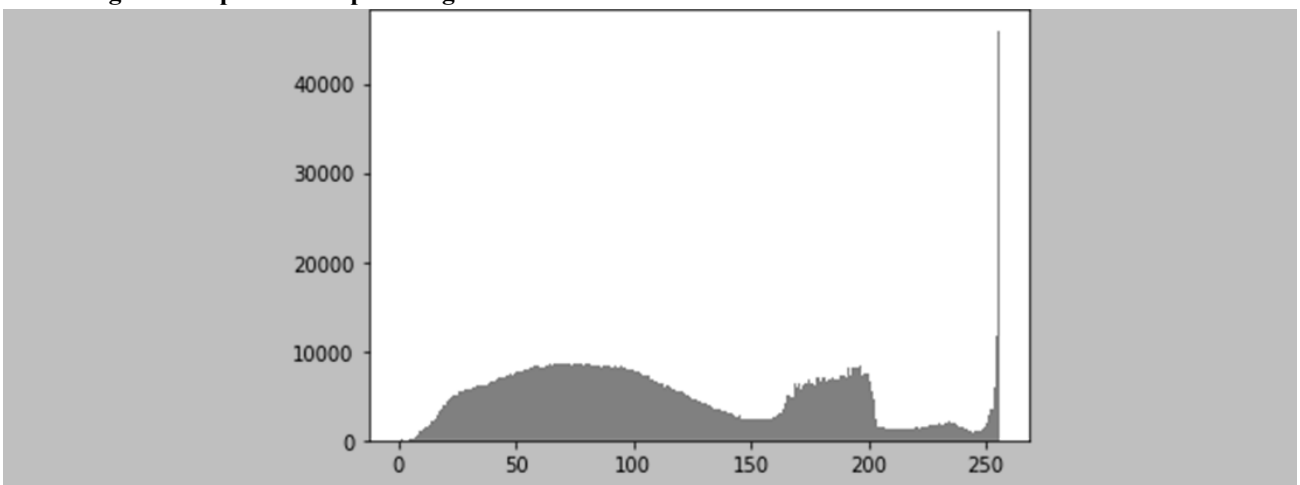


image mean: 118.06344217649648
image variance and std: 4464.0822151870725 66.81378761294013
histogram mean: 118.06344217649648
histogram variance and std: 4464.079084532487 66.81376418472834
histogram variance2 and std2: 4464.079084532486 66.81376418472833
normalized histogram mean: 0.4629938908882215
normalized histogram variance and std: 0.06865173524848116 0.2620147615087386
entropy: 5.325538336800033

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

normalized entropy: 0.9603909685706833

when the comparison comes to the Mean, Variance and Entropy values of both Input and Output image files, we obtain results as mentioned below:

Property	Value for Input Image	Value for Output Image
histogram mean	118.0634	118.0634
histogram variance	4464.0790	4464.0790
histogram entropy	5.3255	5.3255

IV. CONCLUSION

This paper proposes an image encryption technique that makes use of the XOR operator. Based on the results XOR cipher is an important tool to encrypt an picture. When we use XOR cipher randomness of pixels of an original picture increase. Suppose randomness is higher , we can say that the picture is high secure. Using a key, the XOR operator is used to odd rows and columns of a picture to muddle the link between the original and encrypted images. Even rows and columns of the picture are treated with the same key that has been flipped. The suggested algorithm's resistance to many forms of assaults, including statistical and differential attacks, has been tested experimentally with comprehensive numerical analysis (visual testing). Furthermore, performance evaluation experiments show how extremely secure the suggested picture encryption technique is. Additionally, it has quick encryption and decryption capabilities, making it appropriate for real-time Internet encryption and transmission applications.

By analyzing histogram, horizontal and vertical correlation, information entropy it can be concluded that after scramble different images the randomness increases in their ciphered images, it means the ciphered images are more secure that it is not possible to decrypt. The security keys which are used to encrypt and decrypt the original images are same. In this process to encrypt an image XOR operation is performed between original image and security key. Then to decrypt the image again XOR operation is performed between encrypted image and Security key. So decryption using security key is totally dependent on the result after encryption. So we can conclude that this process increases security of an image.

REFERENCES

[1]. P. Sharma, D. Mishra, V.K. Sarthi, P. Bhatpahri and R. Shrivastava, “Visual Encryption Using Bit Shift Technique”, International Journal of Scientific Research in Computer Science and Engineering, Vol. 5, No. 3, pp. 57-61, June 2017.

[2]. XY Wang, YQ Zhang and LT Liu, “An enhanced sub-image encryption method”, Optics and Laser in Engineering, Vol. 86, pp. 248-254, November 2016

[3]. CC Lee, HH Chen, HT Liu, GW Chen and CS Tsai, “A new visual cryptography with multi-level encoding”, Journal of Visual Languages and Computing, Vol. 2,No. 3, pp. 243-250, June 2016.

[4]. HB Kekre, T Sarode and P. Halarnkar, “Image Scrambling using RPrime Shuffle”, International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, Vol. 2, No. 8, pp. 4070 – 4076, August 2013.

[5]. Z. Hua and Y. Zhou, “Design of image cipher using block-based scrambling and image filtering”, Information Sciences, Vol. 396, pp. 97-113, August 2017.

[6]. T Guo, F Liu and C. Wu, “k out of k extended visual cryptography scheme by random grids”, Signal Processing, Vol. 94, pp. 90-101, January 2014.

[7]. A. Soleymani, M. J. Nordin and E. Sundarajan, “A Chaotic Cryptosystem for Images Based on Henon and Arnold Cat Map”, The Scientific World Journal, 2014. DOI:-http://dx.doi.org/10.1155/2014/536930.

[8]. X.Y. Wang, F. Chen and T. Wang, “A new compound mode of confusion and diffusion for block encryption of image based on chaos”, Communications in Nonlinear Science and Numerical Simulation, Vol. 15,No. 9, pp. 2479-2485, September 2010.

[9]. L. Sui and B. Gao, “Single-channel color image encryption based on iterative fractional Fourier transform and chaos”, Optics & Laser Technology, Vol. 48, pp. 117-127, June 2013.

[10]. H. Li, Y. Wang, H. Yan, L. Li, Q. Li and X. Zhao, “Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform”, Optics and Lasers in Engineering, Vol. 51, No. 12, pp.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, March 2023
Impact Factor: 7.301

1327-1331, 2013.

[11]. A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map", Communications in Nonlinear Science and Numerical Simulation, Vol. 17, No. 7, pp. 2943-2959, July 2012.

[12]. C.Y. Song, Y.L. Qiao and X.Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos", Optik, Vol. 124, No.18, pp. 3329-3334, September 2012.

[13]. N. Singh and A. Sinha, "Optical image encryption using improper Hartley transforms and chaos", Optik, Vol. 121, No. 10, pp. 918- 925, June 2010.

[14]. A. Akhshani, S. Behnia, A. Akhavan, H.A. Hassan and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps", Optics Communications, Vol. 283, No. 17, 3259- 3266, September 2010.

[15]. X. Y. Wang, Y.Q Zhang, and L.T. Liu, "An enhanced sub-image encryption method", Optics and Laser in Engineering, Vol. 86, pp. 248-254, November 2016.

[16]. B. Stoyanov, and K. Kordov, "Image Encryption Using Chebyshev Map and Rotation Equation", Entropy, Vol. 17, pp. 2117-2139, April 2015.

[17]. X. Tong, Y. Liu, M. Zhang, H. Xu and Z. Wang, "An Image Encryption Scheme Based on Hyperchaotic Rabinovich and Exponential Chaos Maps", Entropy, Vol. 17, pp. 181-196, January 2015.

[18]. Yue Wu, Student Member, IEEE, Joseph P. Noonan, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011

[19]. https://en.wikipedia.org/wiki/Differential_cryptanalysis, accessed on 16 June 2017. AJCST Vol.7 No.1 January-June 2018